AWS re:Invent

NET315-R

AWS Direct Connect with AWS Transit Gateway

Christian Elsen

Sr. SA, Networking Specialist
Amazon Web Services

AWS re:Invent

aws

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

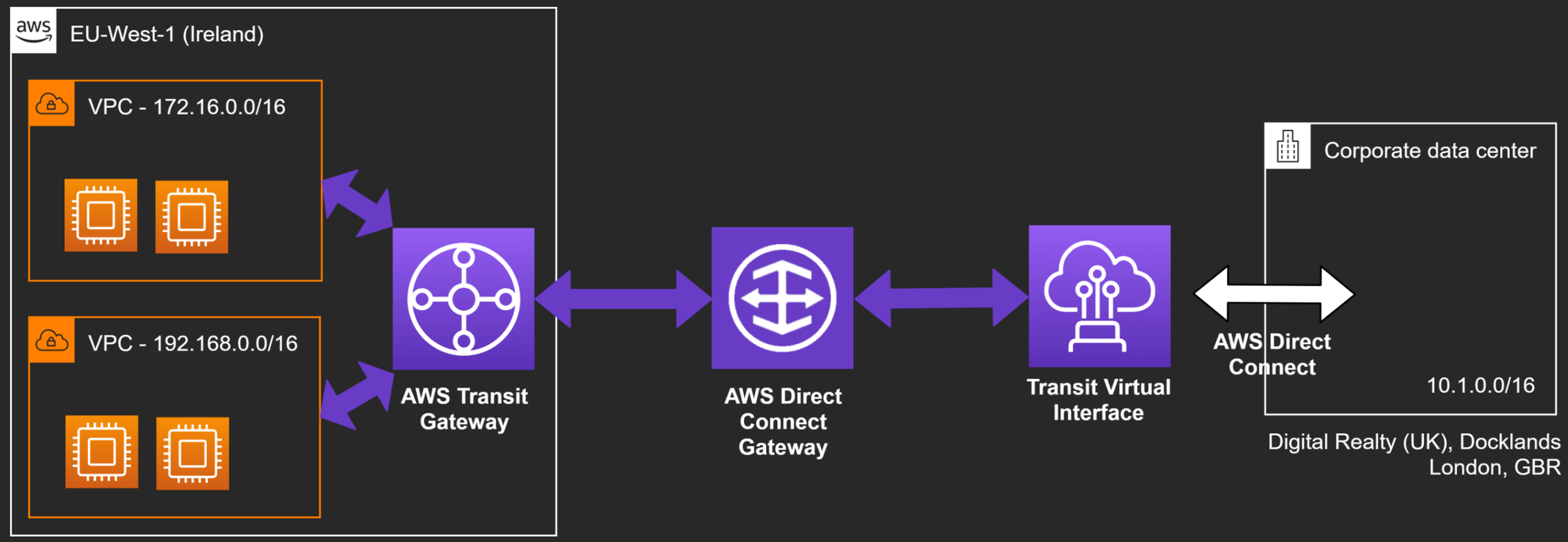
NET406 AWS Transit Gateway reference architectures for many VPCs

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

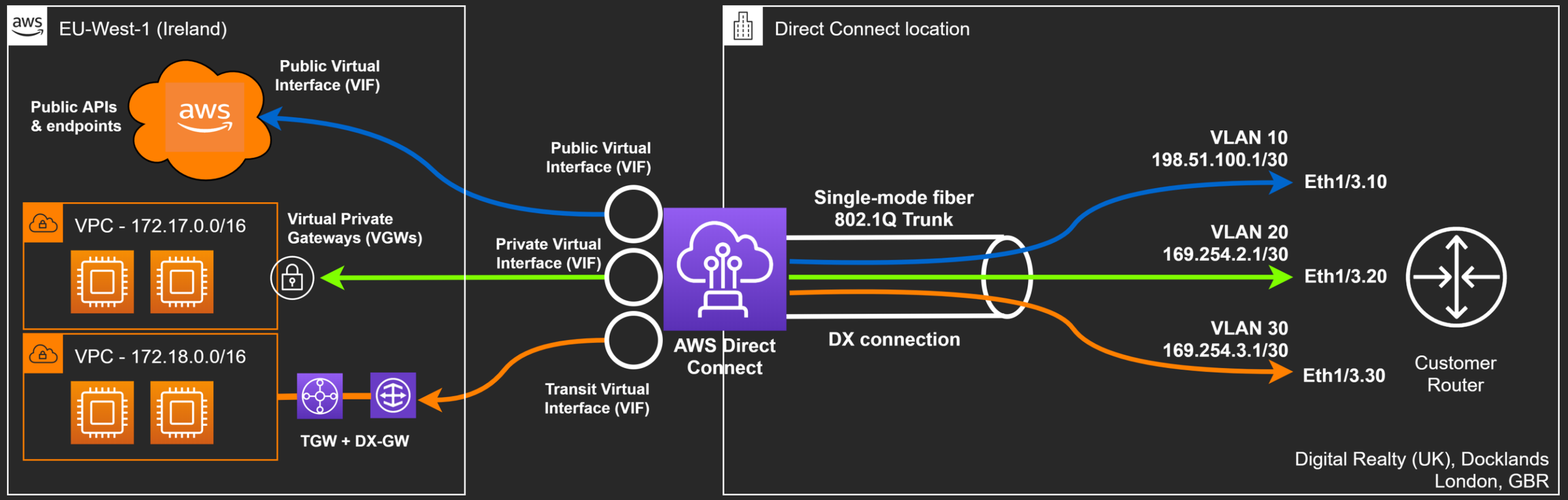
Amazon VPC

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

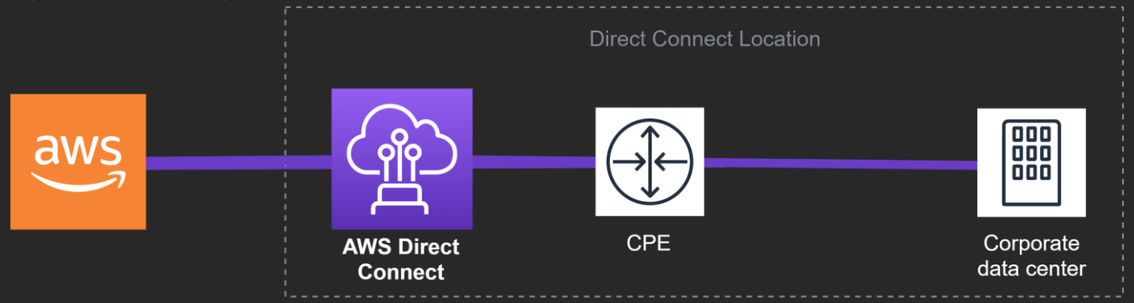
Your datacenter, office, or colocation environment

Direct Connect – Virtual Interfaces

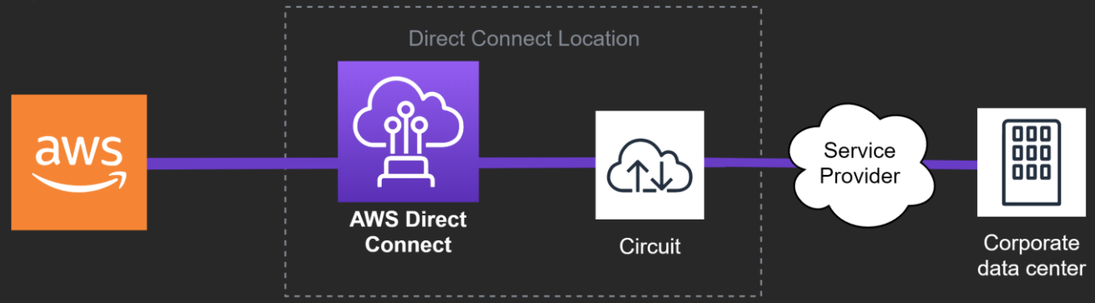


Direct Connect options

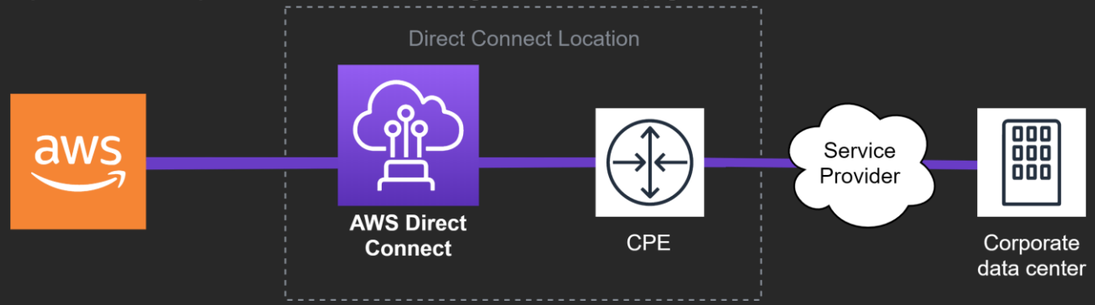
Option 1: Customer presence in the same DX location

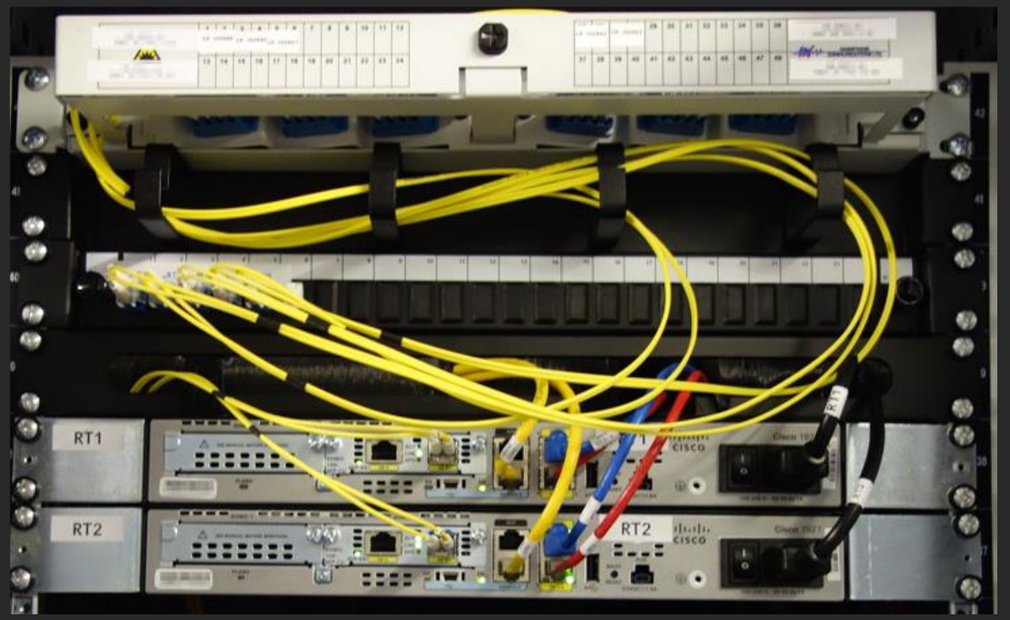


Option 2: Circuit between customer data center and DX location



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





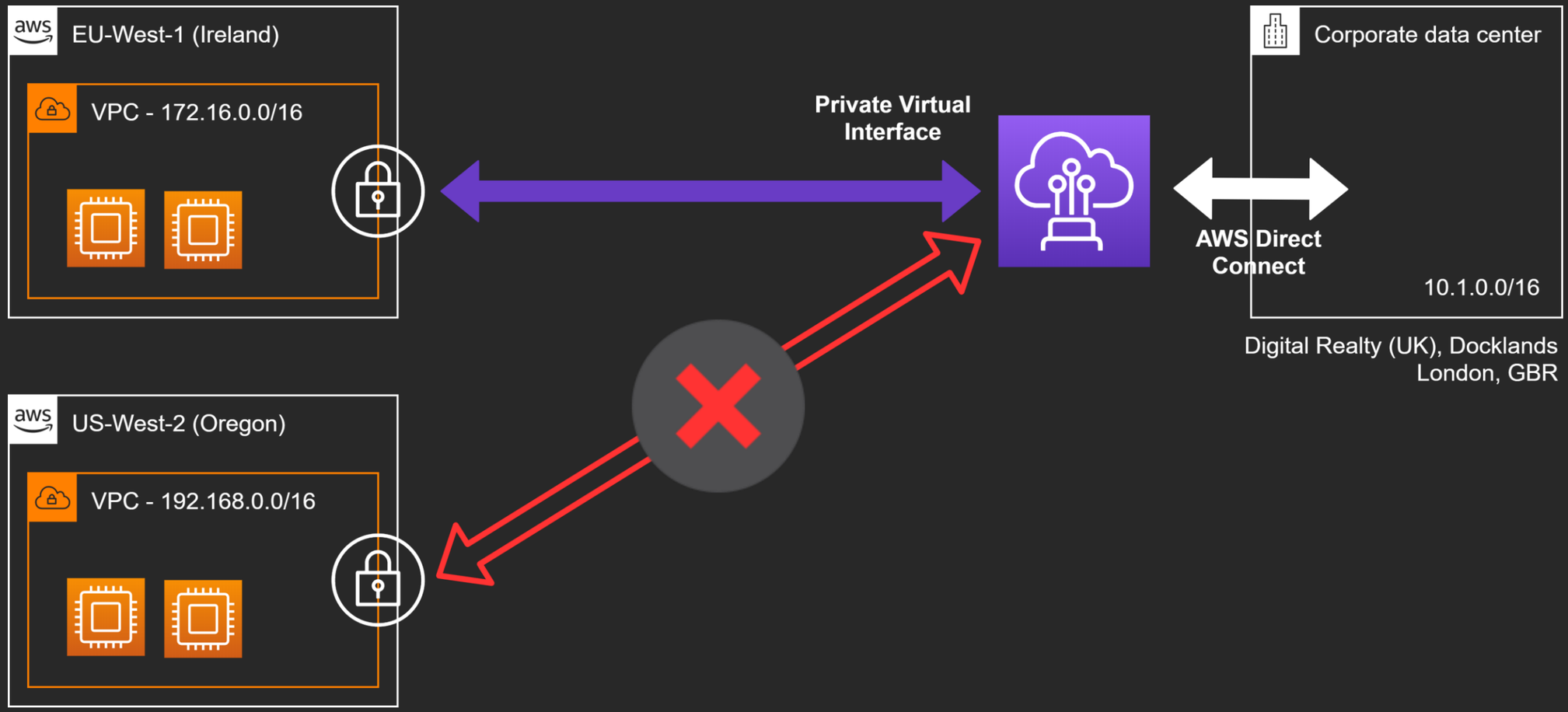
Direct Connect options and AWS Transit Gateway

	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

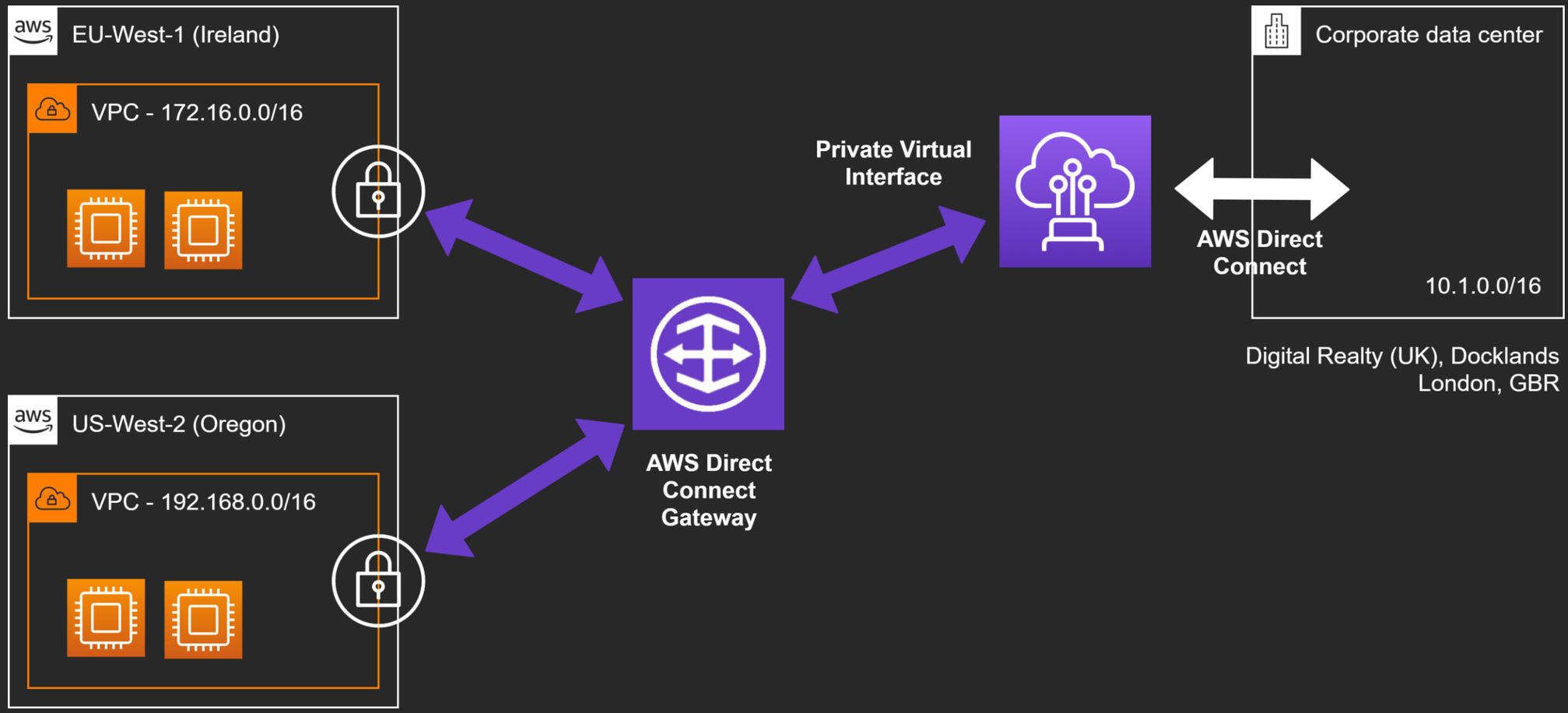
Partner offering

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

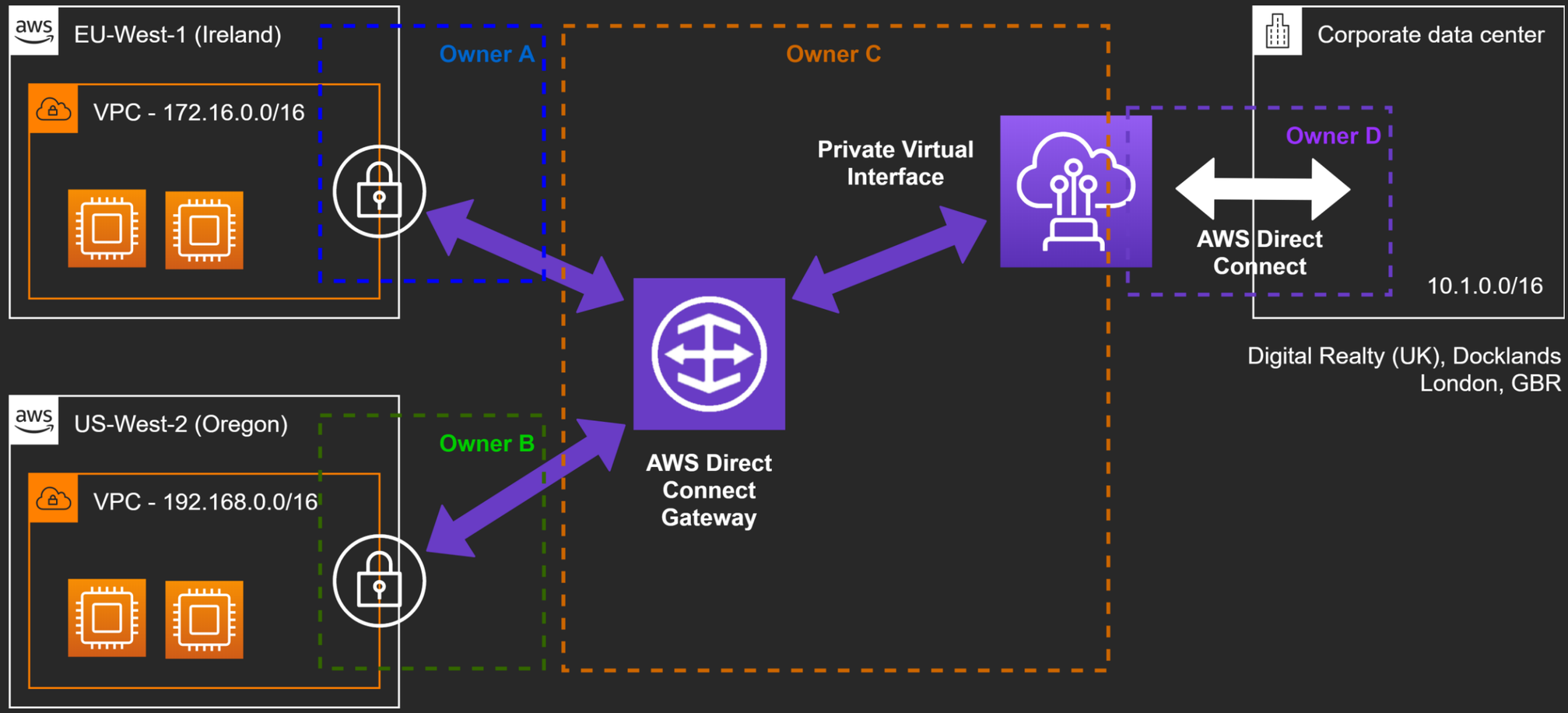
AWS Direct Connect with associated region



AWS Direct Connect Gateway



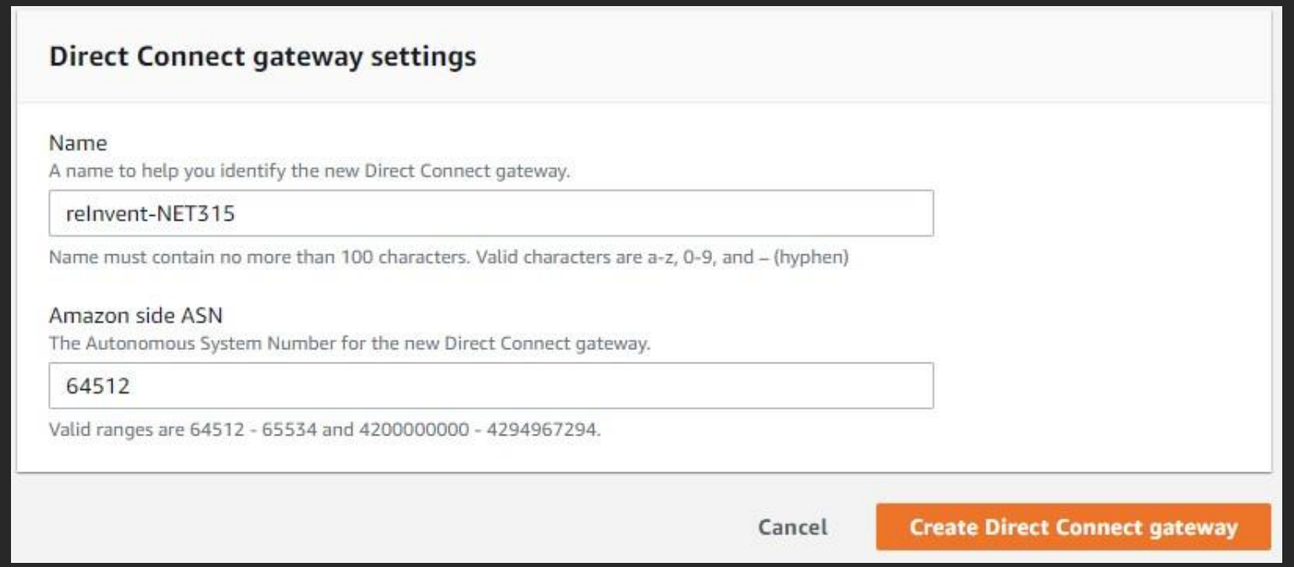
AWS Direct Connect Gateway Account Ownership



Step 1

Create DX Gateway

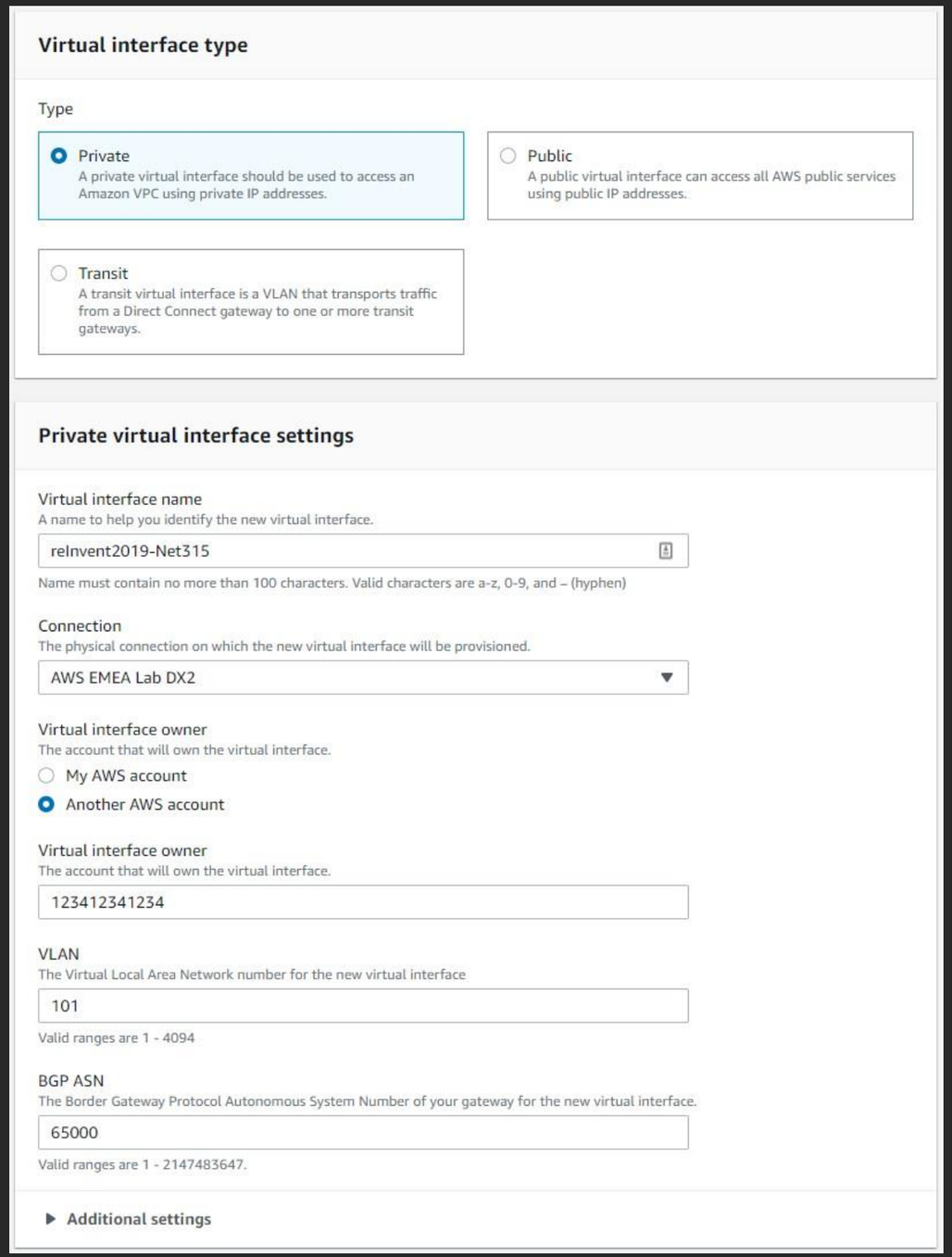
- From account “C” (DX-GW owner)
- Specify BGP ASN of DX Gateway



Step 2

Create Private VIF

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



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 0xGfOWuAvl1bHvFb3Udl2XeC
   network 0.0.0.0
exit
```

Step 2

Create Private VIF

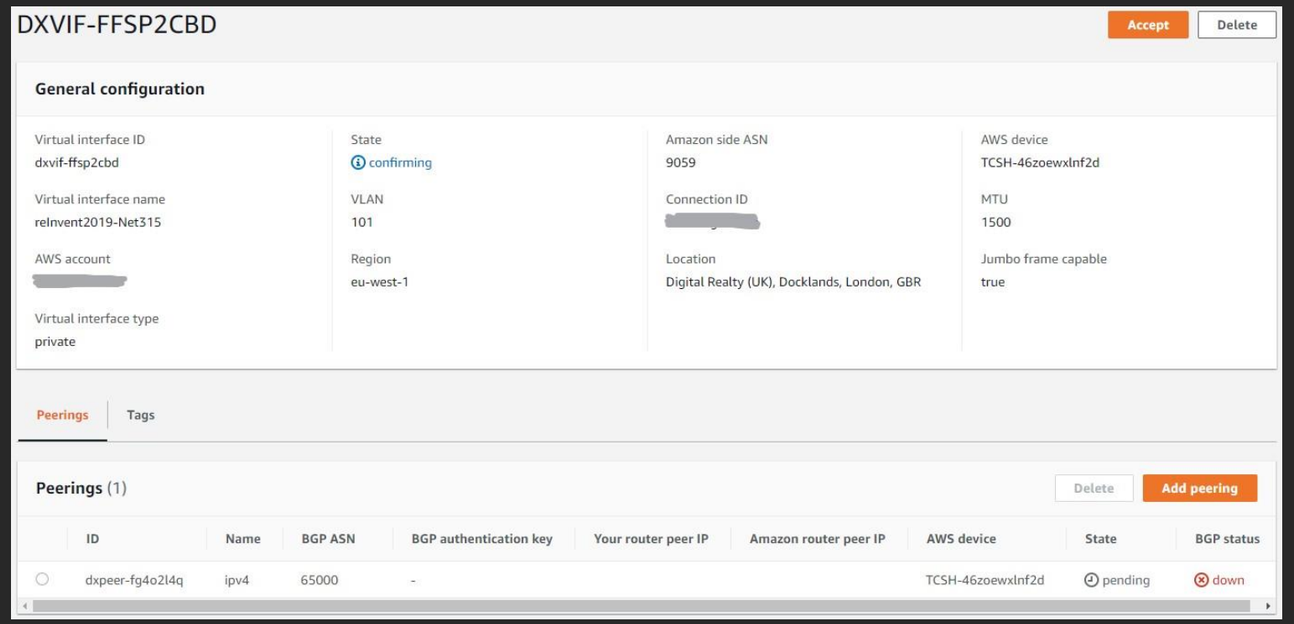
- From account “D” (DX-CON owner)
- Place VIF into account “C”
- Specify VLAN + on-premises BGP ASN

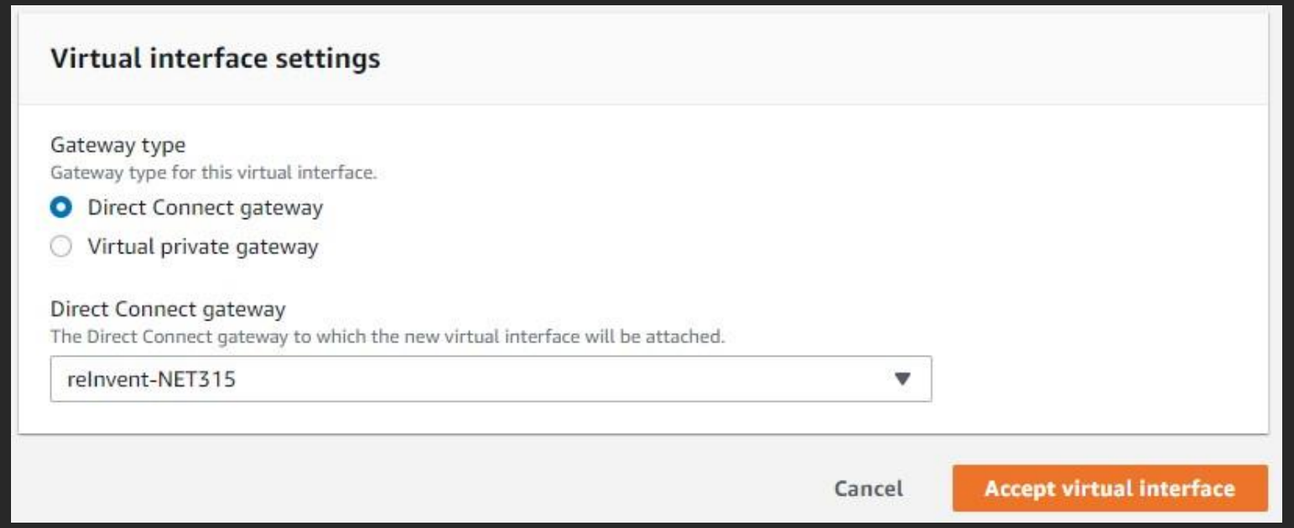
Configure Router

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

Accept Private VIF

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





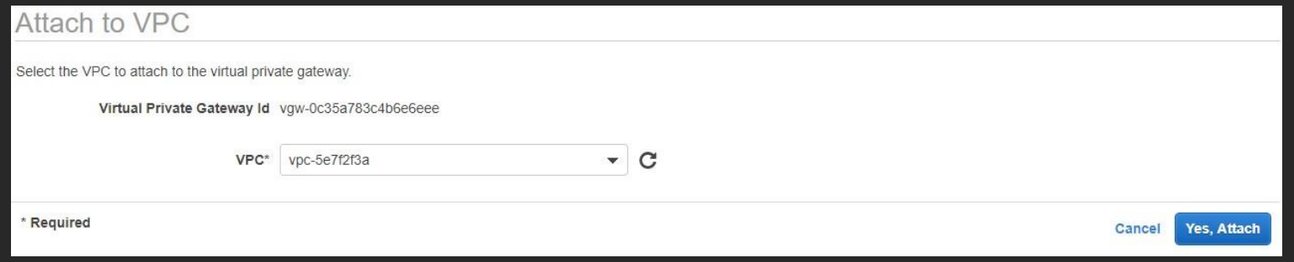
Step 3

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



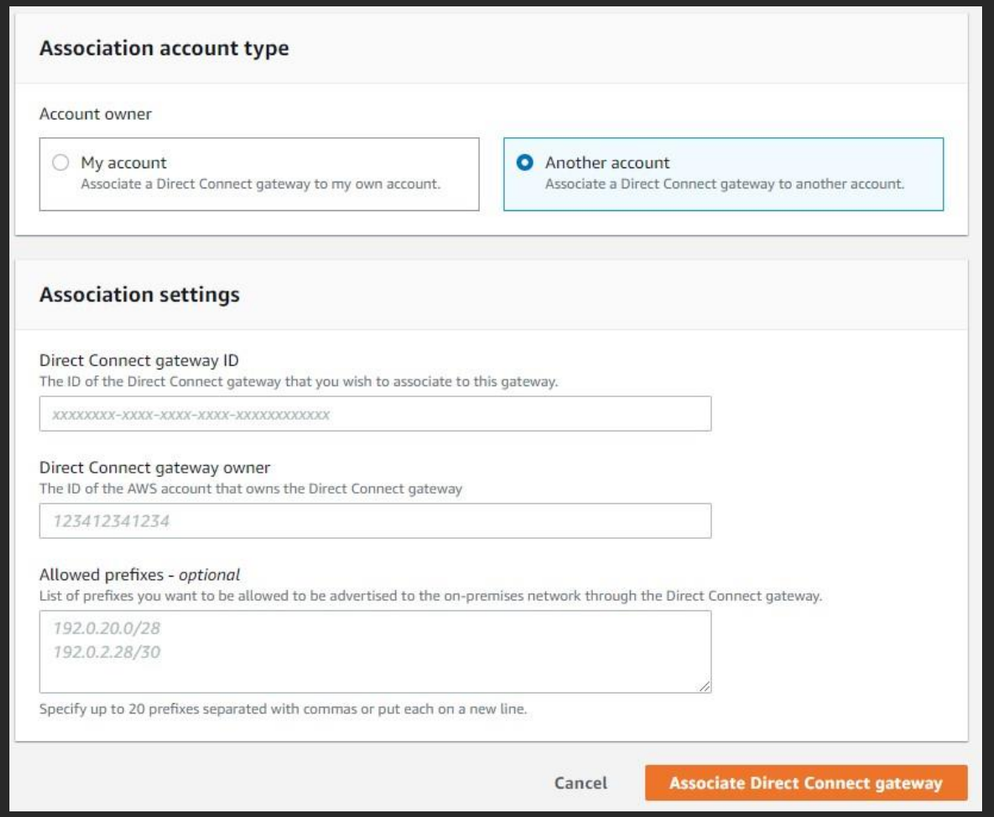
Step 4

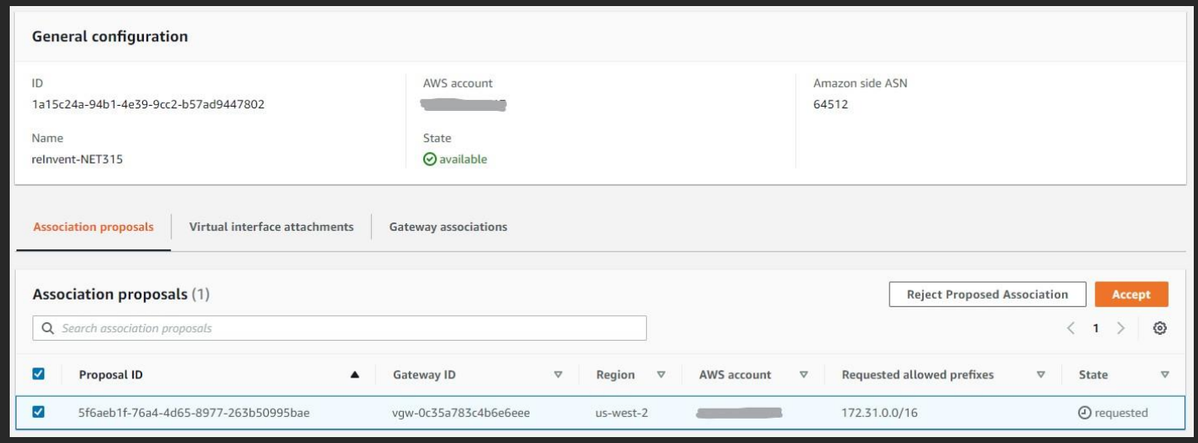
Associate VGW with DX-GW

- 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

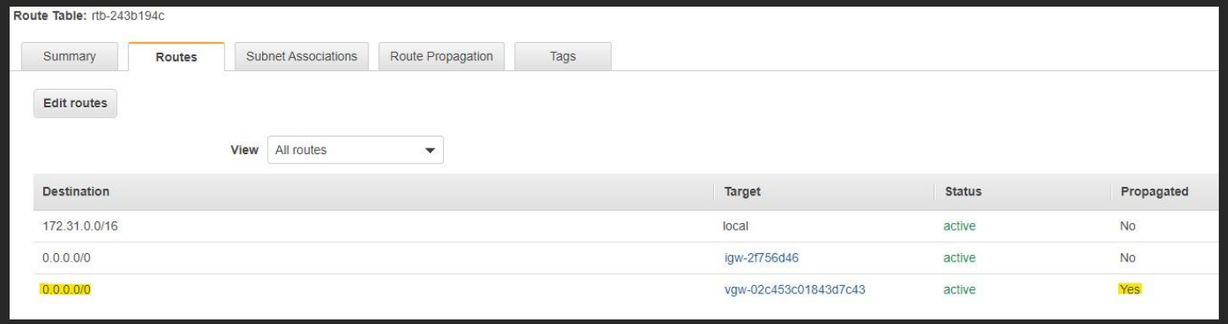




Step 5

Validate BGP routing

- VPC Route table
- On-Site router



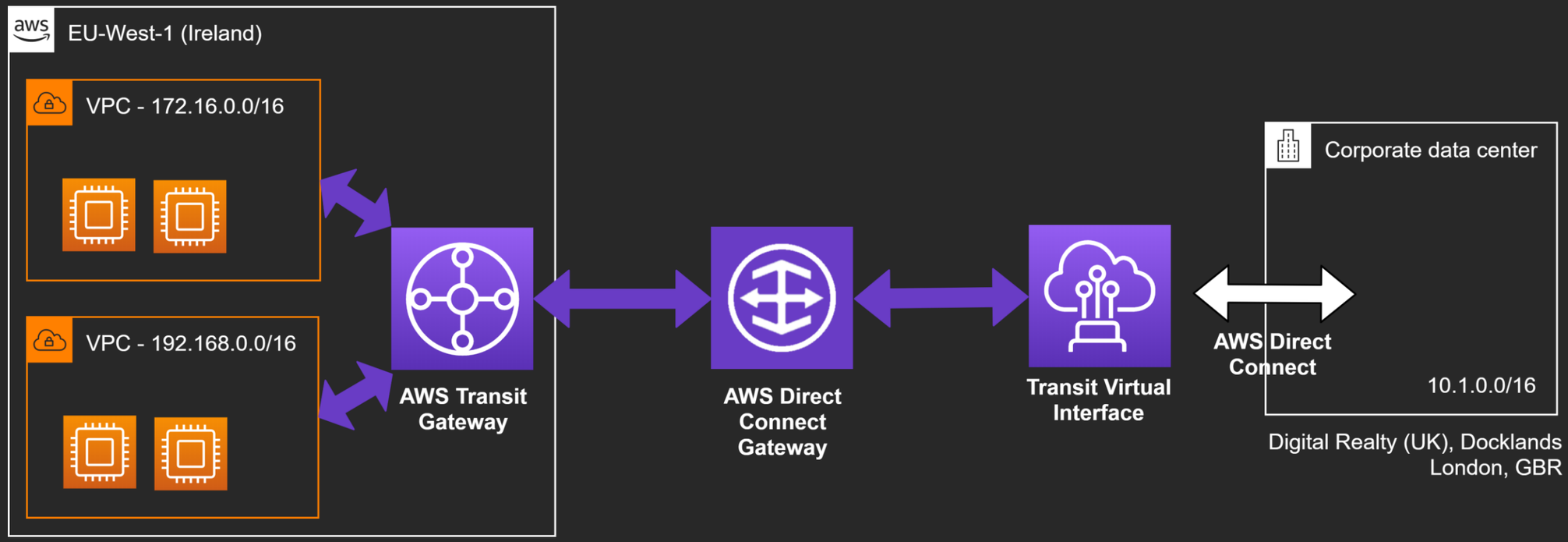

```
RT2#sh ip bgp
BGP table version is 3, local router ID is 192.168.52.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
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 64512 i
RT2#
```

Demo

Scenario 2: AWS Transit Gateway for hybrid connectivity

Hybrid connectivity with Transit Gateway



Scenario 2

Access multiple VPCs

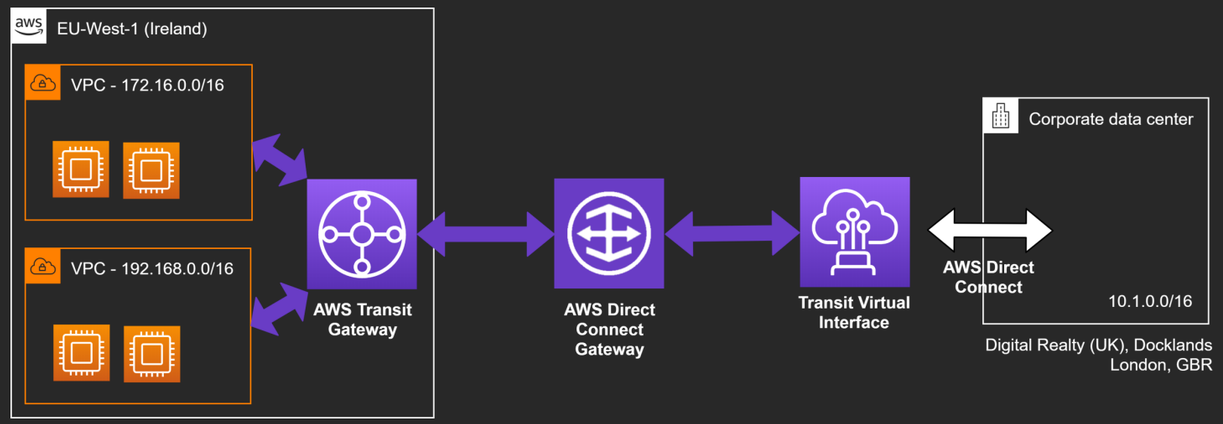
- Within same region
- Allow connectivity between VPCs and to on-premises

Direct Connect requirements

- Uses Transit VIF

Account ownership

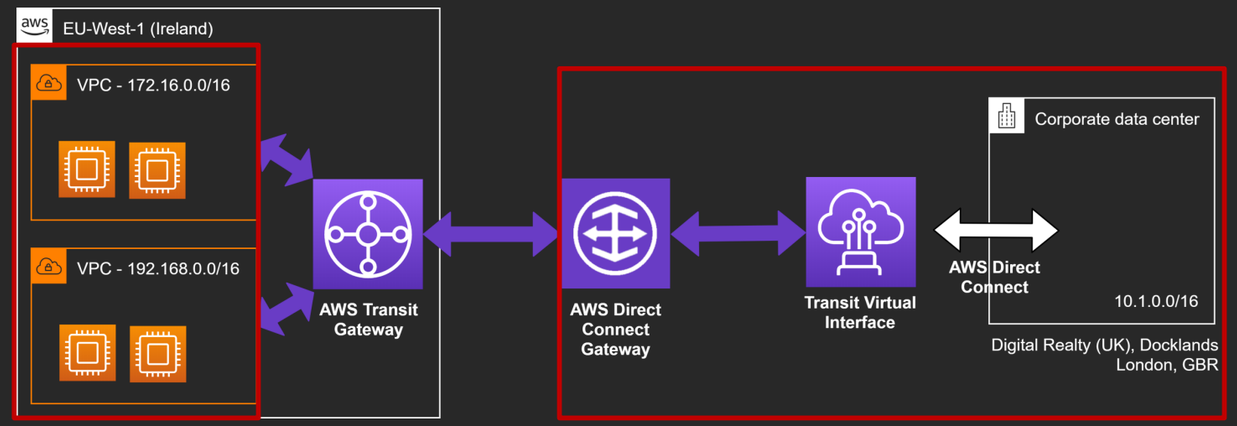
- Optional: Split across AWS accounts
- Typical:
  - Account 1: DX + DX Gateway + Transit GW
  - Account 2 – n: “Leaf” VPCs



Step 0

Prepared beforehand

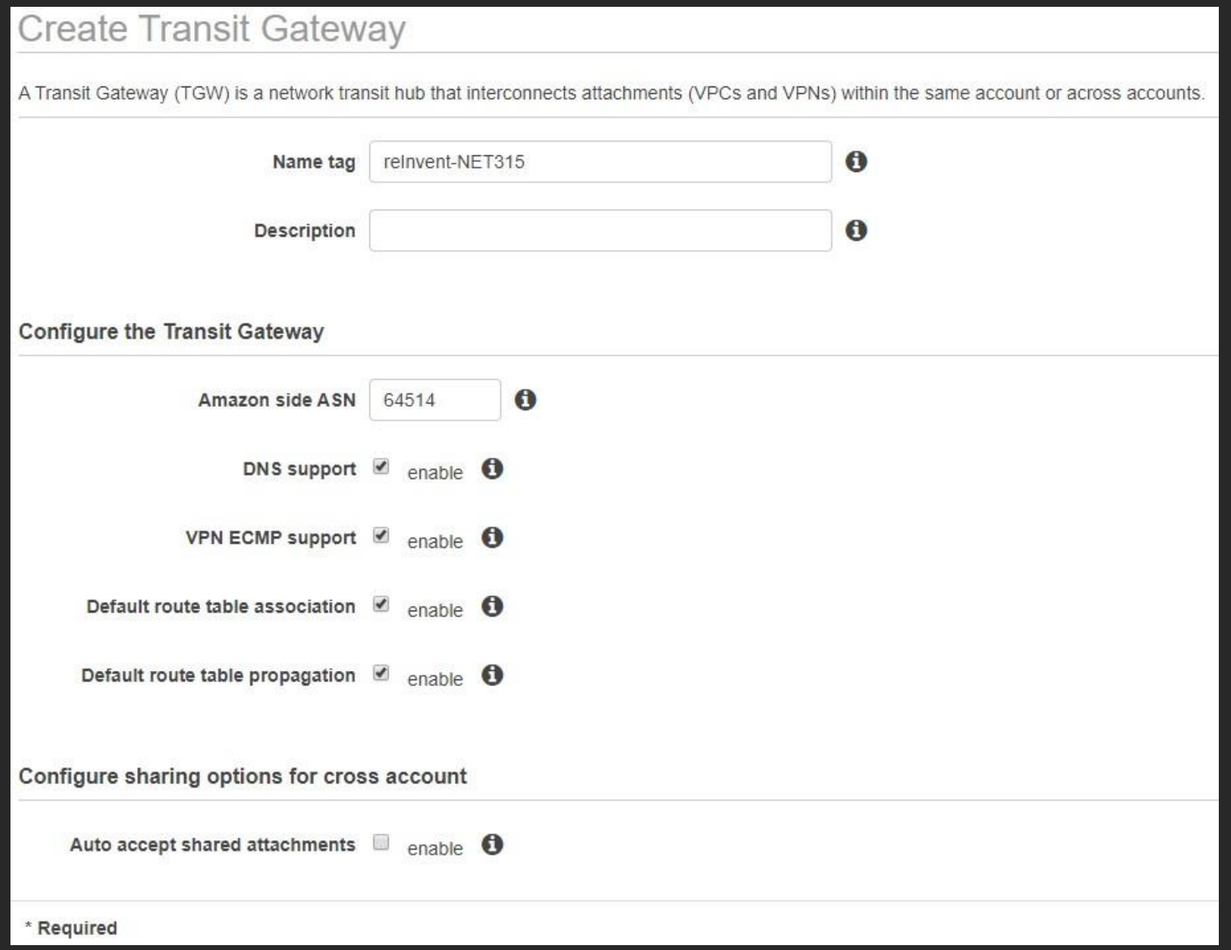
- Transit Virtual Interface
- Physical router configuration
- Direct Connect Gateway
  - Transit VIF attached



Step 1

Create Transit Gateway (TGW)

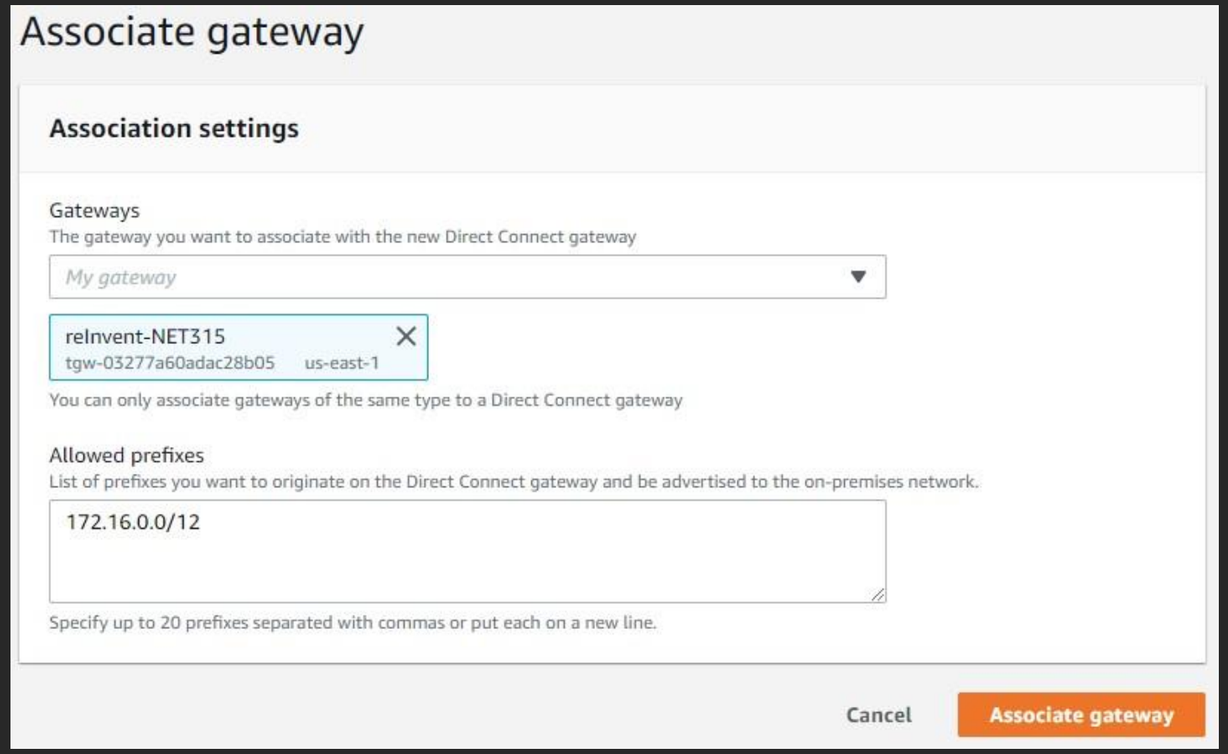
- Specify BGP ASN of Transit Gateway
  - BGP ASN cannot overlap with DX-GW
  - Use unique ASN in each AWS region
- Default route table behavior
  - Important for next use case
  - Here: Leave defaults



Step 2

Associate TGW with DX-GW

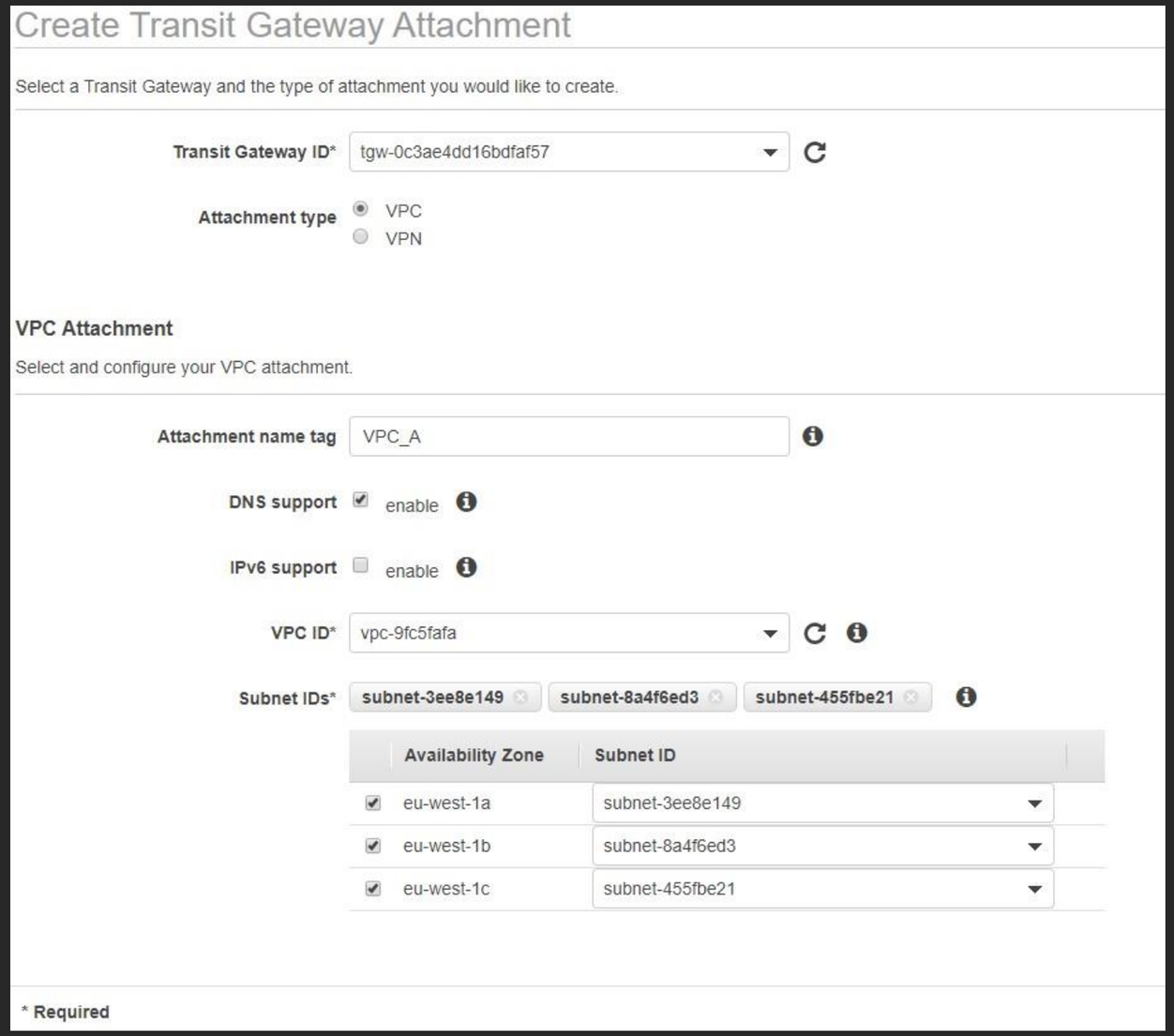
- Specify BGP prefix origination
  - Mandatory, not optional
  - Different from BGP prefix filter with DX-GW + VGW
  - Here: 172.16.0.0/12



Step 3

Attach VPC to TGW

- Select applicable subnets
  - Creates ENI in subnets
  - Determines routing within VPC (route table associated with subnet)



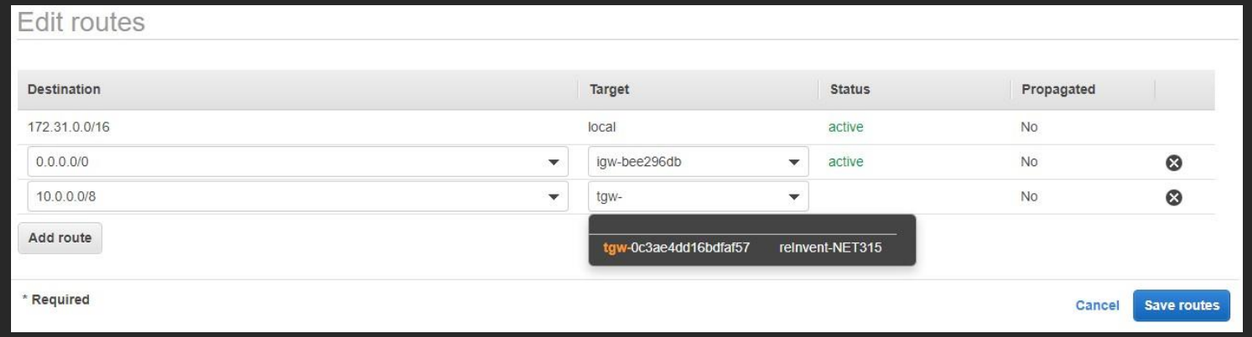
Step 3

Attach VPC to TGW

- Select applicable subnets
  - Creates ENI in subnets
  - Determines routing within VPC (route table associated with subnet)

Update VPC route table

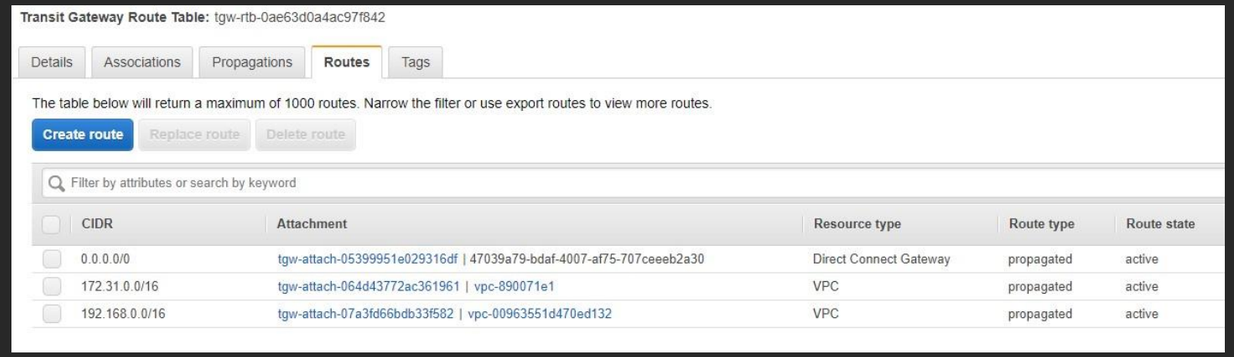
- Point desired CIDRs to TGW attachment



Step 4

Validate BGP routing

- TGW Route table
- On-Site router




```
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#
```

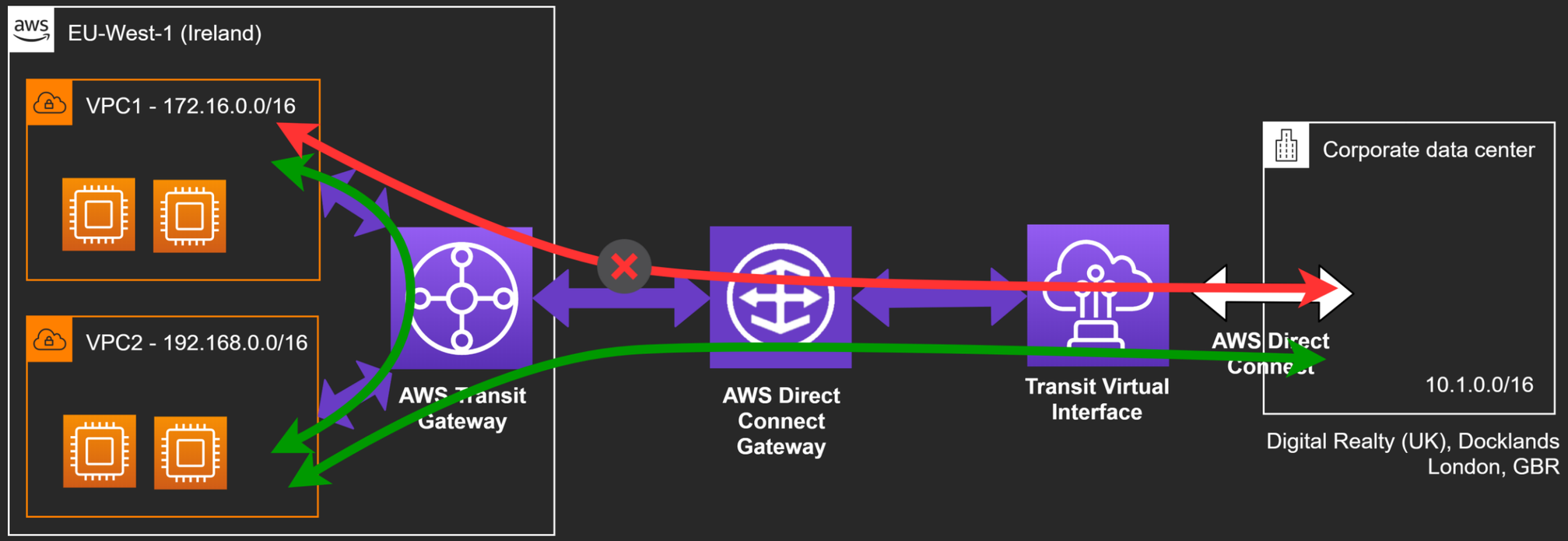
Demo

Extra Credit: Traffic isolation with Transit Gateway

AWS re:Invent

aws

VPC traffic isolation with Transit Gateway

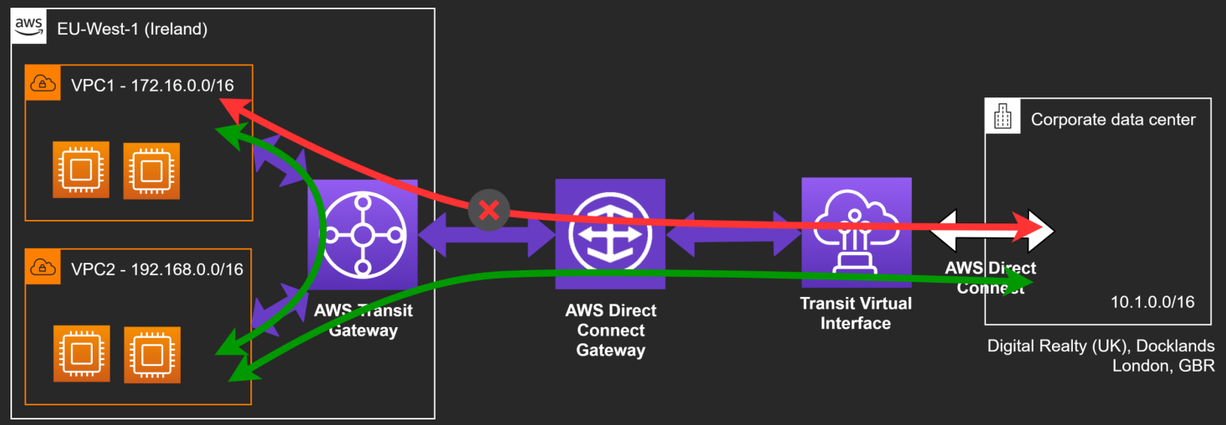


Try yourself

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

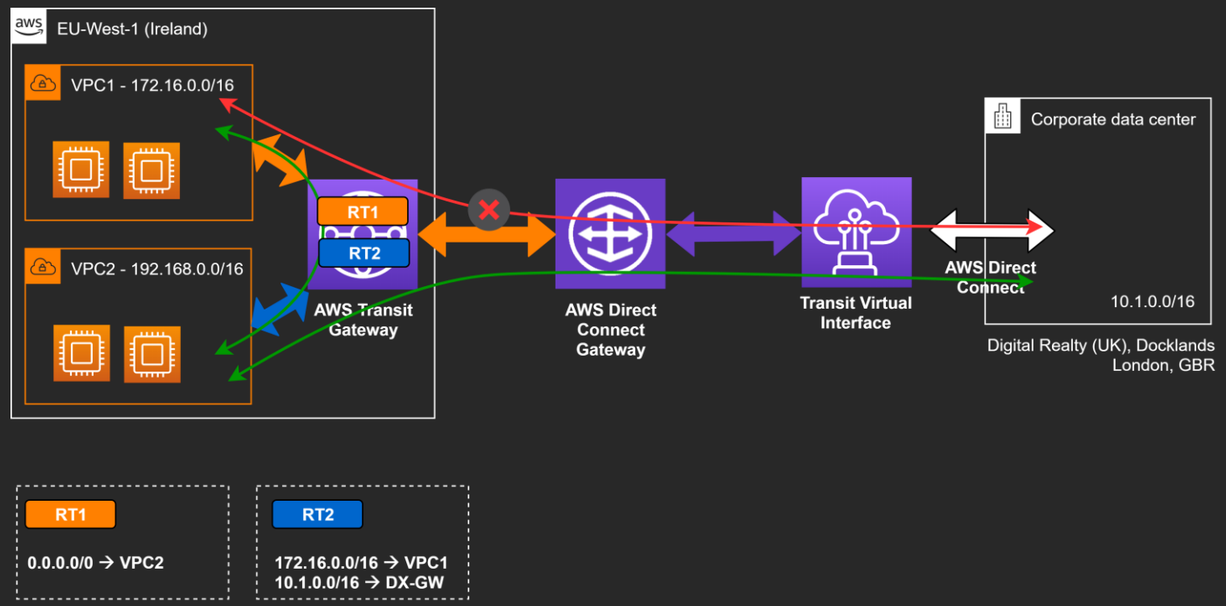
How would you accomplish this?



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

aws training and certification

Thank you!

Christian Elsen

elsenc@amazon.com

Please complete the session survey in the mobile app.