AWS re:Invent

NET405-R

Encryption options for AWS Direct Connect

Sohaib Tahir

Sr. Solutions Architect

Amazon Web Services

400 Level session

Sessions are for attendees who are deeply familiar with the topic, have implemented a solution on their own already, and are comfortable with how the technology works across multiple services, architectures, and implementations

What will you get out of this session?

- Learn different encryption approaches
- Get to know your environment for the session
- Encrypt DX connection with a particular approach

Related breakouts

NET315-R – AWS Direct Connect with AWS Transit Gateway

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

NET406-R – AWS Transit Gateway reference architectures for many VPCs

NET314-R – Use AWS Transit Gateway to interconnect multi-account VPCs

NET317-R – Connectivity to AWS and hybrid AWS network architectures

NET305-R – Advanced VPC design and new capabilities for Amazon VPC

Encrypting DX connection

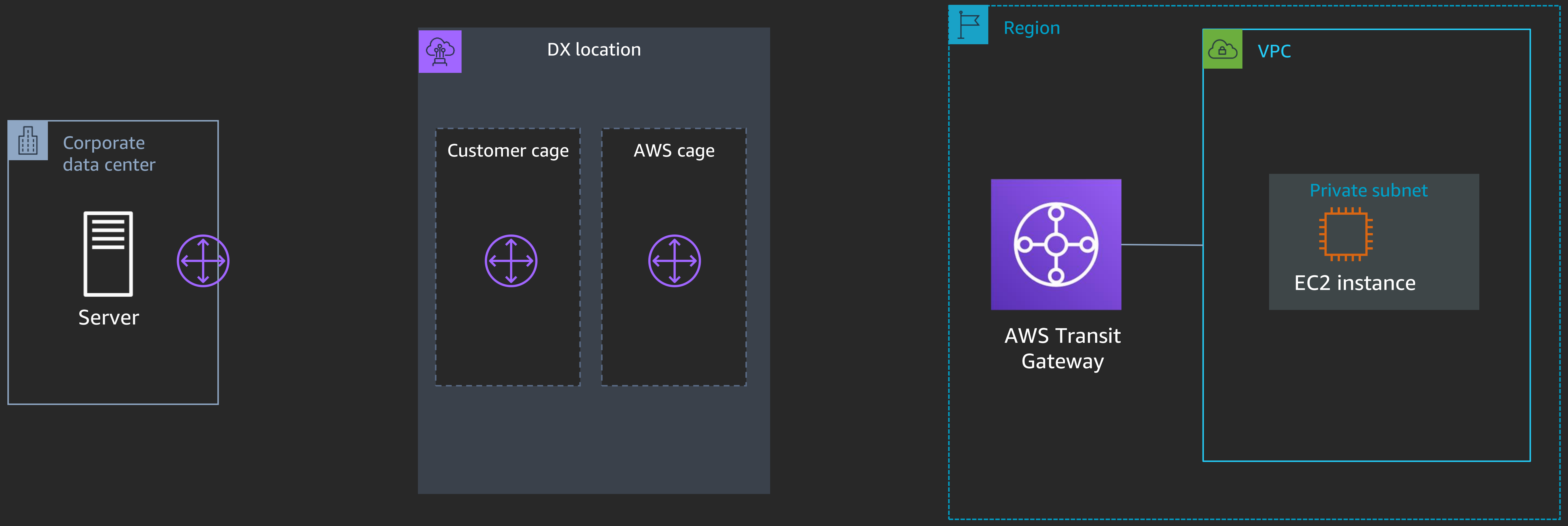
- Private VIF + application-layer TLS
- Private/Transit VIF + virtual VPN appliances (can be transit VPC)
- Private VIF + detached VGW + AWS Site-to-Site VPN (CloudHub functionality)
- Public VIF + AWS Virtual Private Gateway (BGP, IPSec tunnel, BGP)
- Public VIF + AWS Transit Gateway (BGP, IPSec tunnel, BGP) New!

Encrypting DX connection

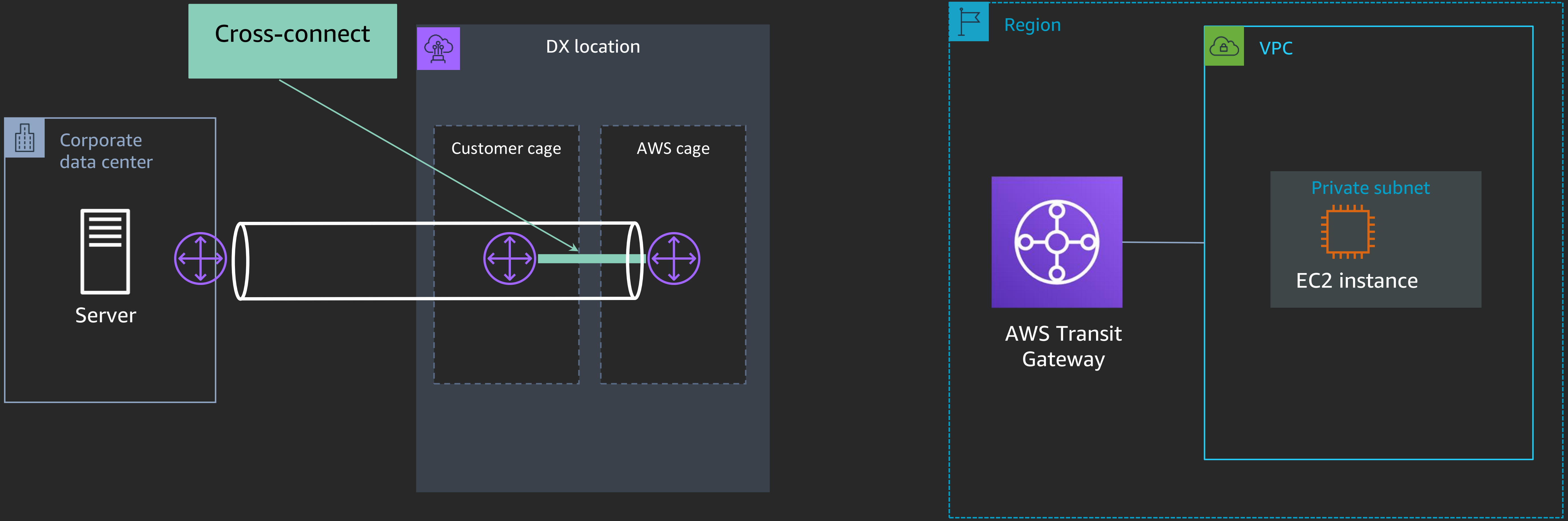
- Private VIF + application-layer TLS
- Private/Transit VIF + virtual VPN appliances (can be transit VPC)
- Private VIF + detached VGW + AWS Site-to-Site VPN (CloudHub functionality)
- Public VIF + AWS Virtual Private Gateway (BGP, IPSec tunnel, BGP)
- Public VIF + AWS Transit Gateway (BGP, IPSec tunnel, BGP) New!

Target architecture

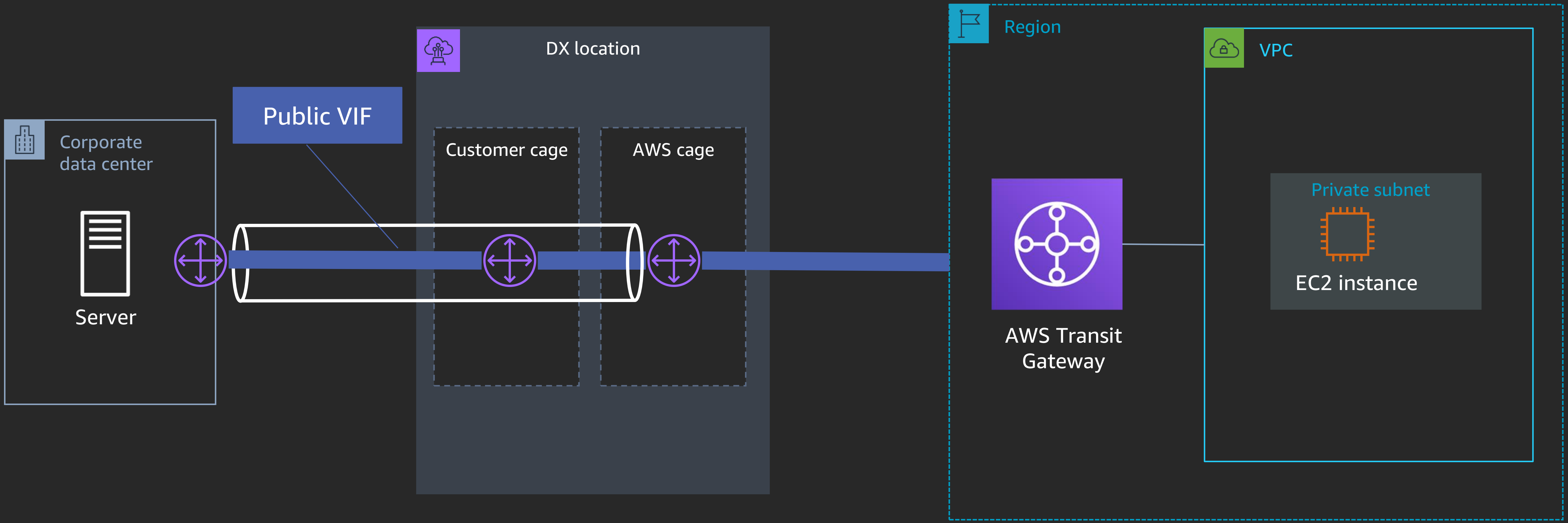
Target architecture



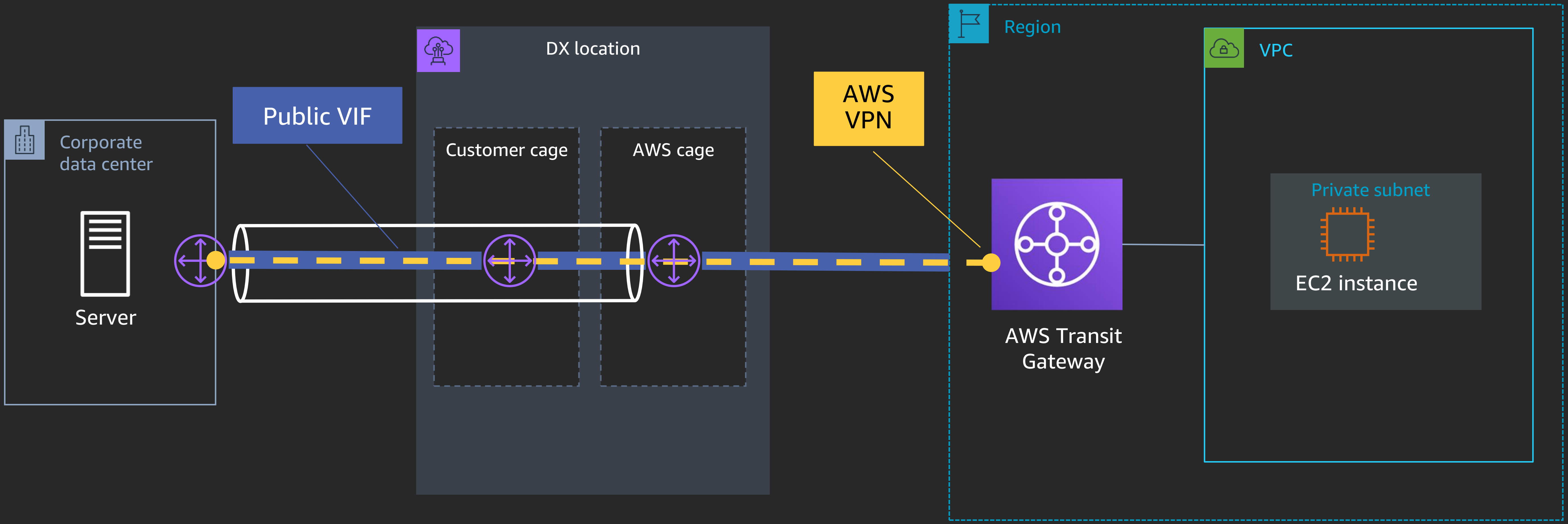
Target architecture



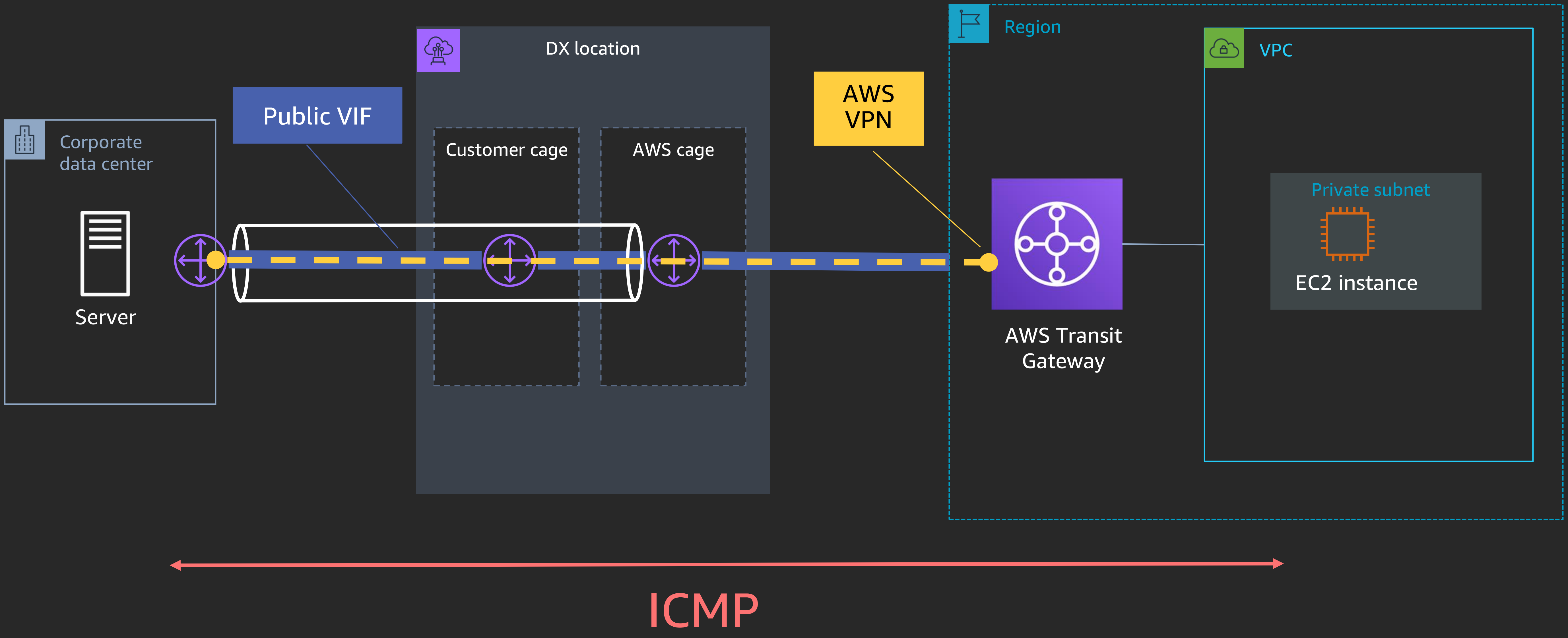
Target architecture



Target architecture

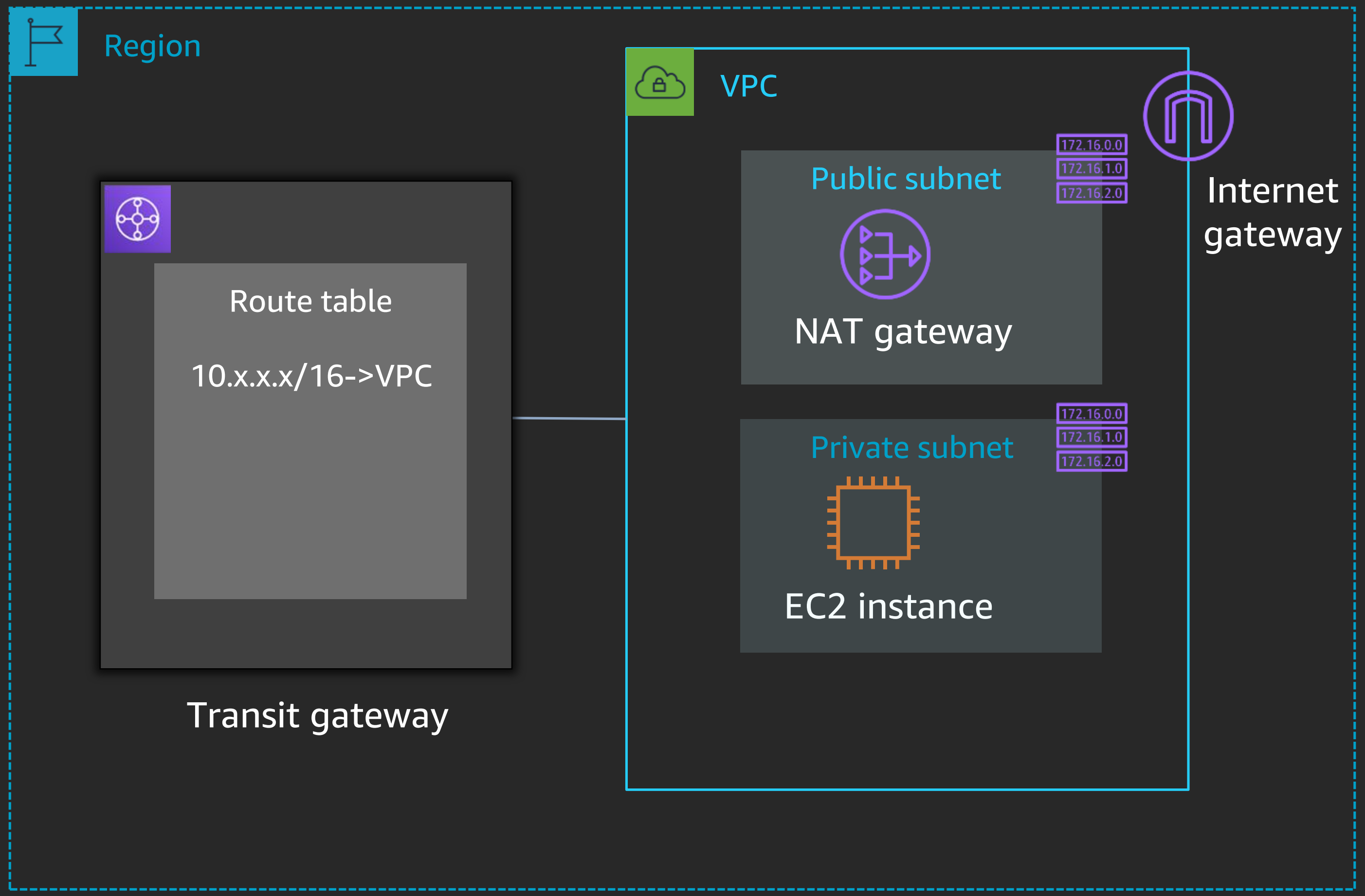


Target architecture

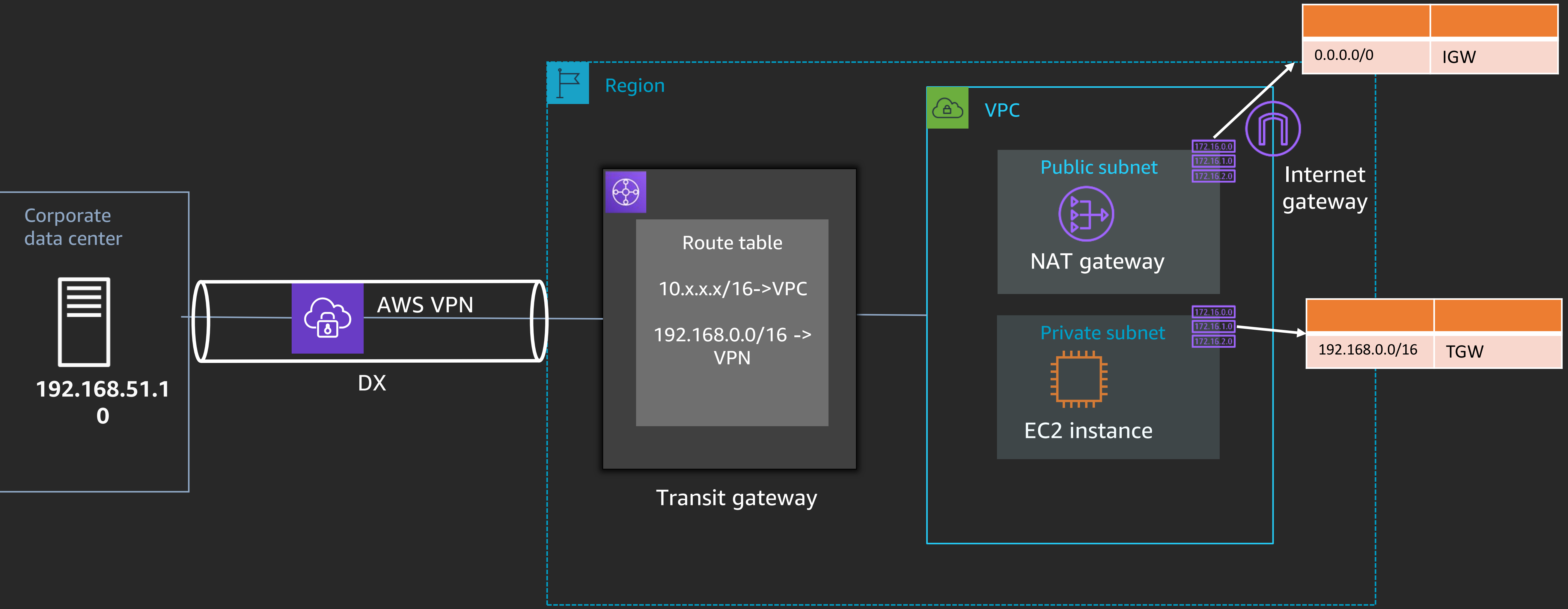


Explore AWS environment

Exploring the environment



After building VPN over DX



0.0.0.0/0	IGW

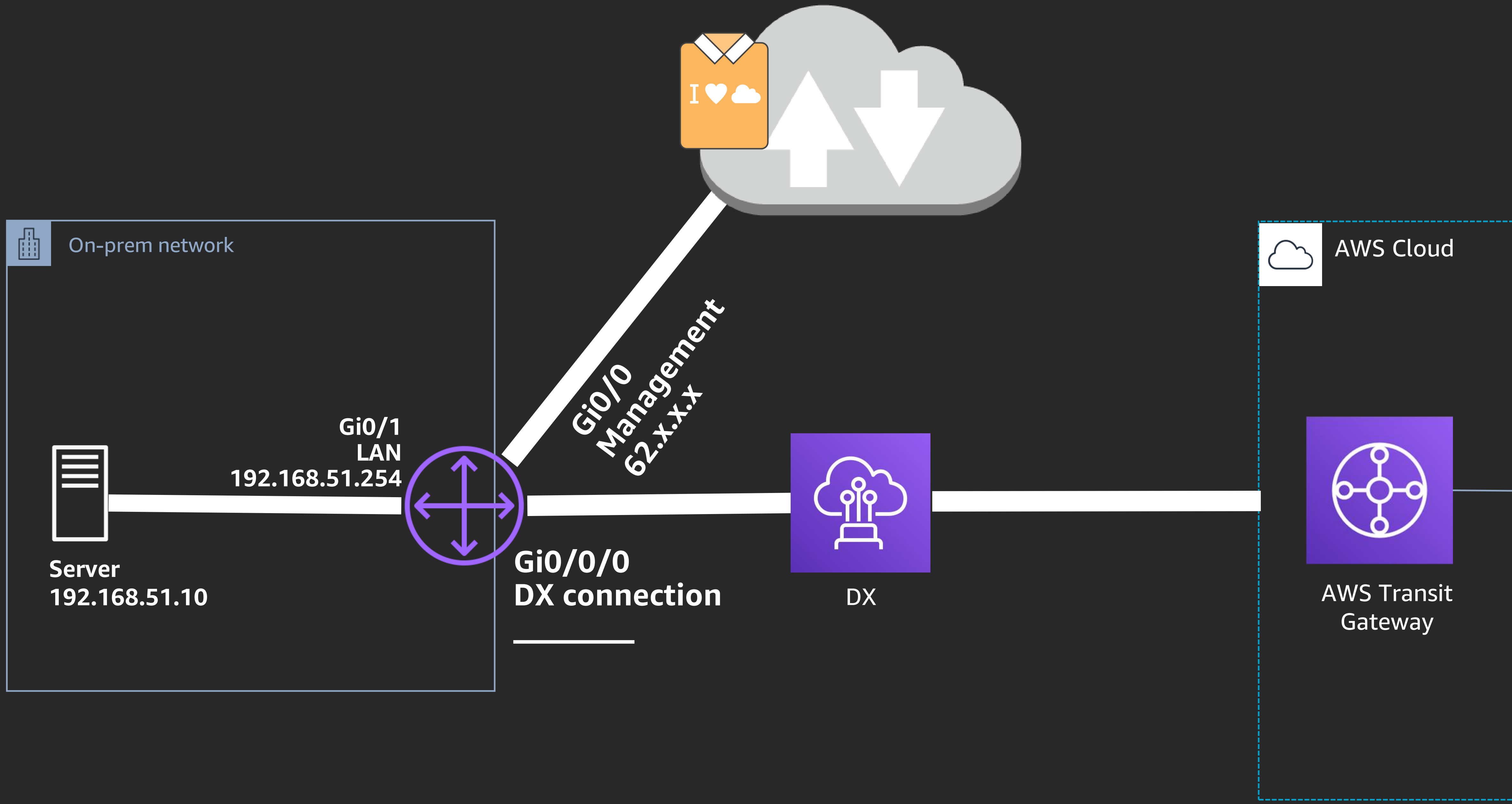
192.168.0.0/16	TGW

Explore AWS environment

Let’s take a look at the following attributes in the AWS Management Console:

- IP range of your VPC
- Routes in the transit gateway routing table
- Routes for private and public subnets
- ASN of your transit gateway

Connect to the shared router



Connect to the shared router

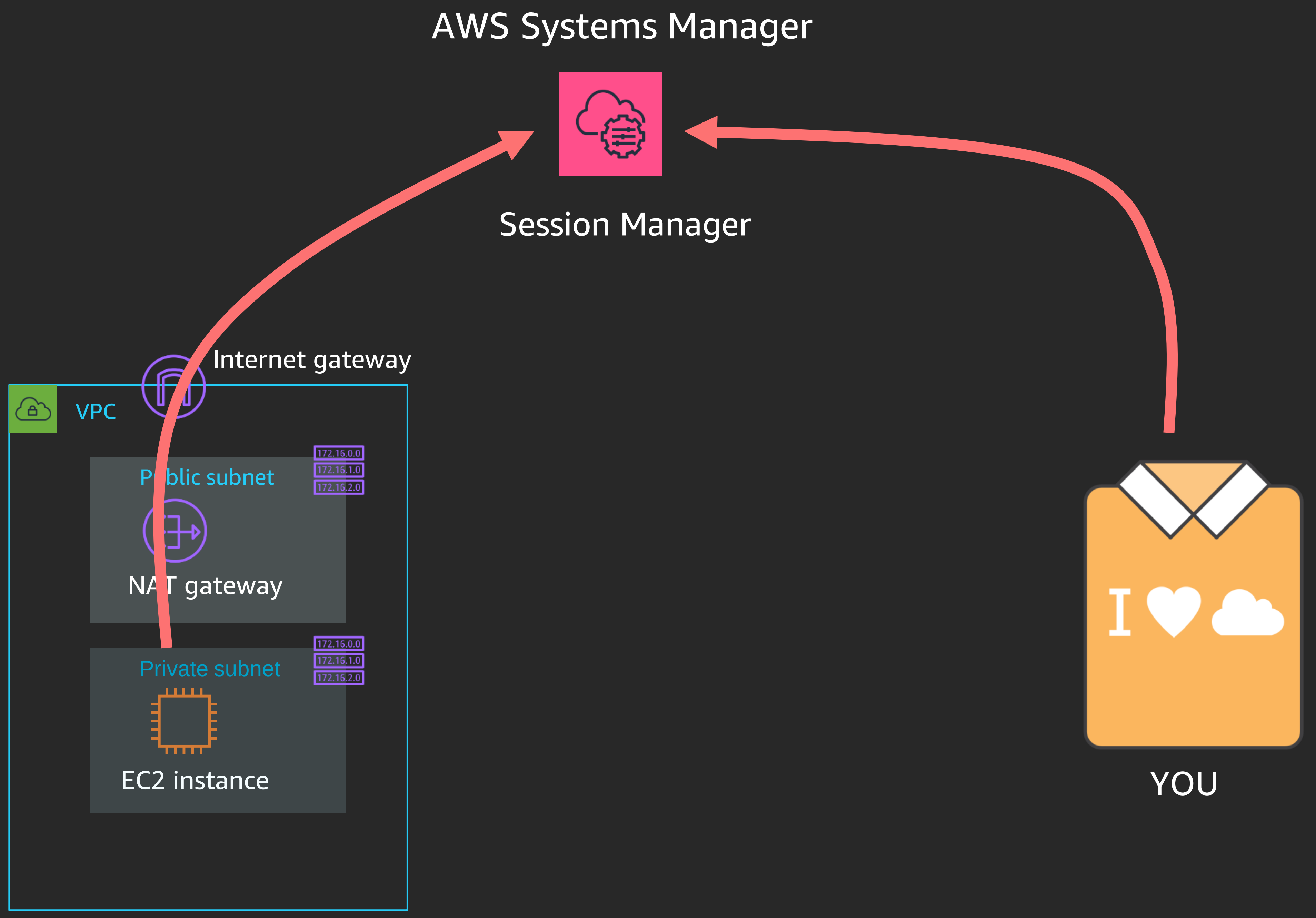
Connect to the router and inspect the configuration to find out the following:

- What’s the ID of the DX connection interface used in the interface description? (Show run/show interfaces description.)

- What routes are in the routing table? What’s each route for? (Show IP route.)

Can you “ping” a public IP address? (Ping bbc.co.uk.) Can you ping an Amazon S3 IP? (Ping s3.amazonaws.com.)

Connect to your instance



Connect to your instance

Go to Systems Manager/Sessions Manager and “Start Session” to your instance. You will need to upgrade the agent first.

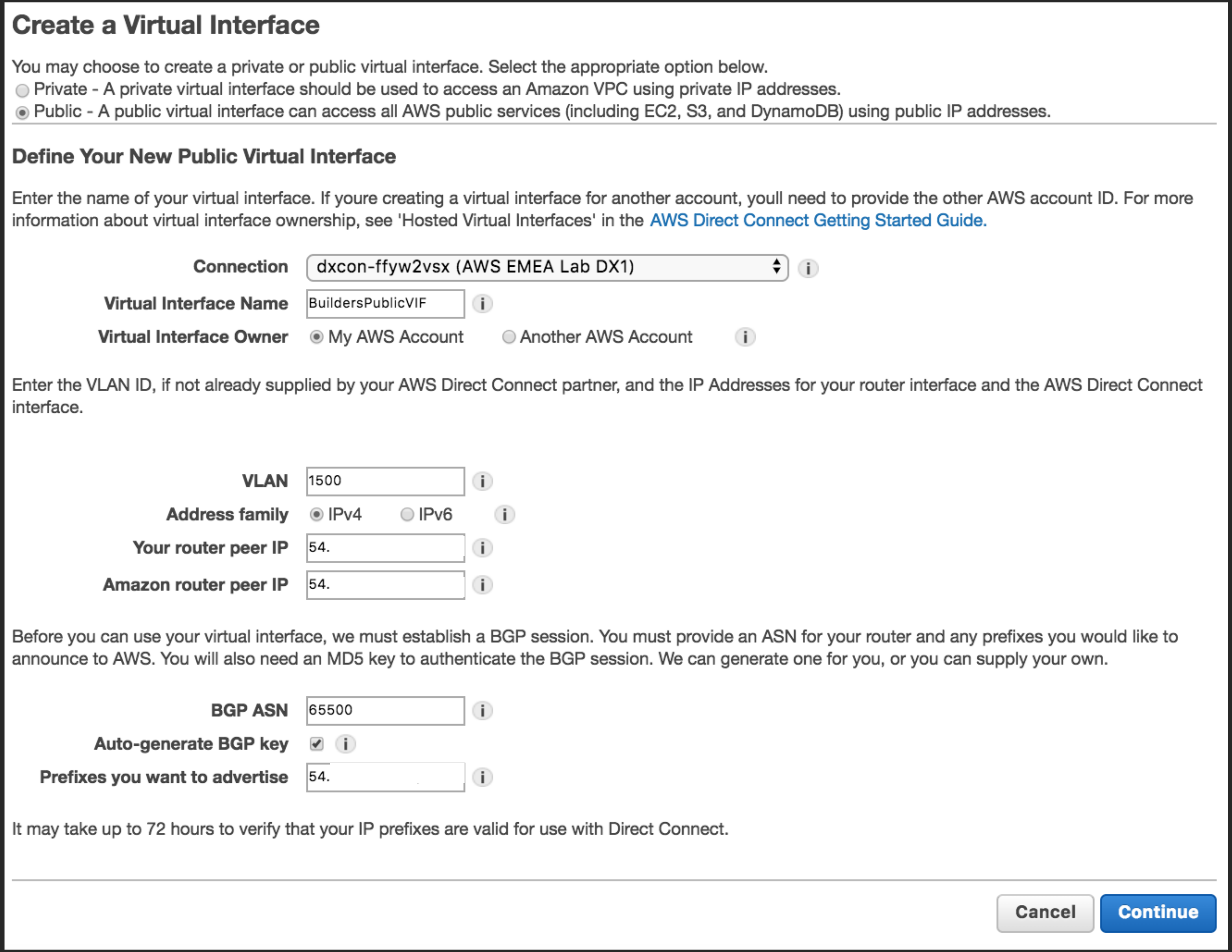
When connected, take note of the following details:

- IP address of your instance (ifconfig)
- Default gateway (IP route)

Can you ping a public IP address? (Ping bbc.co.uk).

Create a public VIF

Creating a public VIF



Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

○ 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 (including EC2, S3, and DynamoDB) using public IP addresses.

Define Your New Public Virtual Interface

Enter the name of your virtual interface. If youre creating a virtual interface for another account, youll need to provide the other AWS account ID. For more information about virtual interface ownership, see 'Hosted Virtual Interfaces' in the AWS Direct Connect Getting Started Guide.

Connection	dxcon-ffyw2vsx (AWS EMEA Lab DX1)
Virtual Interface Name	BuildersPublicVIF
Virtual Interface Owner	● My AWS Account ○ Another AWS Account

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN	1500
Address family	● IPv4 ○ IPv6
Your router peer IP	54.
Amazon router peer IP	54.

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router and any prefixes you would like to announce to AWS. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN	65500
Auto-generate BGP key	☑
Prefixes you want to advertise	54.

It may take up to 72 hours to verify that your IP prefixes are valid for use with Direct Connect.

- What account is used?
- Why do we need only a single public VIF?
- What BGP ASN is used?
- What VLAN is used?

Deploying a public VIF on router

```
interface GigabitEthernet0/0/0.1500
 description "Direct Connect to your Amazon VPC or AWS Cloud"
 encapsulation dot1Q 1500
 ip address 54.x.x.x 255.255.255.254

router bgp 65000
 address-family ipv4
  neighbor 54.x.x.x remote-as 7224
  neighbor 54.x.x.x password 0xGlvTwWD.DecFlUT4aSZvV6
  network 54.x.x.x mask 255.255.255.254
```

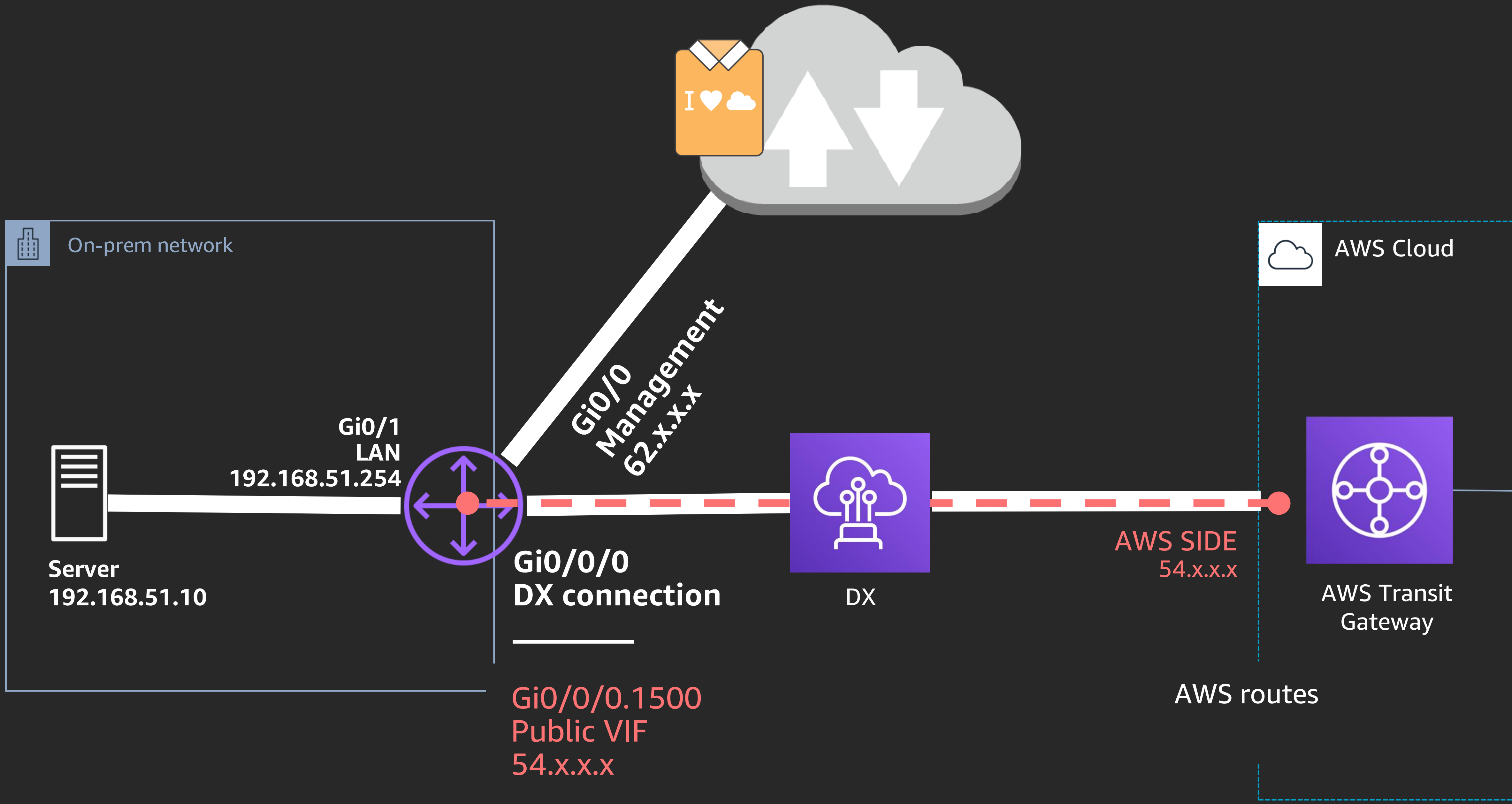
VLAN specified during public VIF creation

Public AWS IP for router DX interface

ASN specified during public VIF creation

Address range to advertise to AWS

Connect to the shared router



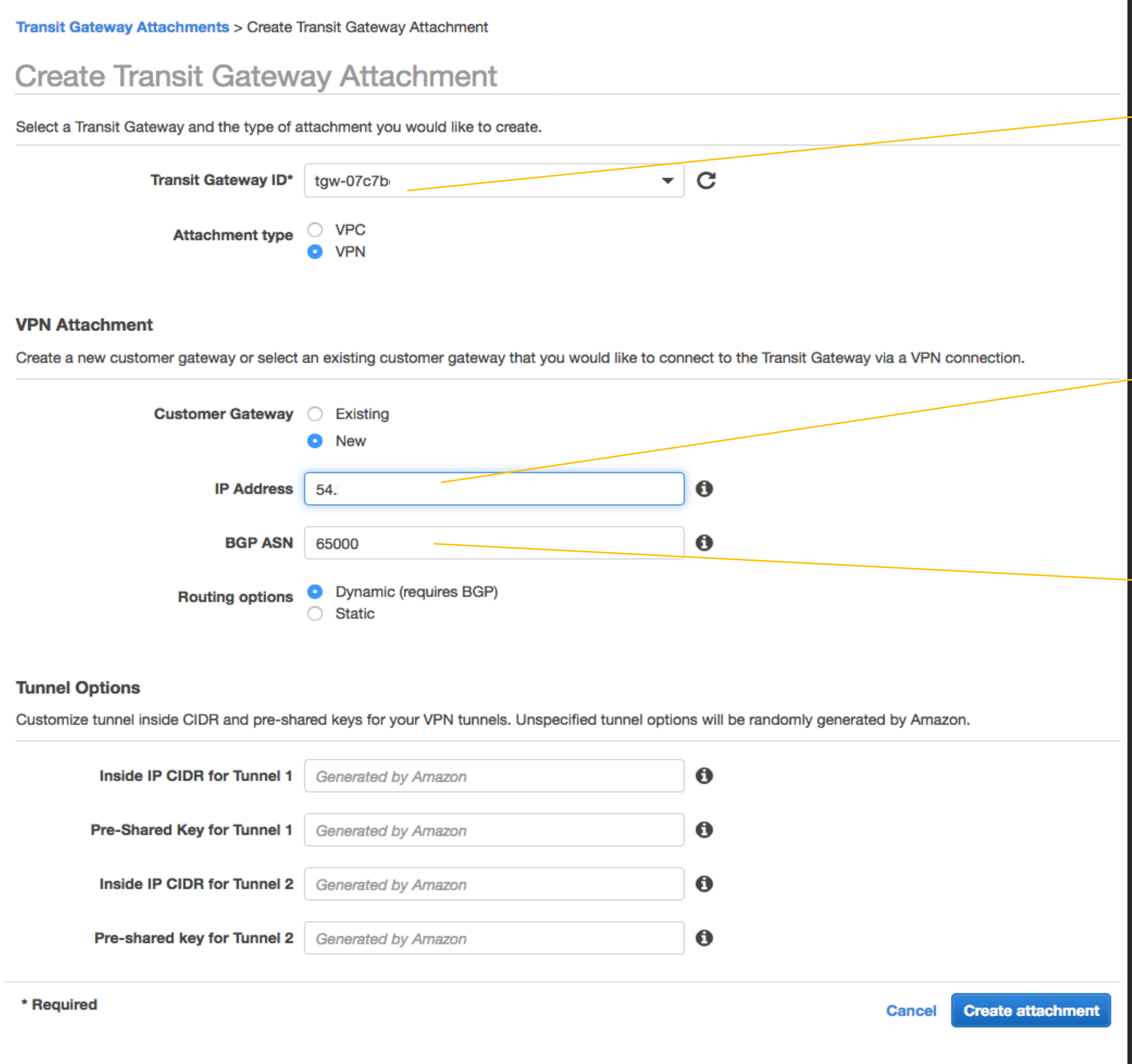
Connect to the shared router

Public VIF to AWS is now connected. What has changed?

- Connect to the router and inspect the route table. (Show IP route).
- Can you ping a public IP address? (Ping bbc.co.uk). Can you ping an Amazon S3 IP? (Ping s3.amazonaws.com).
- Check how many routes the router is receiving from AWS. (Show IP BGP summary).
- Check what routes are advertised to AWS. (Show IP BGP neighbors 54.x.x.x advertised-route).

Building site-to-site VPN

Site-to-site VPN setup: Transit gateway VPN attachment



Transit Gateway Attachments > Create Transit Gateway Attachment

Create Transit Gateway Attachment

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

Transit Gateway ID* tgw-07c7b

Attachment type ○ VPC ● VPN

VPN Attachment

Create a new customer gateway or select an existing customer gateway that you would like to connect to the Transit Gateway via a VPN connection.

Customer Gateway ○ Existing ● New

IP Address 54.

BGP ASN 65000

Routing options ● Dynamic (requires BGP) ○ Static

Tunnel Options

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IP CIDR for Tunnel 1 *Generated by Amazon*

Pre-Shared Key for Tunnel 1 *Generated by Amazon*

Inside IP CIDR for Tunnel 2 *Generated by Amazon*

Pre-shared key for Tunnel 2 *Generated by Amazon*

* Required

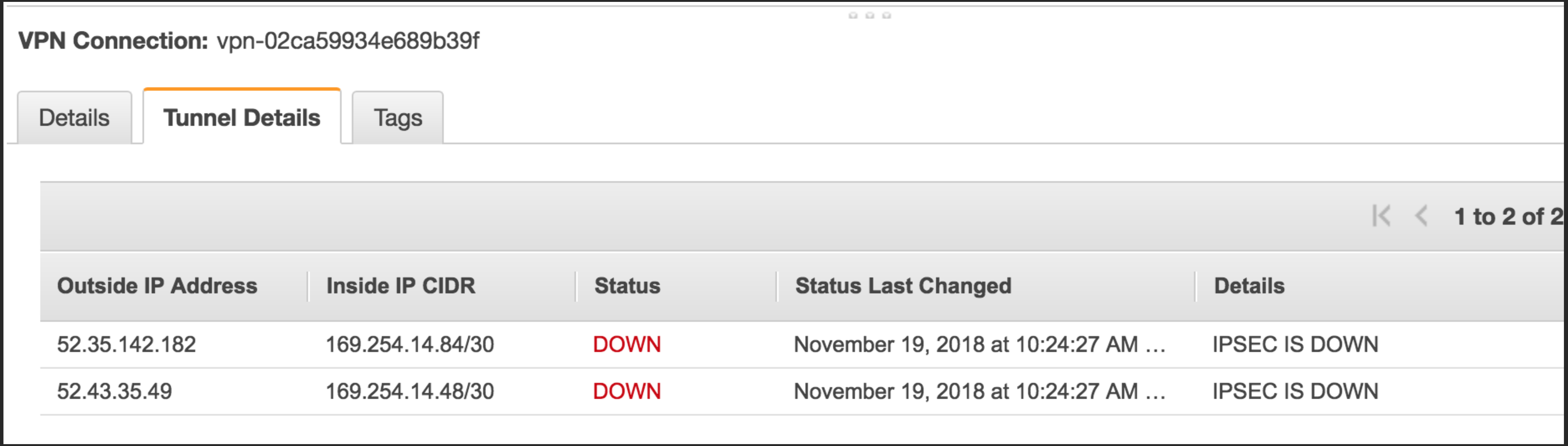
Cancel Create attachment

Select your transit gateway

DX IP address on the router

Use the ASN already defined on the router

VPN tunnel details



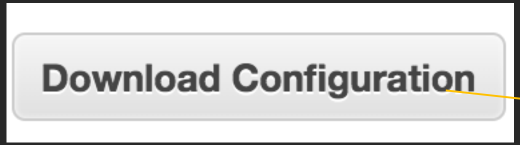
VPN Connection: vpn-02ca59934e689b39f

Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
52.35.142.182	169.254.14.84/30	DOWN	November 19, 2018 at 10:24:27 AM ...	IPSEC IS DOWN
52.43.35.49	169.254.14.48/30	DOWN	November 19, 2018 at 10:24:27 AM ...	IPSEC IS DOWN

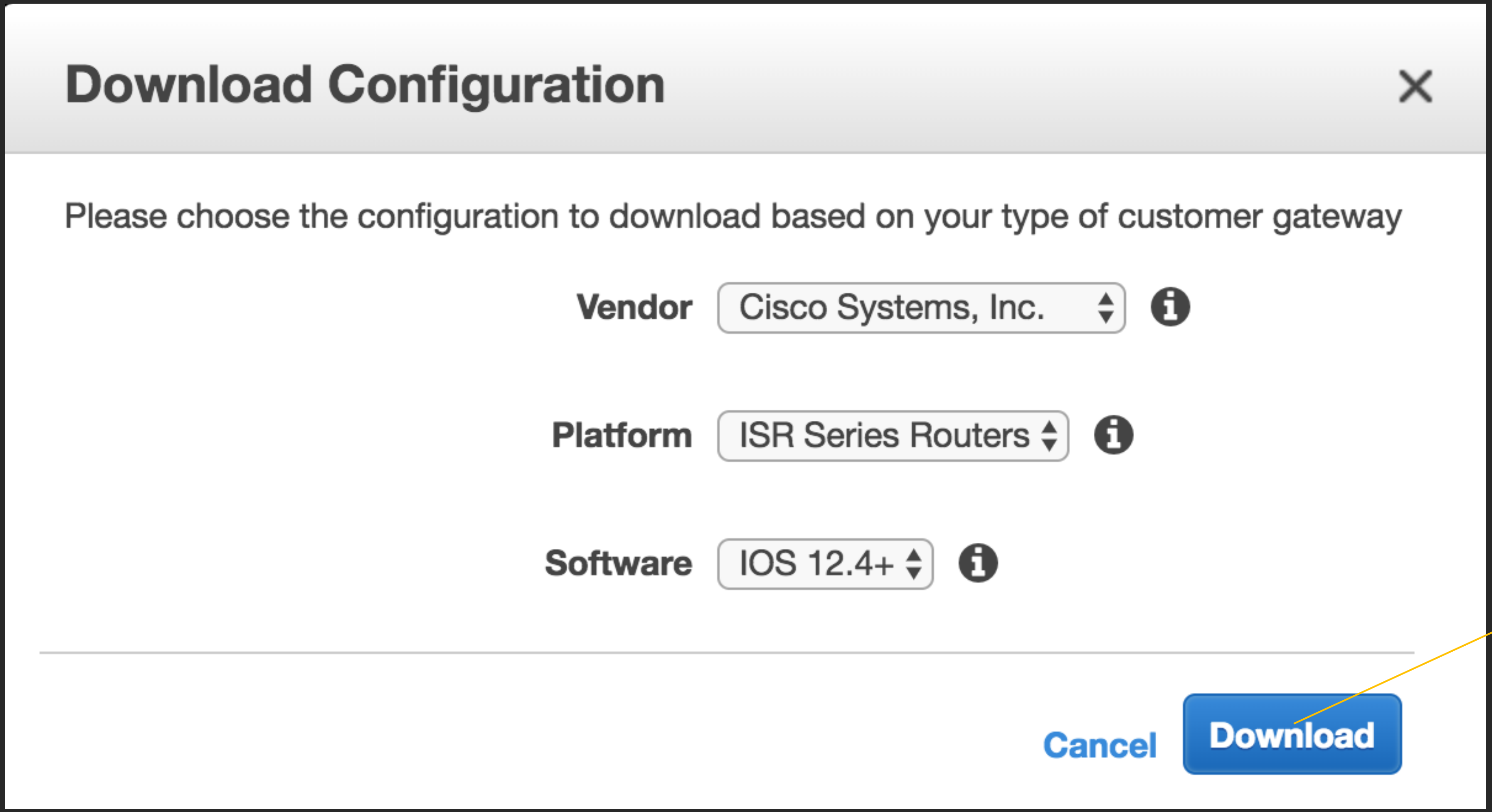
When completed, find out what public AWS outside IP addresses were used for the VPN endpoints:

- Can you see them in the router route table? (Show IP route <VPNIP>).
- Why are there two VPN IP addresses?
- Can you ping them from the router? (Ping <VPNIP>).

Site-to-site VPN setup: Configure router



When VPN is ready



Download Configuration

Please choose the configuration to download based on your type of customer gateway

Vendor: Cisco Systems, Inc.

Platform: ISR Series Routers

Software: IOS 12.4+

Fill details for your router vendor

Configure router – Update sample config (ISAKMP)

ISAKMP policy defines parameters for the initial key exchange:

```
configure terminal
crypto isakmp policy 20X
  encryption aes 128
  authentication pre-share
  group 2
  lifetime 28800
  hash sha
exit
```

First, get your router into configuration mode

Update policy number with your student ID: student1=201

Configure router – Update sample config (tunnel)

```
interface Tunnel10X
  ip address 169.254.x.x 255.255.255.252
  ip virtual-reassembly
  tunnel source 54.x.x.x
  tunnel destination 52.x.x.x
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsec-vpn-profileID
  ip tcp adjust-mss 1379
  no shutdown
```

Update tunnel ID with your student ID: student1=101

What is this IP in your setup?

What is this IP in your setup?

Configure router – Update sample config (BGP)

```
router bgp 65000
 neighbor 169.254.x.x remote-as 64512
 neighbor 169.254.x.x activate
 neighbor 169.254.x.x timers 10 30 30
 address-family ipv4 unicast
  neighbor 169.254.x.x remote-as 64512
  neighbor 169.254.x.x timers 10 30 30
  ~~neighbor 169.254.x.x default-originate~~
  neighbor 169.254.x.x activate
  neighbor 169.254.x.x soft-reconfiguration inbound
  network 192.168.51.0 mask 255.255.255.0
```

What is this ASN?

What is this IP address?

Remove line to stop advertising default route to your VPC

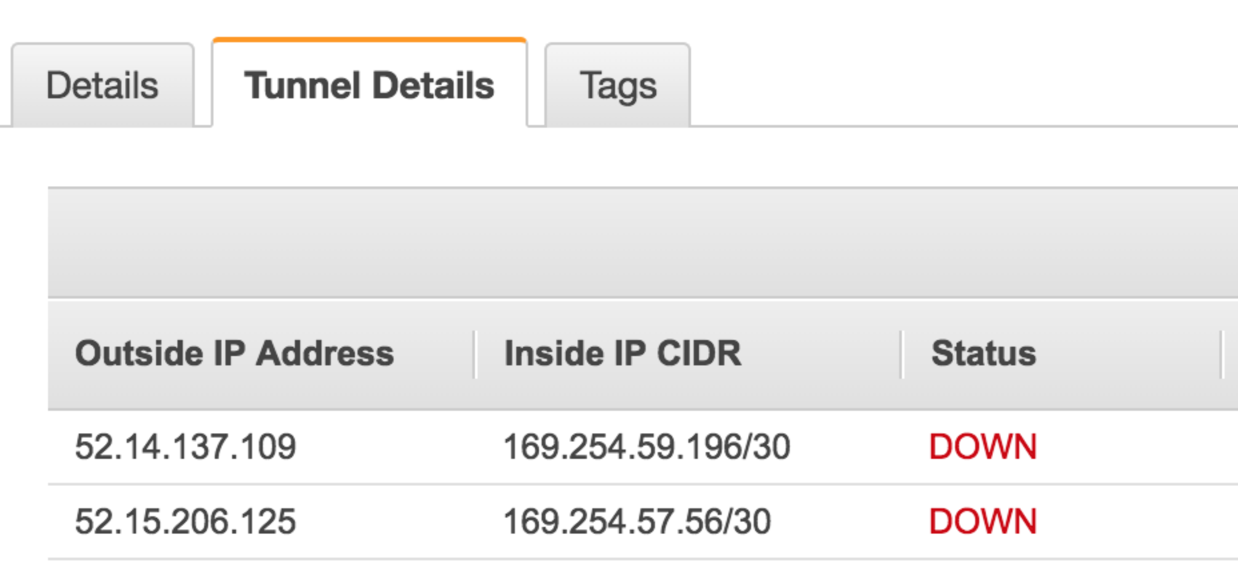
Add line to advertise router LAN to your VPC

Site-to-site VPN – Check status

Ping the other side of the tunnel: *ping 169.254.x.x*

Check BGP neighbor status: *show ip bgp summary*

Check VPN status in the console:



Outside IP Address	Inside IP CIDR	Status
52.14.137.109	169.254.59.196/30	DOWN
52.15.206.125	169.254.57.56/30	DOWN

Final connectivity test

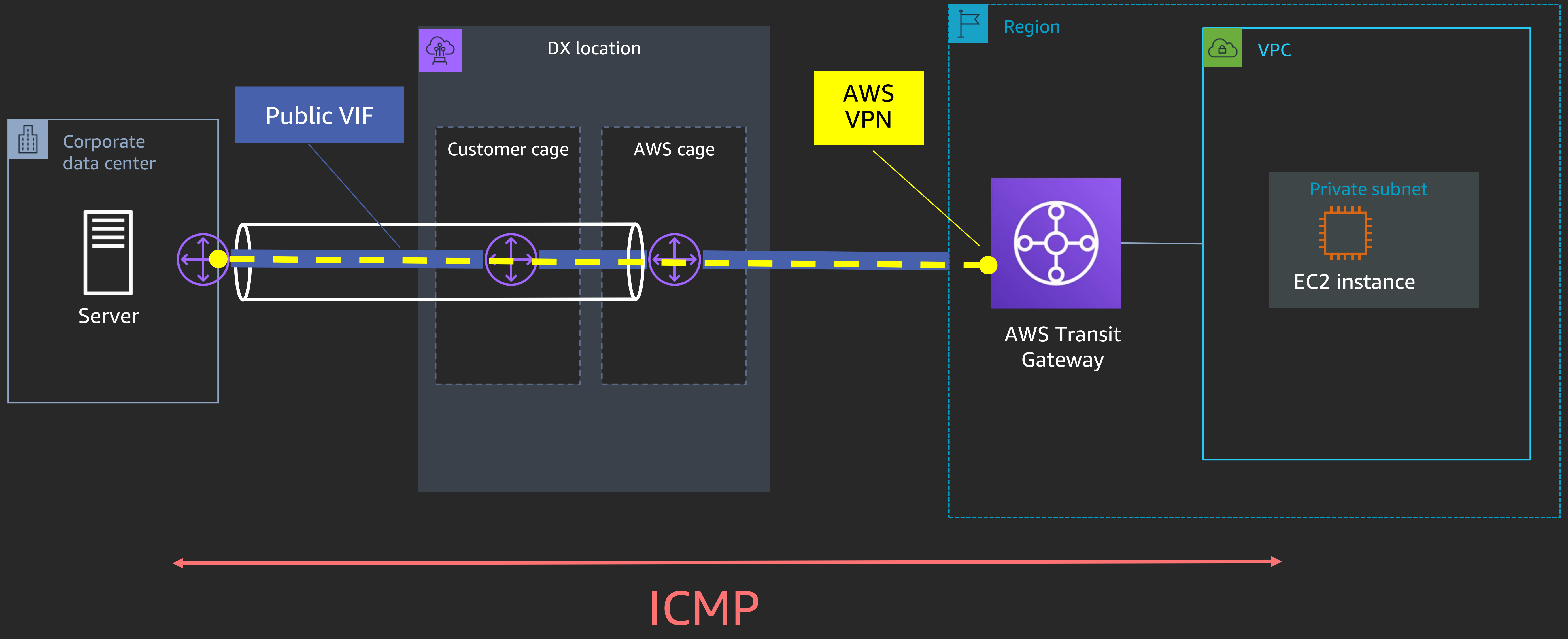
Check your VPC route table:

- Can you see a route for router LAN range (192.168.51.0/24)?
- Why was it added automatically?

Log into the instance and ping the on-premises server (192.168.51.10).

Success …

Final architecture



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

Useful Links

Please check out the following whitepaper and blog post:

Building a Scalable and Secure Multi-VPC AWS Network Infrastructure

Integrating sub-1 Gbps hosted connections with AWS Transit Gateway

Thank you!

Sohaib Tahir

sohaibt@amazon.com

Please complete the session survey in the mobile app.