



AWS
re:Invent

NET 315 - R

AWS Direct Connect with AWS Transit Gateway

Christian Elsen

Sr. SA, Networking Specialist
Amazon Web Services

Agenda

Target architecture

Building blocks

Scenario 1: AWS Direct Connect gateway for cross-region connectivity

Scenario 2: AWS Transit Gateway for hybrid connectivity

Scenario 3: Traffic isolation with AWS Transit Gateway

Q&A

Related breakouts

NET317 Connectivity to AWS and hybrid AWS network architectures

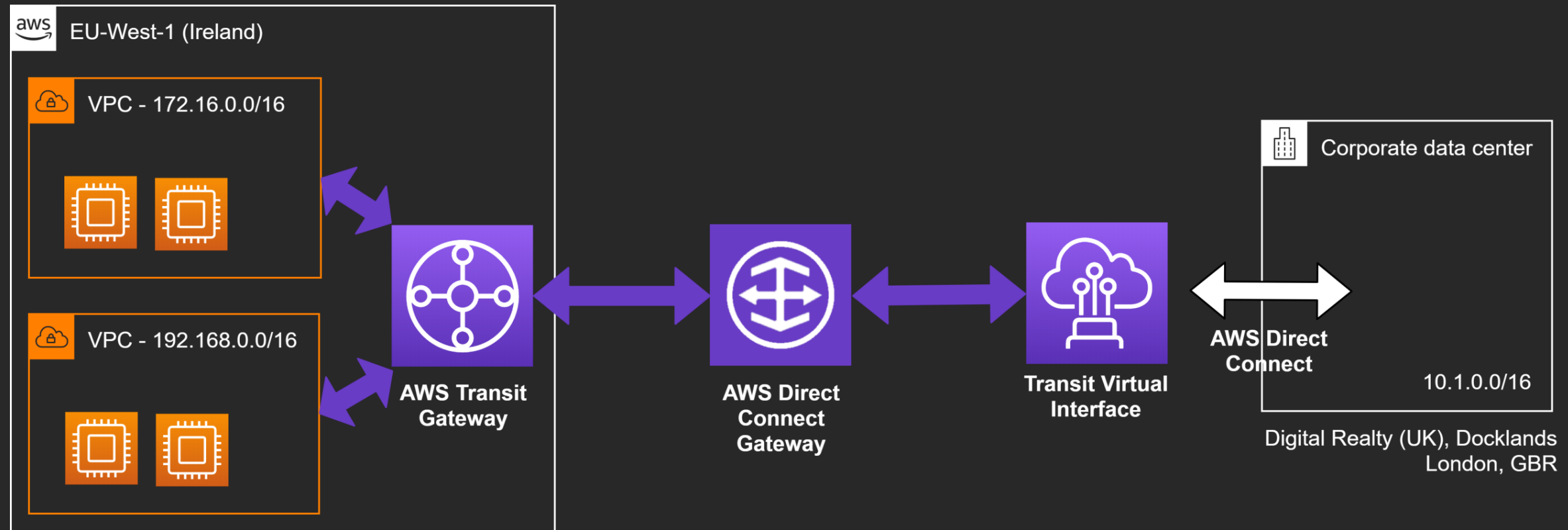
NET406 AWS Transit Gateway reference architectures for many VPCs

NET333 Building hybrid architectures with AWS Transit Gateway, AWS Direct Connect, and VPNs

NET204 Hybrid connectivity on AWS

Target architecture

AWS Transit Gateway with AWS Direct Connect



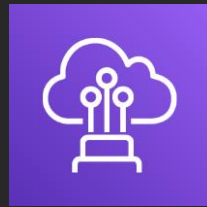
Building blocks

Building blocks



AWS Transit Gateway

Easily scale connectivity across thousands of Amazon VPCs, AWS accounts, and on-premises networks



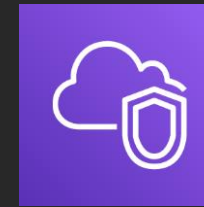
DX

Establish private connectivity between AWS and on-premises



AWS Direct Connect gateway

Connect to multiple VPCs, spread across multiple AWS regions through a single BGP session



Amazon VPC

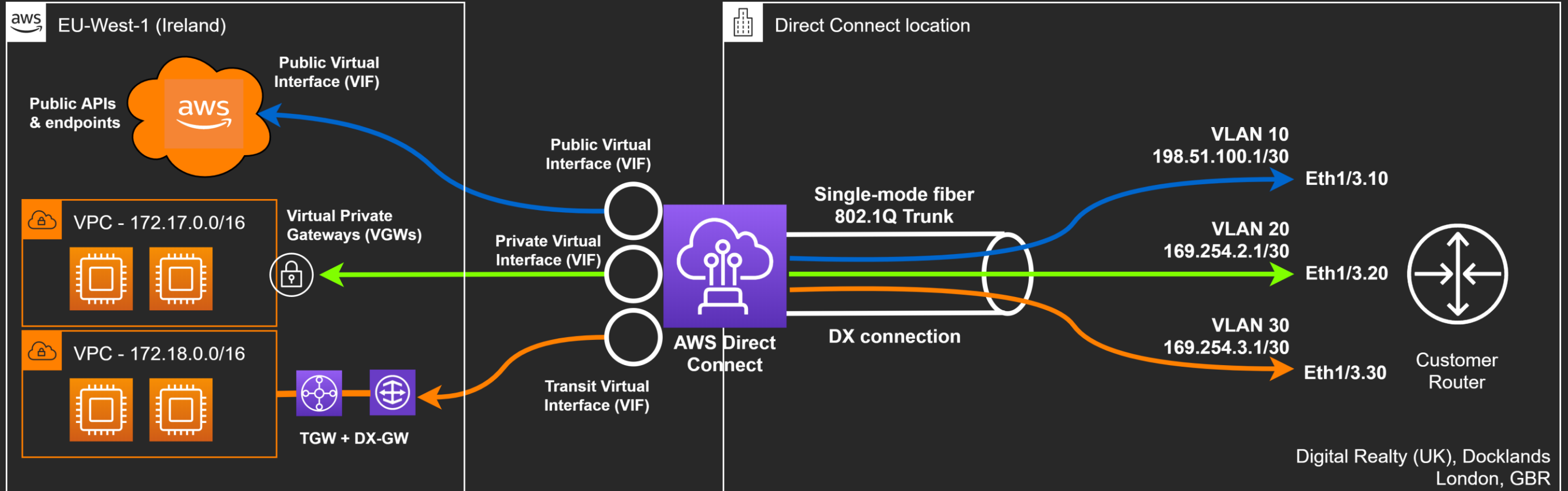
Provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define



On-Premises

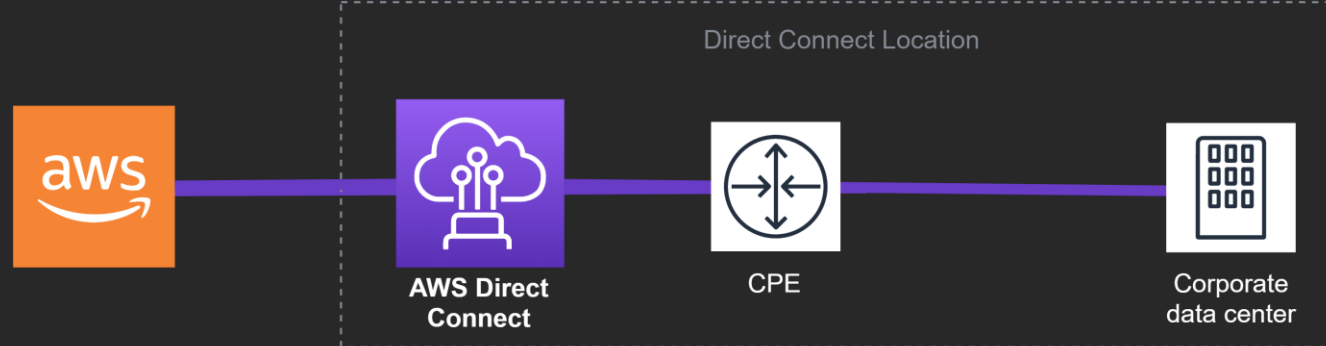
Your datacenter, office, or colocation environment

Direct Connect – Virtual Interfaces

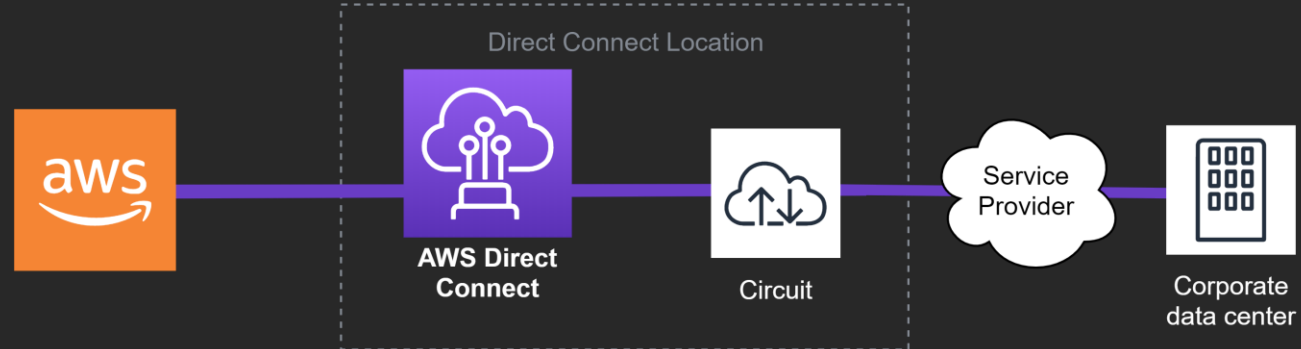


Direct Connect options

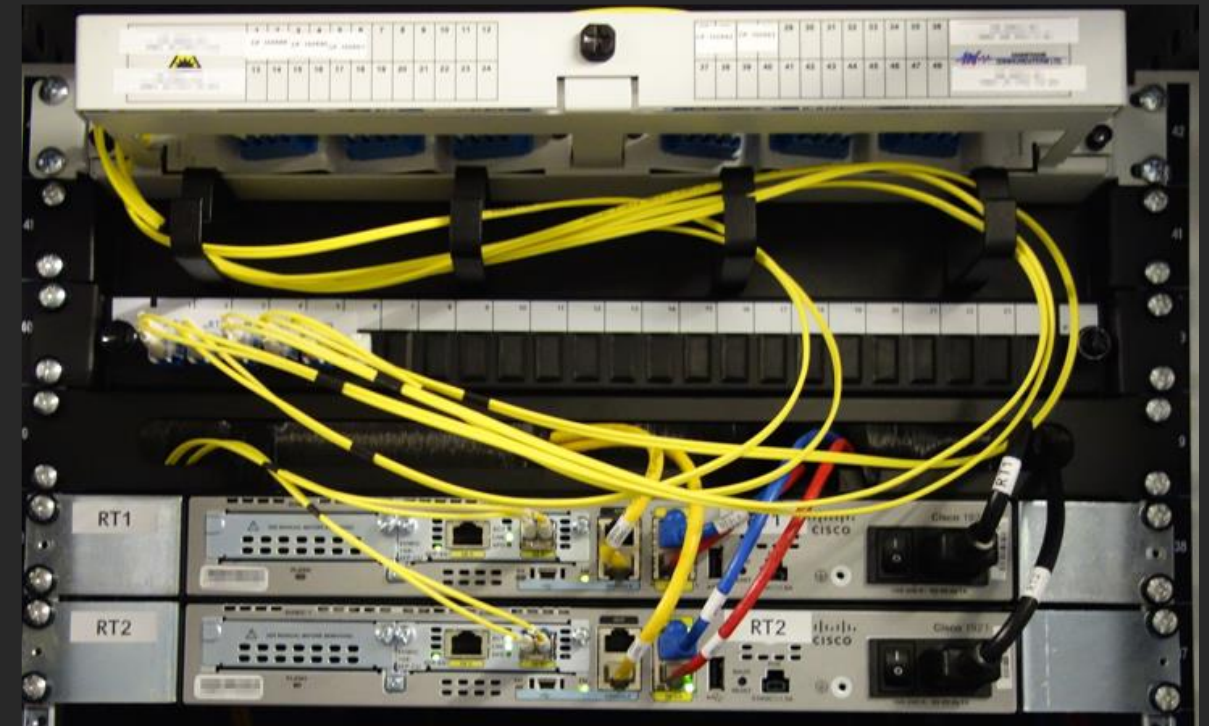
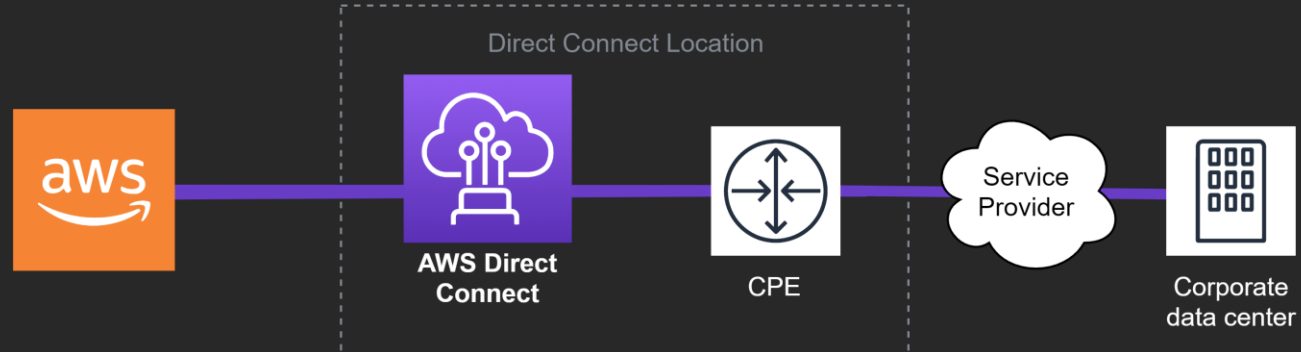
Option 1: Customer presence in the same DX location



Option 2: Circuit between customer data center and DX location



Option 3: Service provider network extending to DX location (e.g MPLS)



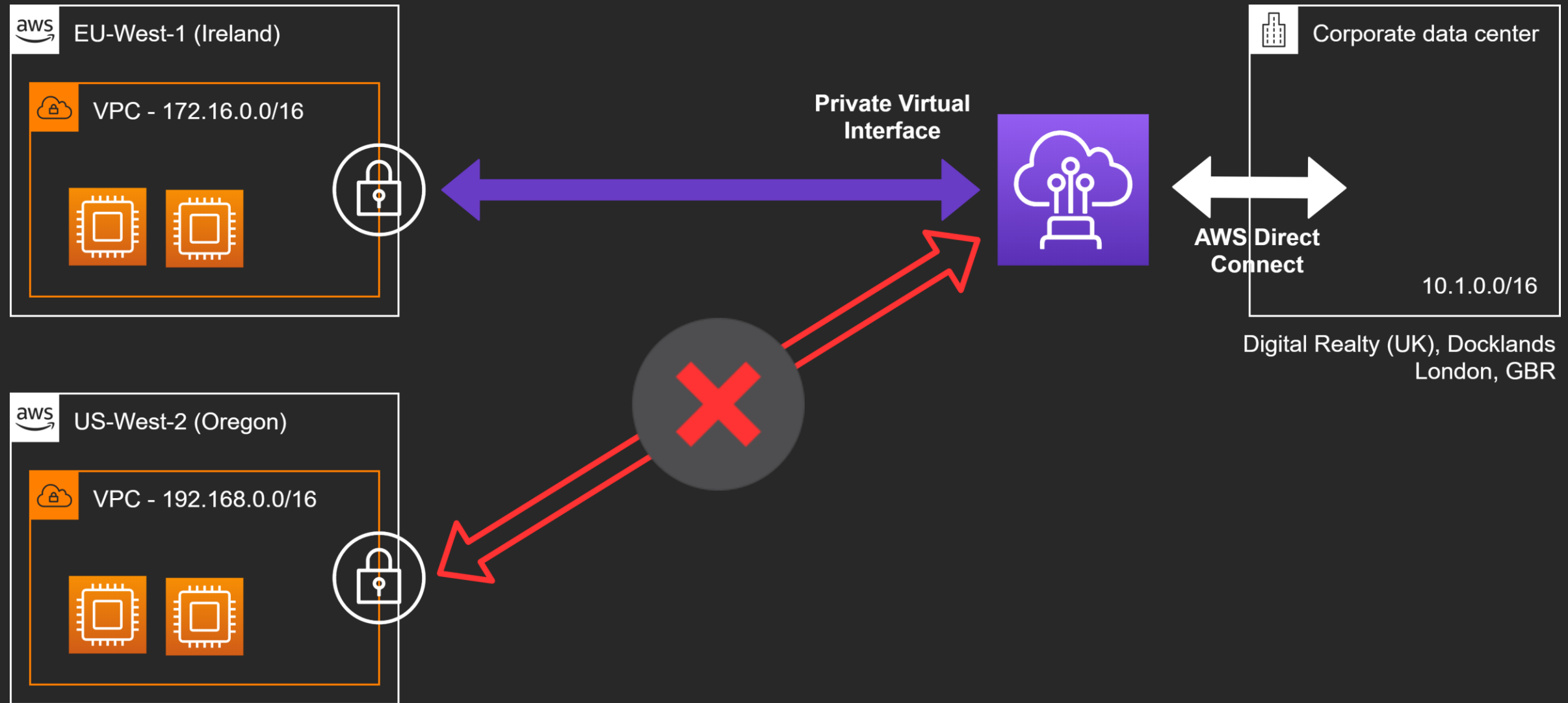
Direct Connect options and AWS Transit Gateway

	Dedicated Connections	Hosted Connections	Hosted Virtual Interfaces
AWS assigned capacity	1Gbps or 10Gbps	50Mbps to 10Gbps	None
Private or Public Virtual Interfaces (VIF)	50	1	1
Transit Virtual Interface (VIF)	1	1 (if assigned capacity >= 1Gbps)	None

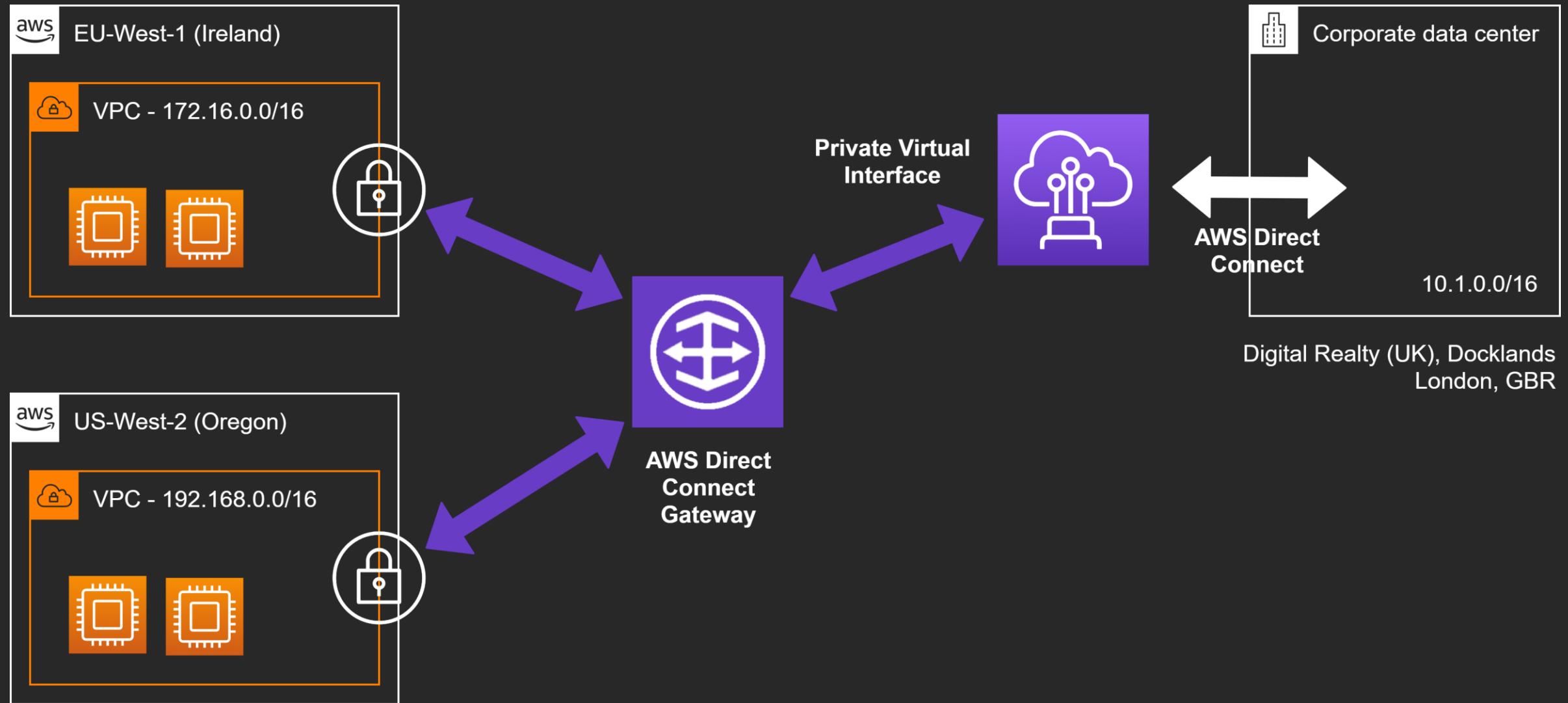
Partner offering

Scenario 1: AWS Direct Connect gateway for cross-region connectivity

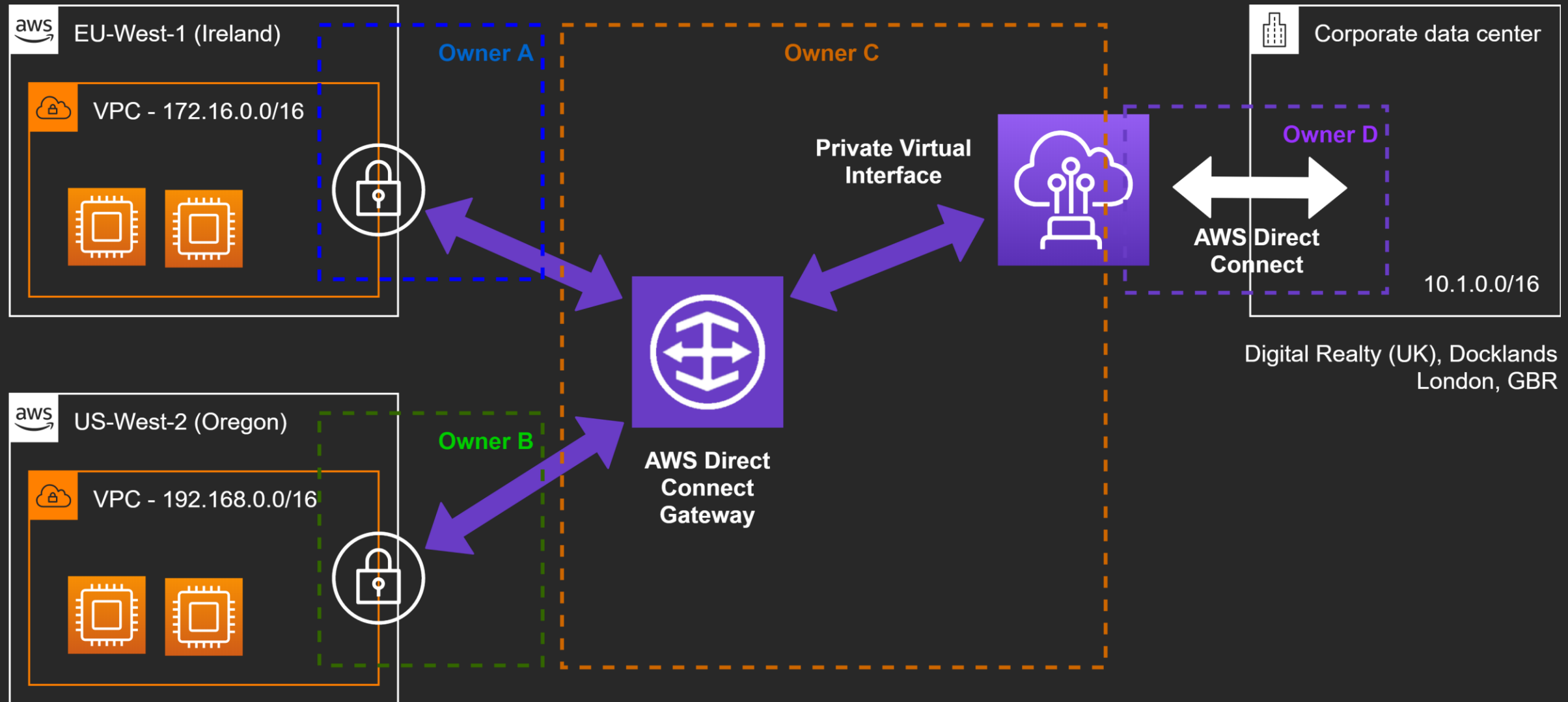
AWS Direct Connect with associated region



AWS Direct Connect Gateway



AWS Direct Connect Gateway Account Ownership



Step 1

Create DX Gateway

From account “C” (DX-GW owner)

Specify BGP ASN of DX Gateway

Direct Connect gateway settings

Name
A name to help you identify the new Direct Connect gateway.

reInvent-NET315

Name must contain no more than 100 characters. Valid characters are a-z, 0-9, and – (hyphen)

Amazon side ASN
The Autonomous System Number for the new Direct Connect gateway.

64512

Valid ranges are 64512 - 65534 and 42000000000 - 4294967294.

Cancel

Create Direct Connect gateway

Step 2

Create Private VIF

From account “D” (DX-CON owner)

Place VIF into account “C”

Specify VLAN + on-premises BGP ASN

Virtual interface type

Type

☒ **Private**
A private virtual interface should be used to access an Amazon VPC using private IP addresses.

☐ **Public**
A public virtual interface can access all AWS public services using public IP addresses.

☐ **Transit**
A transit virtual interface is a VLAN that transports traffic from a Direct Connect gateway to one or more transit gateways.

Private virtual interface settings

Virtual interface name
A name to help you identify the new virtual interface.

Name must contain no more than 100 characters. Valid characters are a-z, 0-9, and - (hyphen)

Connection
The physical connection on which the new virtual interface will be provisioned.

AWS EMEA Lab DX2

Virtual interface owner
The account that will own the virtual interface.

☐ My AWS account

☒ Another AWS account

Virtual interface owner
The account that will own the virtual interface.

VLAN
The Virtual Local Area Network number for the new virtual interface.

Valid ranges are 1 - 4094

BGP ASN
The Border Gateway Protocol Autonomous System Number of your gateway for the new virtual interface.

Valid ranges are 1 - 2147483647.

► Additional settings

Step 2

Create Private VIF

From account "D" (DX-CON owner)

Place VIF into account "C"

Specify VLAN + on-premises BGP ASN

Configure router

Account "D" (DX-CON owner) "owns"
physical router (download config)

```
!=====IPV4=====
interface GigabitEthernet0/1.101
  description "Direct Connect to your Amazon VPC or AWS Cloud"
  encapsulation dot1Q 101
  ip address 169.254.254.2 255.255.255.252

router bgp 65000
  address-family ipv4
    neighbor 169.254.254.1 remote-as 64512
    neighbor 169.254.254.1 password 0xGf0WuAv11bHvFb3Ud12XeC
    network 0.0.0.0
exit
```

Step 2

Create Private VIF

- From account “D” (DX-CON owner)
- Place VIF into account “C”
- Specify VLAN + on-premises BGP ASN

Configure Router

- Account “D” (DX-CON owner) “owns” physical router (download config)

Accept Private VIF

- From account “C” (DX-GW owner)
- Attach to DX Gateway

DXVIF-FFSP2CBD

AcceptDelete

General configuration

Virtual interface ID

dxvif-ffsp2cbd

Virtual interface name

reInvent2019-Net315

AWS account

Virtual interface type

private

State

confirming

VLAN

101

Region

eu-west-1

Amazon side ASN

9059

Connection ID

Location

Digital Realty (UK), Docklands, London, GBR

AWS device

TCSH-46zoewxlnf2d

MTU

1500

Jumbo frame capable

true

Peerings

Tags

Peerings (1)

DeleteAdd peering

	ID	Name	BGP ASN	BGP authentication key	Your router peer IP	Amazon router peer IP	AWS device	State	BGP status
	dxpeer-fg4o2l4q	ipv4	65000	-			TCSH-46zoewxlnf2d	pending	down

Virtual interface settings

Gateway type

Gateway type for this virtual interface.

Direct Connect gateway

Virtual private gateway

Direct Connect gateway

The Direct Connect gateway to which the new virtual interface will be attached.

reInvent-NET315

Cancel

Accept virtual interface

Step 3

Create Virtual Gateway (VGW)

From account “A” (VPC owner)

Here: Chosen ASN irrelevant

Attach VGW to VPC

Determines CIDR to be announced via DX-GW to on-premises

Here: Default VPC

Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag ⓘ

ASN ☒ Amazon default ASN ⓘ ☐ Custom ASN

* Required

Cancel Create Virtual Private Gateway

Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id vgw-0c35a783c4b6e6eee

VPC* ⓘ

* Required

Cancel Yes, Attach

Step 4

Associate VGW with DX-GW

From account “A” (VPC owner)

Specify DX-GW ID

Optional: Prefix filter to be announced from VGW

Accept VGW association

From account “C” (DX-GW owner)

Ability to review and correct prefix filter

Association account type

Account owner

☐ My account

Associate a Direct Connect gateway to my own account.

☒ Another account

Associate a Direct Connect gateway to another account.

Association settings

Direct Connect gateway ID

The ID of the Direct Connect gateway that you wish to associate to this gateway.

XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

Direct Connect gateway owner

The ID of the AWS account that owns the Direct Connect gateway

123412341234

Allowed prefixes - optional

List of prefixes you want to be allowed to be advertised to the on-premises network through the Direct Connect gateway.

192.0.20.0/28

192.0.2.28/30

Specify up to 20 prefixes separated with commas or put each on a new line.

Cancel

Associate Direct Connect gateway

General configuration

ID

1a15c24a-94b1-4e39-9cc2-b57ad9447802

AWS account

Amazon side ASN

64512

Name

reInvent-NET315

State

available

Association proposals

Virtual interface attachments

Gateway associations

Association proposals (1)

Reject Proposed Association

Accept

Search association proposals

<input checked="" type="checkbox"/>	Proposal ID	Gateway ID	Region	AWS account	Requested allowed prefixes	State
<input checked="" type="checkbox"/>	5f6aeb1f-76a4-4d65-8977-263b50995bae	vgw-0c35a783c4b6e6eee	us-west-2		172.31.0.0/16	requested

Step 5

Validate BGP routing

VPC Route table

On-Site router

Route Table: rtb-243b194c

Summary

Routes

Subnet Associations

Route Propagation

Tags

Edit routes

View

All routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
0.0.0.0/0	igw-2f756d46	active	No
0.0.0.0/0	vgw-02c453c01843d7c43	active	Yes

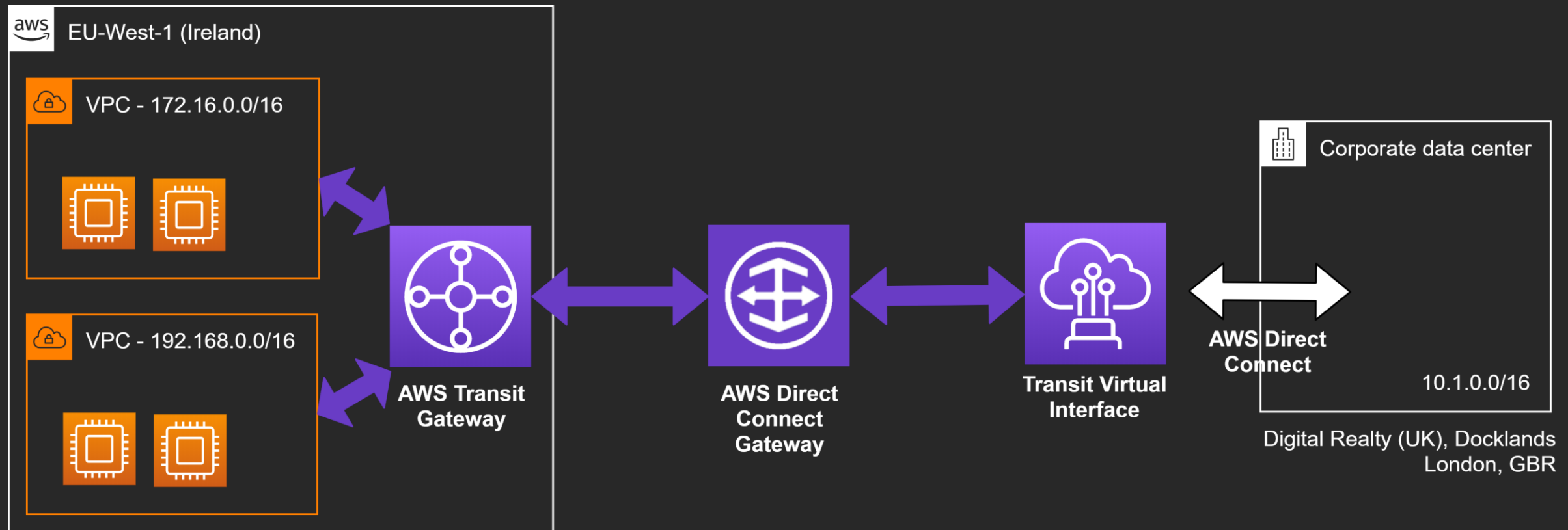
```
RT2#sh ip bgp
BGP table version is 3, local router ID is 192.168.52.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

      Network        Next Hop           Metric LocPrf Weight Path
*> 0.0.0.0           62.216.229.129      0         32768 i
*> 172.31.0.0        169.254.254.1       0         0 64512 i
RT2#
```


Demo

Scenario 2: AWS Transit Gateway for hybrid connectivity

Hybrid connectivity with Transit Gateway



Scenario 2

Access multiple VPCs

Within same region

Allow connectivity between VPCs and to on-premises

Direct Connect requirements

Uses Transit VIF

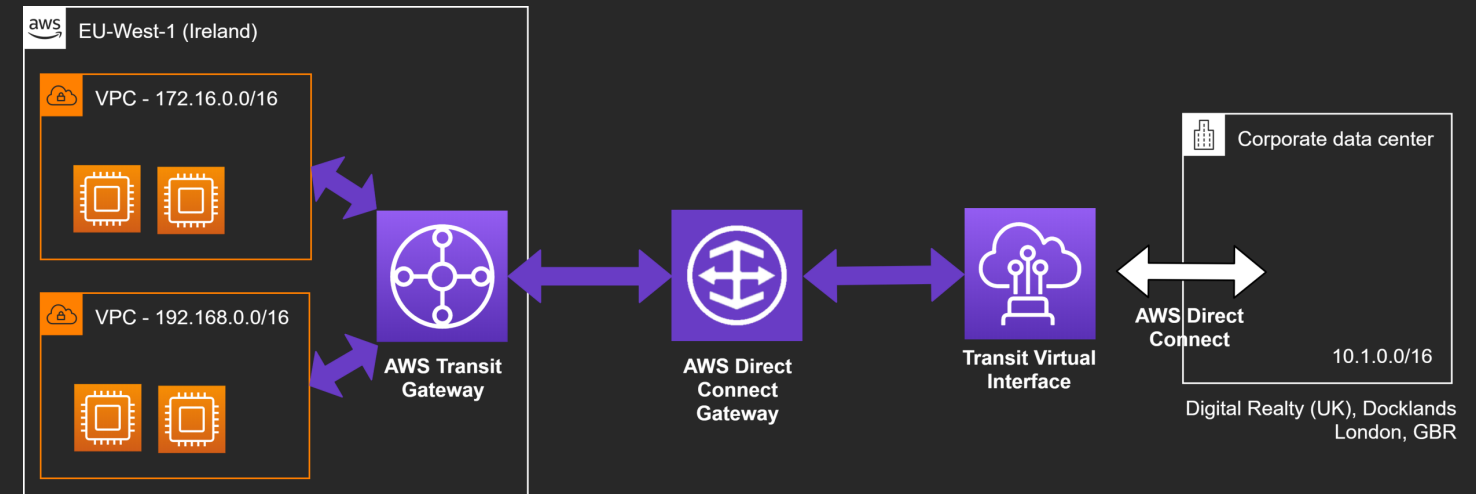
Account ownership

Optional: Split across AWS accounts

Typical:

Account 1: DX + DX Gateway + Transit GW

Account 2 – n: “Leaf” VPCs



Step 0

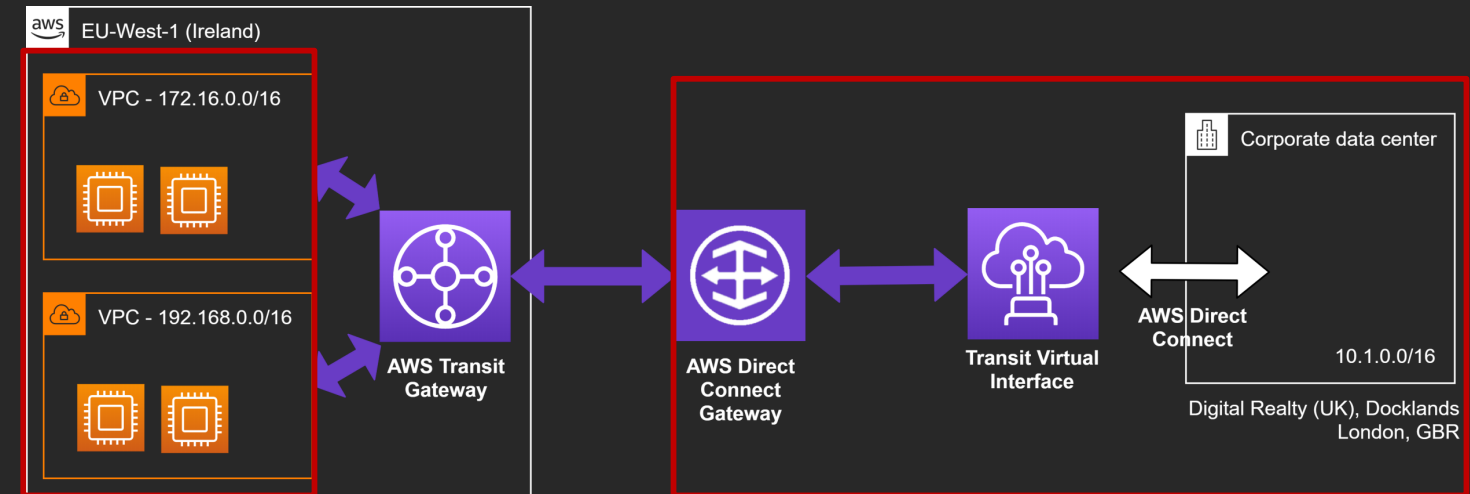
Prepared beforehand

Transit Virtual Interface

Physical router configuration

Direct Connect Gateway

Transit VIF attached



Step 1

Create Transit Gateway (TGW)

Specify BGP ASN of Transit Gateway

BGP ASN cannot overlap with DX-GW

Use unique ASN in each AWS region

Default route table behavior

Important for next use case

Here: Leave defaults

Create Transit Gateway

A Transit Gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across accounts.

Name tag ⓘ

Description ⓘ

Configure the Transit Gateway

Amazon side ASN ⓘ

DNS support ☒ enable ⓘ

VPN ECMP support ☒ enable ⓘ

Default route table association ☒ enable ⓘ

Default route table propagation ☒ enable ⓘ

Configure sharing options for cross account

Auto accept shared attachments ☐ enable ⓘ

* Required

Step 2

Associate TGW with DX-GW

Specify BGP prefix origination

Mandatory, not optional

Different from BGP prefix filter with
DX-GW + VGW

Here: 172.16.0.0/12

Associate gateway

Association settings

Gateways

The gateway you want to associate with the new Direct Connect gateway

My gateway

reInvent-NET315

tgw-03277a60adac28b05 us-east-1



You can only associate gateways of the same type to a Direct Connect gateway

Allowed prefixes

List of prefixes you want to originate on the Direct Connect gateway and be advertised to the on-premises network.

172.16.0.0/12

Specify up to 20 prefixes separated with commas or put each on a new line.

Cancel

Associate gateway

Step 3

Attach VPC to TGW

Select applicable subnets

Creates ENI in subnets

Determines routing within VPC
(route table associated with subnet)

Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID*

Attachment type ☒ VPC ☐ VPN

VPC Attachment

Select and configure your VPC attachment.

Attachment name tag

DNS support ☒ enable

IPv6 support ☐ enable

VPC ID*

Subnet IDs*

	Availability Zone	Subnet ID
<input checked="" type="checkbox"/>	eu-west-1a	<input type="text" value="subnet-3ee8e149"/>
<input checked="" type="checkbox"/>	eu-west-1b	<input type="text" value="subnet-8a4f6ed3"/>
<input checked="" type="checkbox"/>	eu-west-1c	<input type="text" value="subnet-455fbe21"/>

* Required

Step 3

Attach VPC to TGW

Select applicable subnets

Creates ENI in subnets

Determines routing within VPC
(route table associated with subnet)

Update VPC route table

Point desired CIDRs to TGW attachment

Edit routes

Destination	Target	Status	Propagated	
172.31.0.0/16	local	active	No	
0.0.0.0/0	igw-bee296db	active	No	✕
10.0.0.0/8	tgw-		No	✕

Add route

tgw-0c3ae4dd16bdfaf57 reinvent-NET315

* Required

Cancel Save routes

Step 4

Validate BGP routing

TGW Route table

On-Site router

Transit Gateway Route Table: tgw-rtb-0ae63d0a4ac97f842

DetailsAssociationsPropagationsRoutesTags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create routeReplace routeDelete route

Filter by attributes or search by keyword

	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	0.0.0.0/0	tgw-attach-05399951e029316df 47039a79-bdaf-4007-af75-707ceeeb2a30	Direct Connect Gateway	propagated	active
<input type="checkbox"/>	172.31.0.0/16	tgw-attach-064d43772ac361961 vpc-890071e1	VPC	propagated	active
<input type="checkbox"/>	192.168.0.0/16	tgw-attach-07a3fd66bdb33f582 vpc-00963551d470ed132	VPC	propagated	active

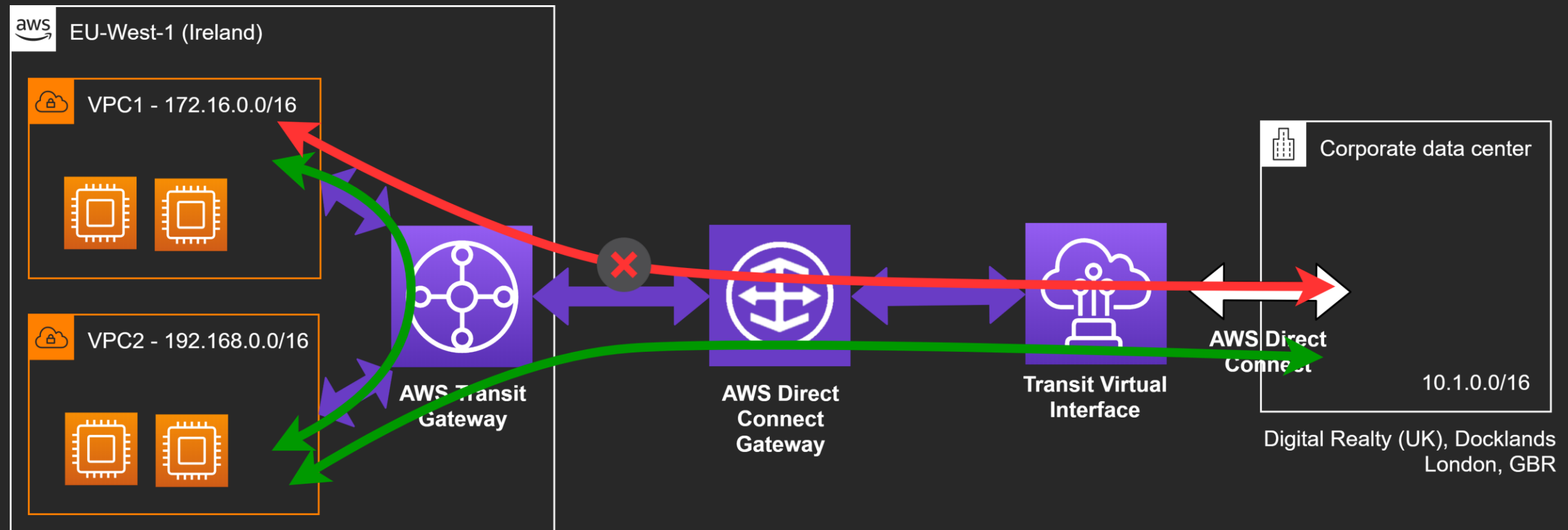
```
RT2#sh ip bgp
BGP table version is 6, local router ID is 192.168.52.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

      Network            Next Hop           Metric LocPrf Weight Path
*>  0.0.0.0              62.216.229.129         0           32768 i
*>  172.16.0.0           169.254.254.5          0        64514 i
*>  192.168.0.0/16       169.254.254.5          0        64514 i
RT2#
```


Demo

Extra Credit: Traffic isolation with Transit Gateway

VPC traffic isolation with Transit Gateway



Try yourself

Security controls for multiple VPCs

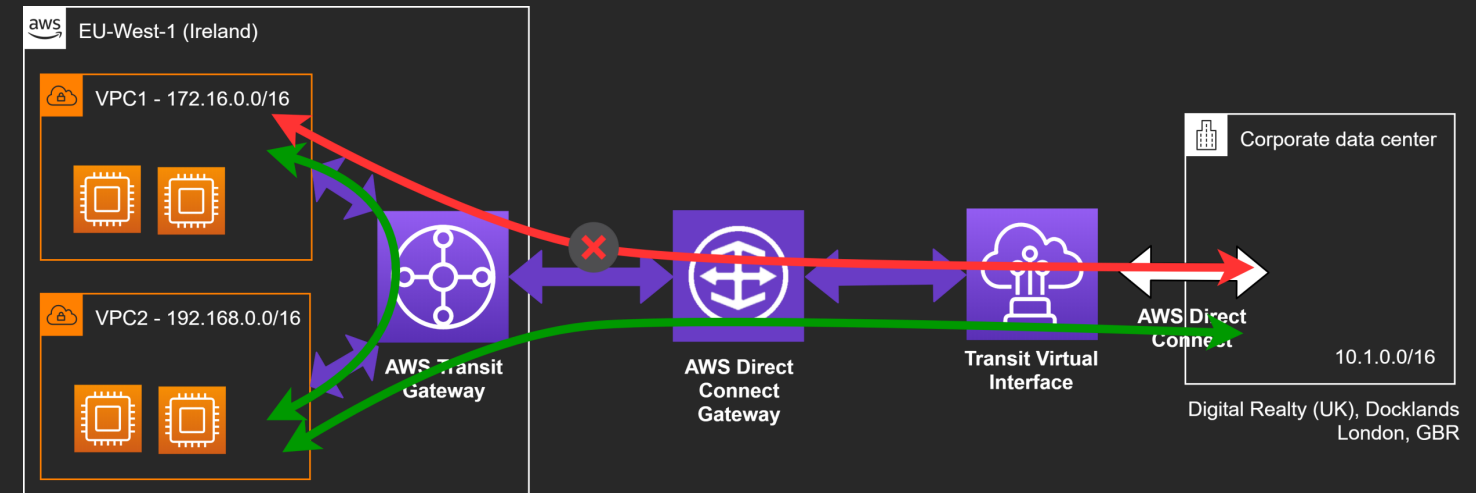
Manage connectivity between VPCs and to on-premises

Leverage Transit Gateway Route Tables

Here: Use VPC for traffic inspection, e.g. DPI

Possible: Centralized ingress/egress routing to Internet

How would you accomplish this?



Try yourself - Hint

Use TGW Route Tables

TGW can have multiple Route Tables

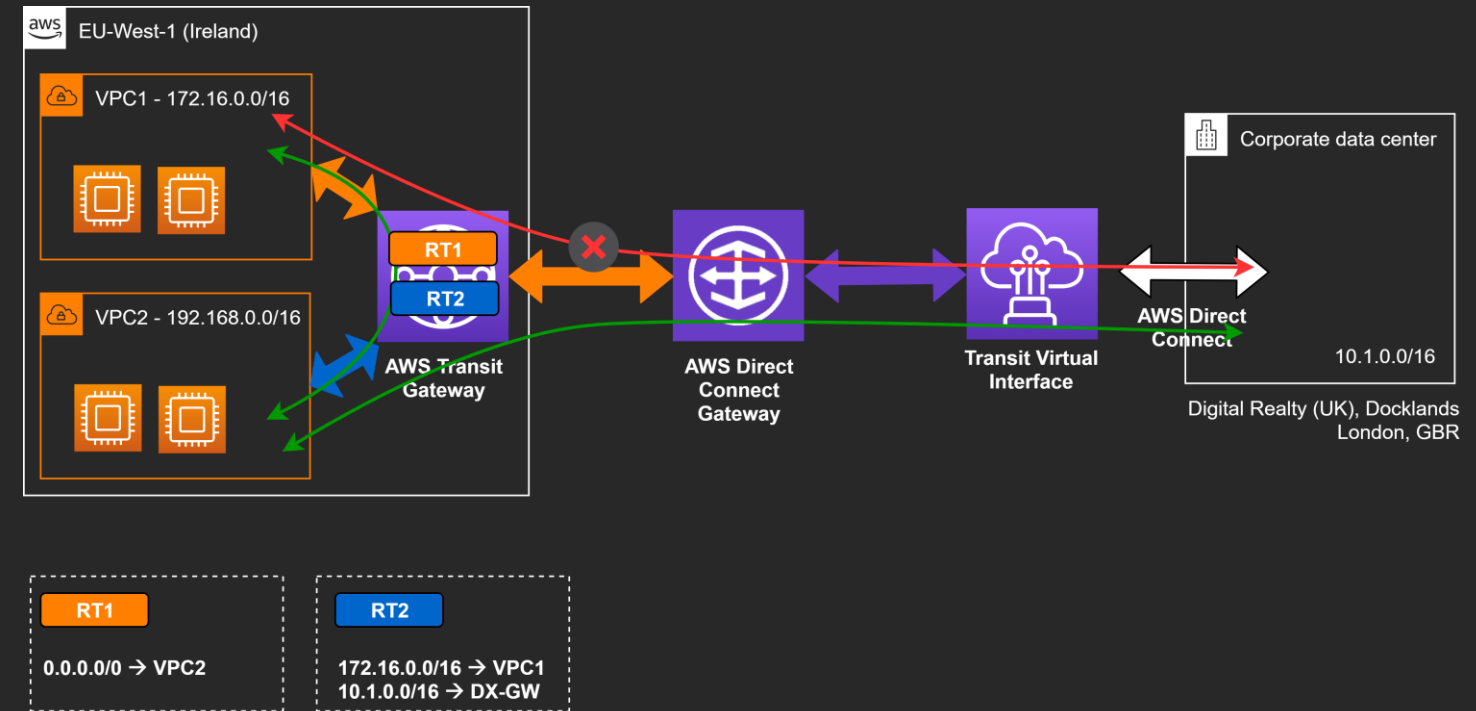
Each attachment drops traffic into one route table

Route tables can use any attachment as target

VPC / DX CIDRs can be automatically propagated into route table

Here: Don't want default route table association and propagation at the same time

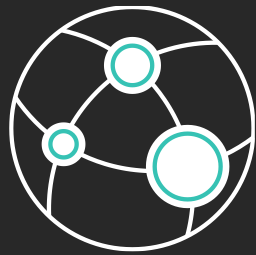
At home: Replace DX with VPN + EC2 Linux instance to experiment



Questions & Answers

Learn networking with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate networking skills



Free digital courses cover topics related to networking and content delivery, including Introduction to Amazon CloudFront and Introduction to Amazon VPC



Validate expertise with the
AWS Certified Advanced Networking - Specialty exam

Visit aws.amazon.com/training/paths-specialty

Thank you!

Christian Elsen

elsenc@amazon.com



Please complete the session
survey in the mobile app.