AWS Networking

Andersen

Presenter:

Andrey Avdeev

a.avdeev@andersenlab.com

aws certified
Solutions Architect
Associate

aws certified
Advanced Networking
Specialty

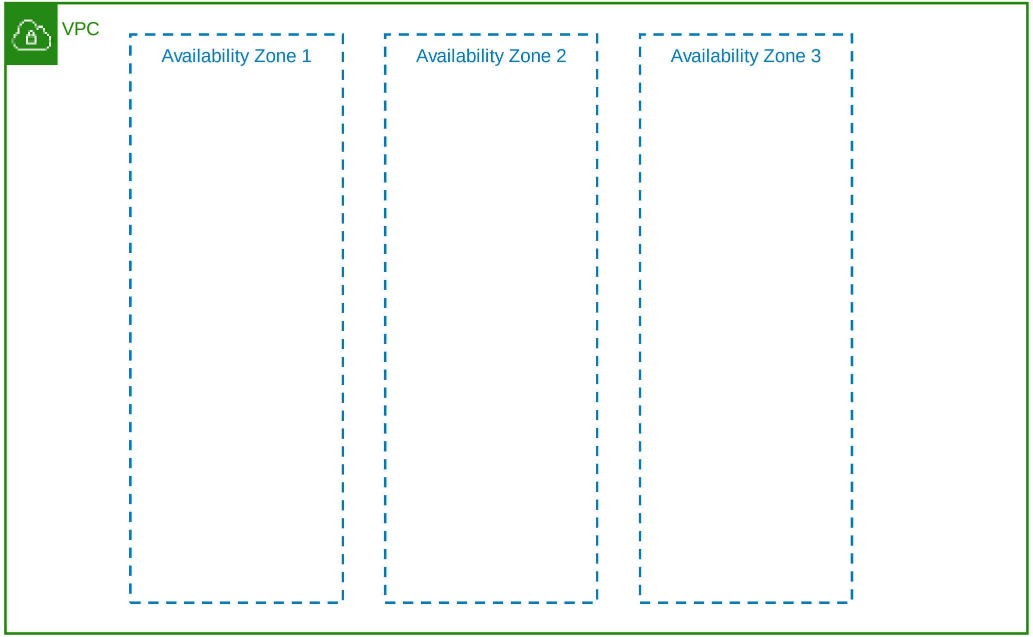
Andersen

AGENDA:

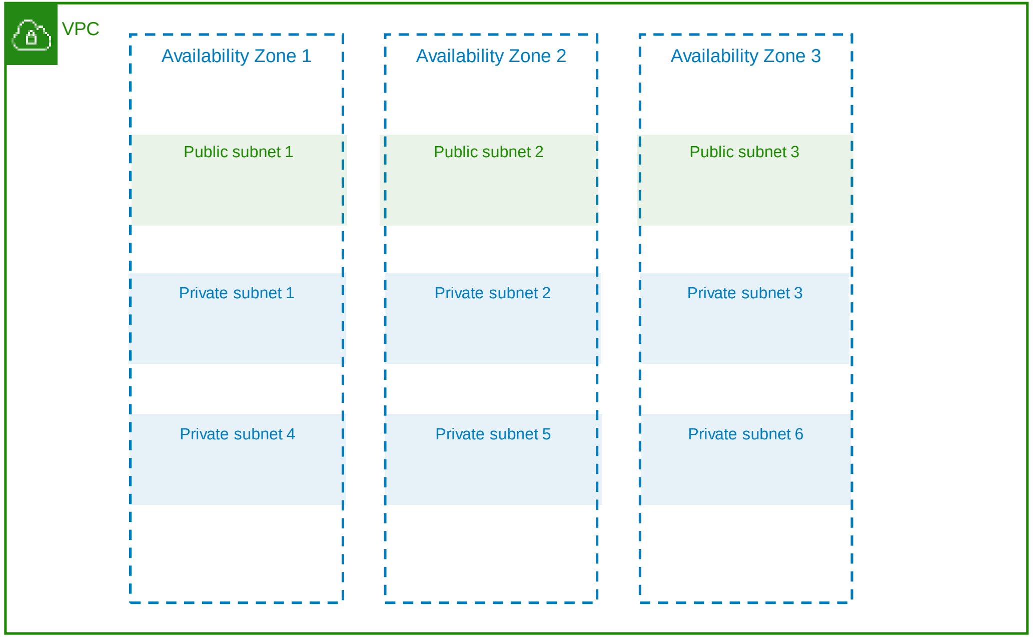
- AWS VPC concept
- AWS VPC peering
- AWS Endpoint
- AWS Site-to-Site VPN
- AWS Client VPN
- AWS Transit Gateway
- AWS Direct Connect
- AWS CloudFront
- AWS Route53

AWS VPC concept

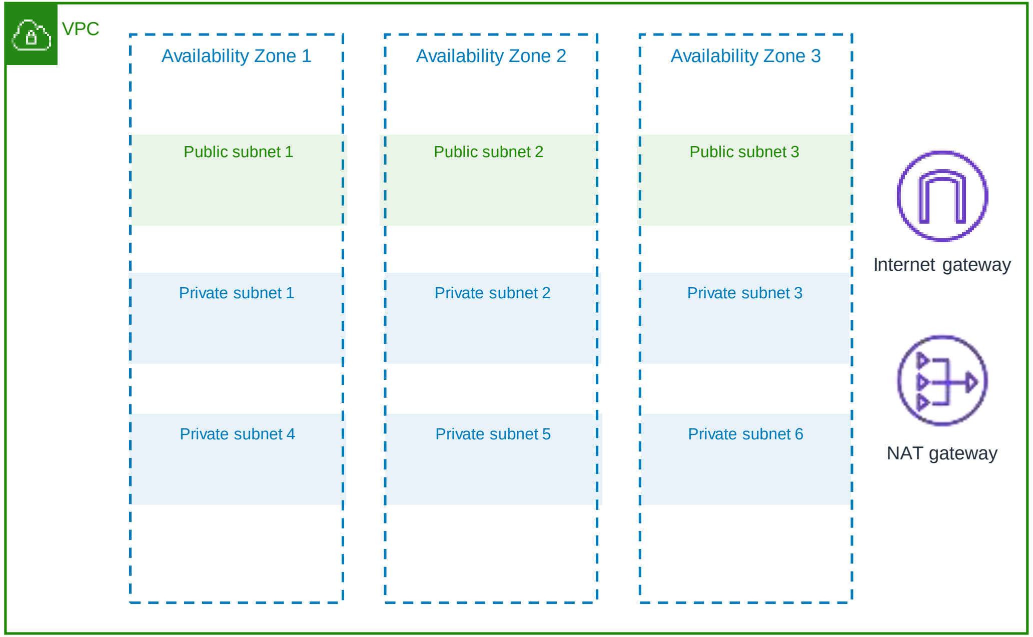
AWS VPC concept



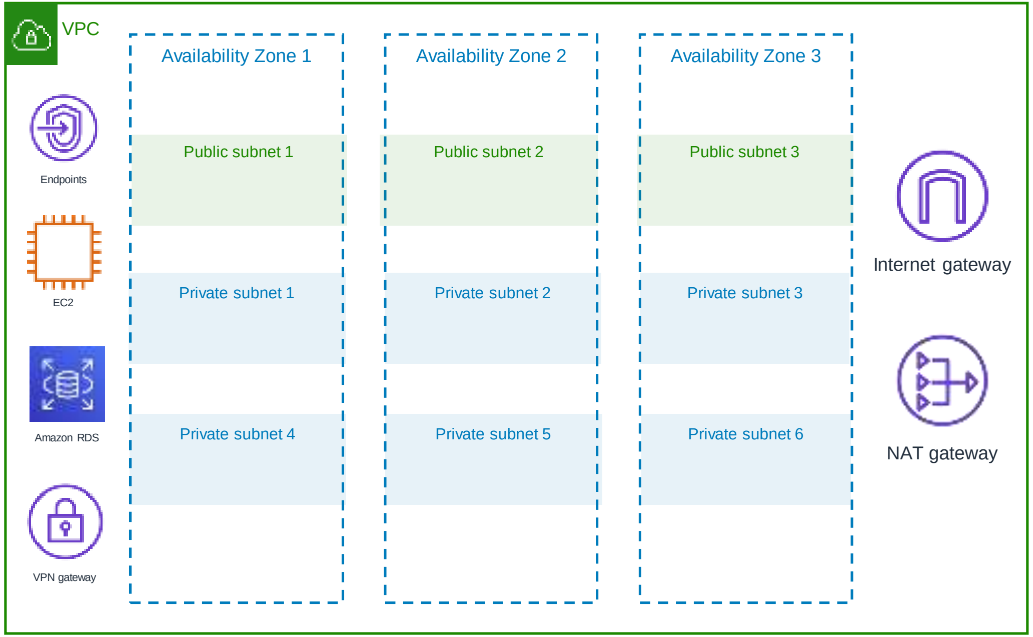
AWS VPC concept



AWS VPC concept

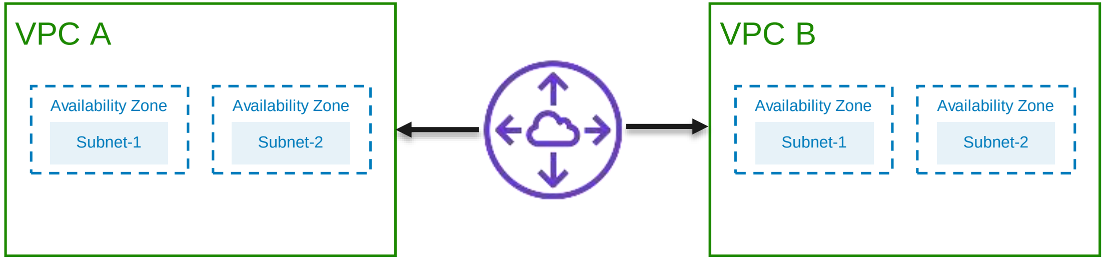


AWS VPC concept



VPC peering connection

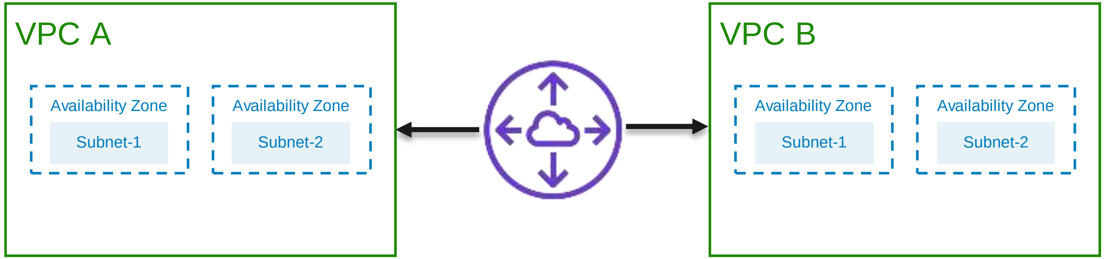
VPC peering connection

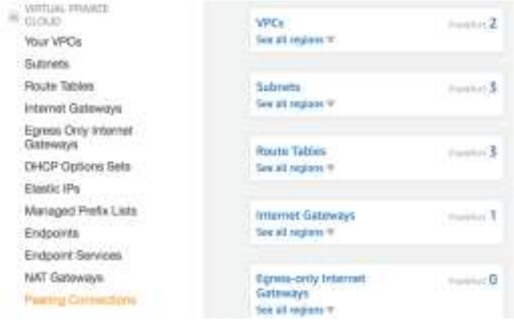


Cases:

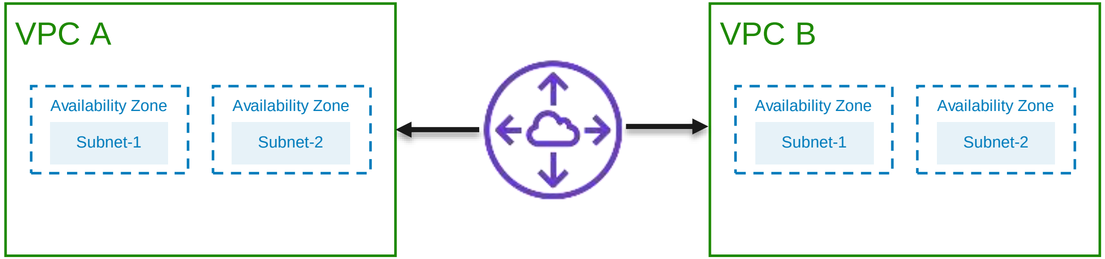
- resources in different VPCs
- security reasons

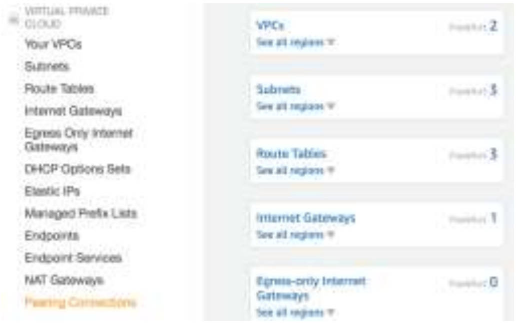
VPC peering connection





VPC peering connection





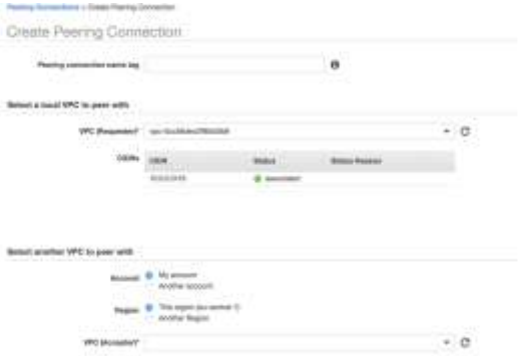
VPCs Frankfurt: 2
See all regions ▾

Subnets Frankfurt: 3
See all regions ▾

Route Tables Frankfurt: 3
See all regions ▾

Internet Gateways Frankfurt: 1
See all regions ▾

Egress-only Internet Gateways Frankfurt: 0
See all regions ▾



Create Peering Connection

Peering connection name tag

Select a local VPC to peer with

VPC (Requester)* vpc-[illegible]

CIDRs

CIDR	Status	Status Reason
[illegible]	associated	

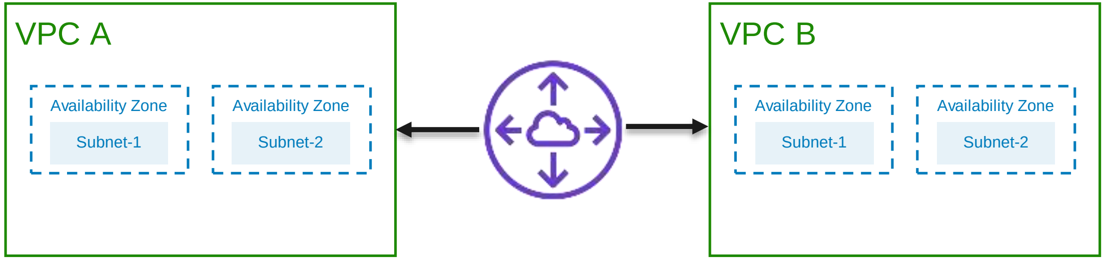
Select another VPC to peer with

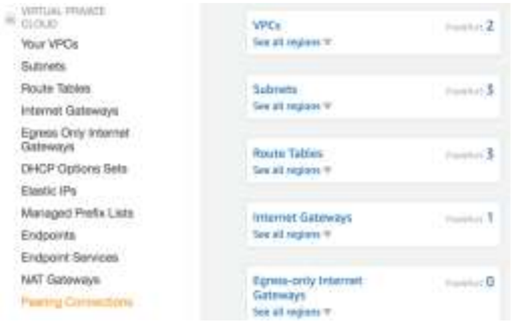
Account ● My account ○ Another account

Region ● This region ([illegible]) ○ Another Region

VPC (Accepter)*

VPC peering connection





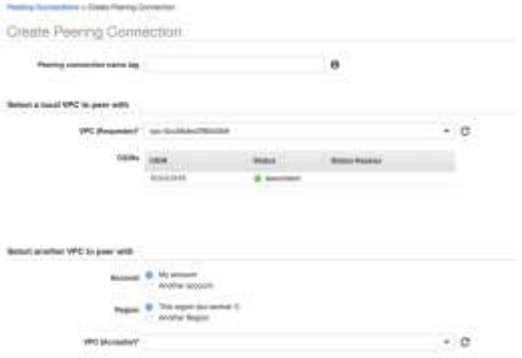
VPCs : 2
See all regions ▾

Subnets : 3
See all regions ▾

Route Tables : 3
See all regions ▾

Internet Gateways : 1
See all regions ▾

Egress-only Internet Gateways : 0
See all regions ▾



Create Peering Connection

Peering connection name tag

Select a local VPC to peer with

VPC (Requester)* [illegible]

CIDRs

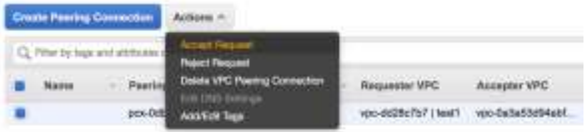
CIDR	Status	Status Reason
[illegible]	● associated	

Select another VPC to peer with

Account ● My account
○ Another account

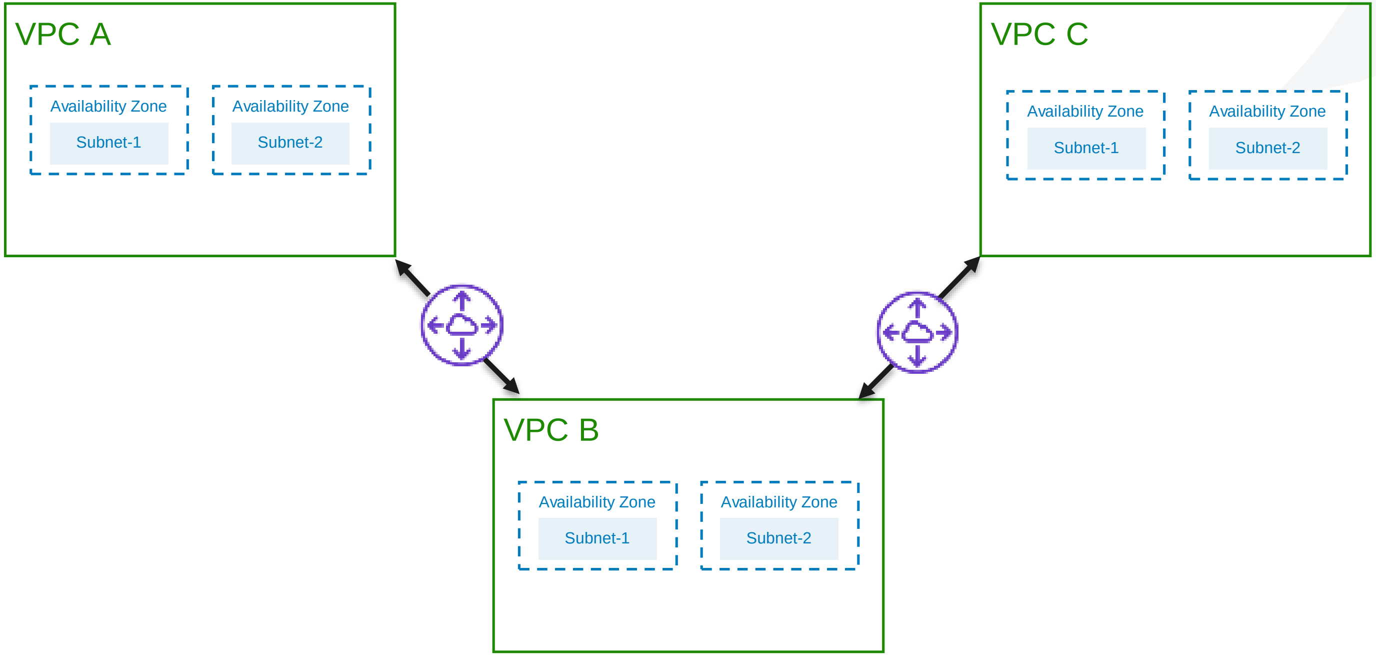
Region ● This region (eu-central-1)
○ Another Region

VPC (Accepter)*

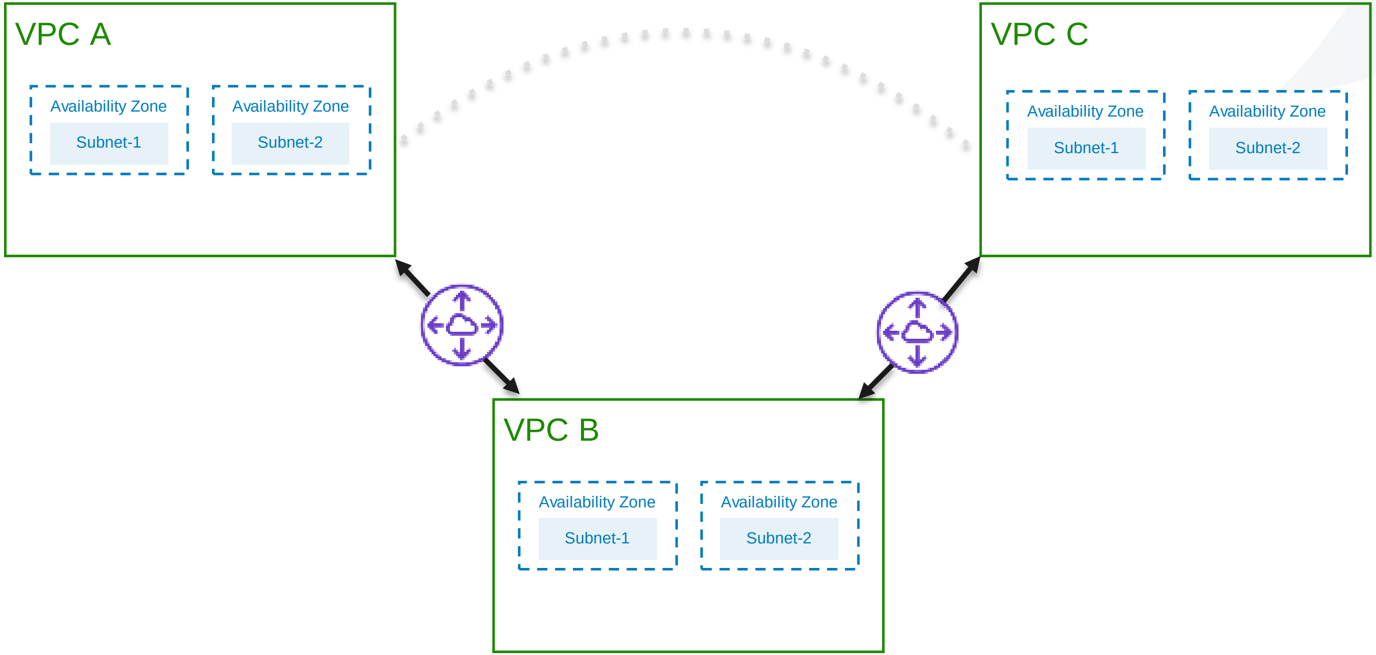

Create Peering Connection
Actions ^
Filter by tags and attributes
Accept Request
Reject Request
Delete VPC Peering Connection
Edit DNS Settings
Add/Edit Tags

Name	Peering	Requester VPC	Accepter VPC
	pcx-0d	vpc-dd28cfb7 | test1	vpc-0a3a53d94ebf...

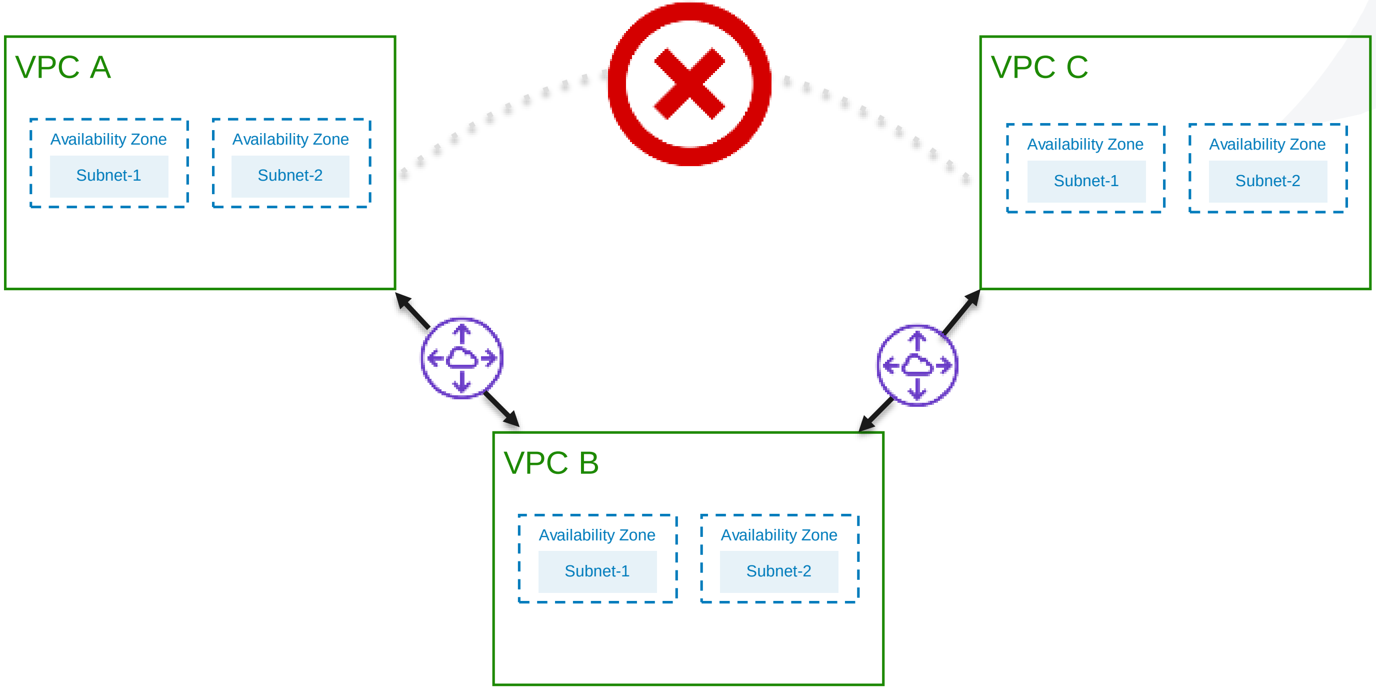
VPC peering connection



VPC peering connection

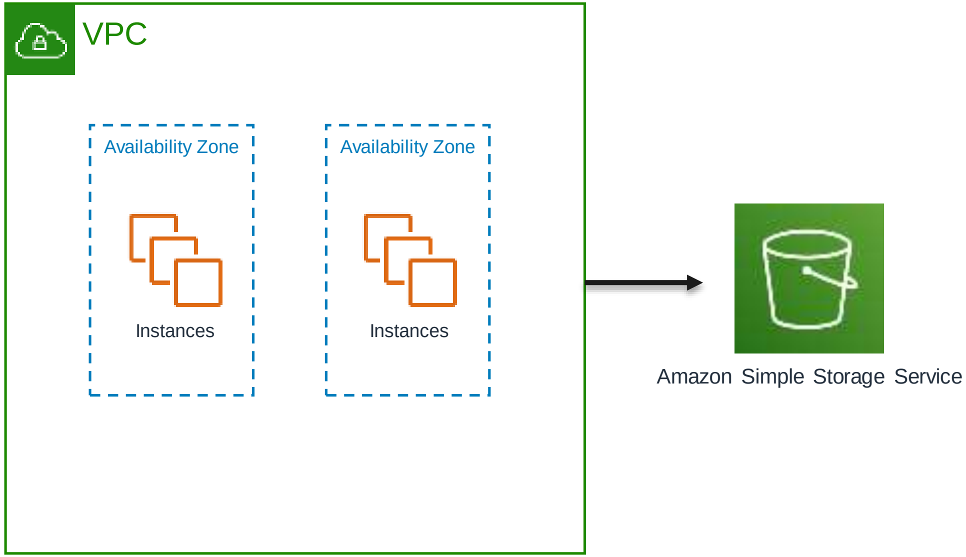


VPC peering connection

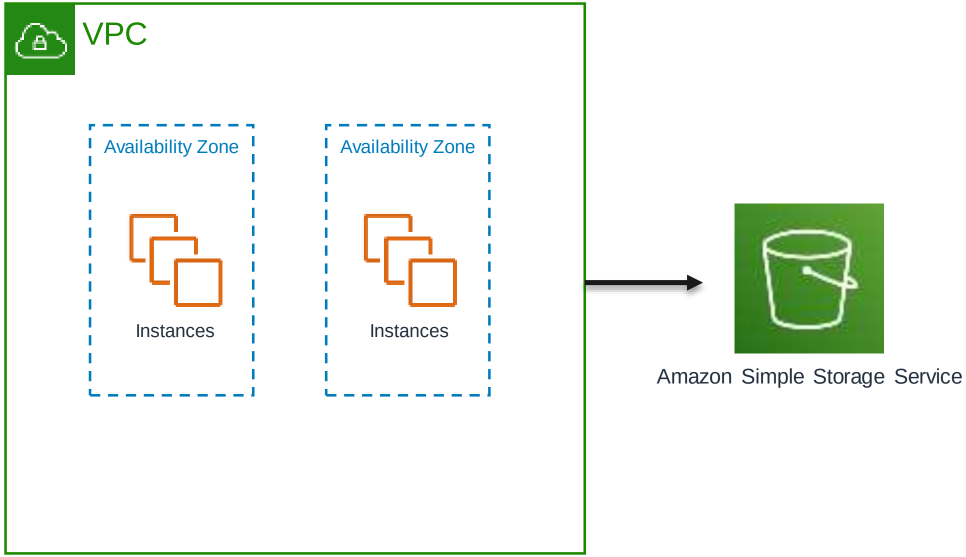


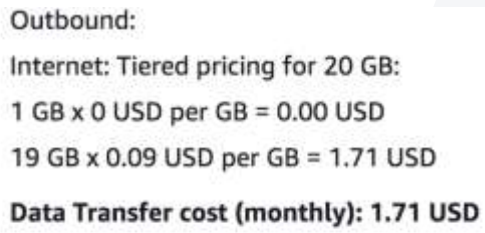
AWS Endpoints Services

AWS Endpoints Services



AWS Endpoints Services





Outbound:

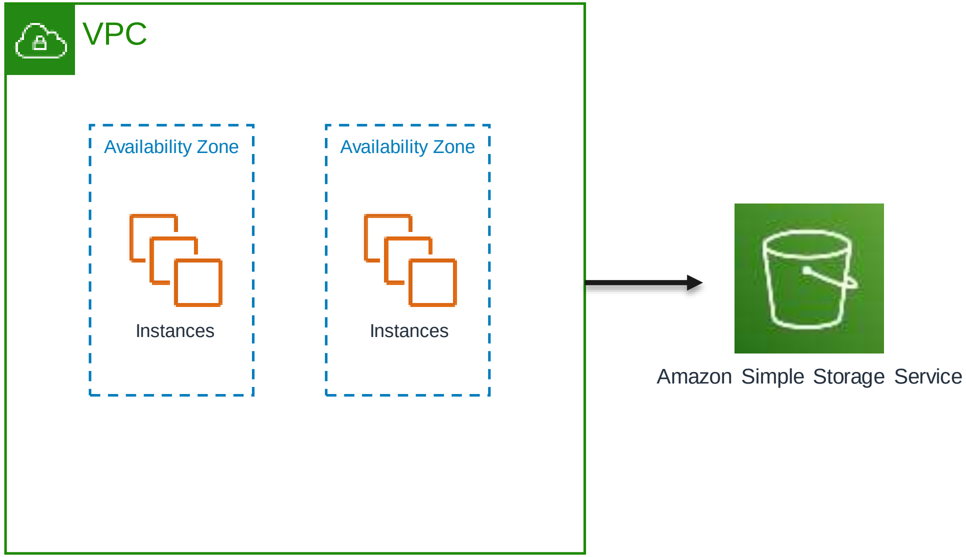
Internet: Tiered pricing for 20 GB:

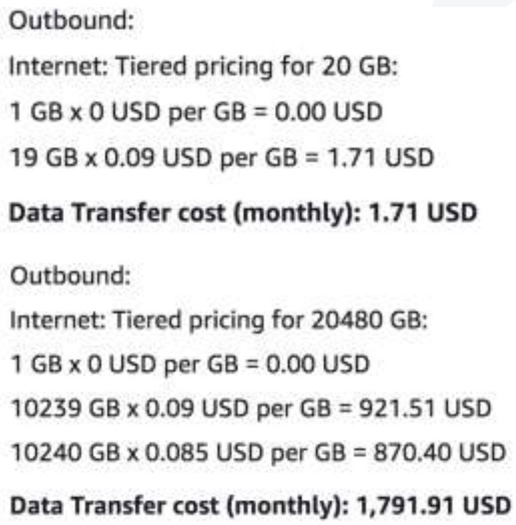
1 GB x 0 USD per GB = 0.00 USD

19 GB x 0.09 USD per GB = 1.71 USD

Data Transfer cost (monthly): 1.71 USD

AWS Endpoints Services




Outbound:

Internet: Tiered pricing for 20 GB:

1 GB x 0 USD per GB = 0.00 USD

19 GB x 0.09 USD per GB = 1.71 USD

Data Transfer cost (monthly): 1.71 USD

Outbound:

Internet: Tiered pricing for 20480 GB:

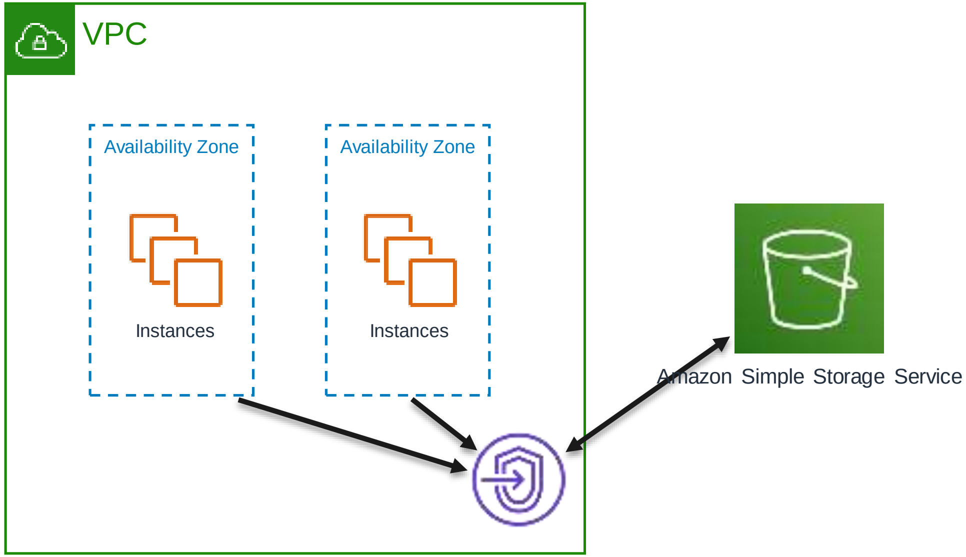
1 GB x 0 USD per GB = 0.00 USD

10239 GB x 0.09 USD per GB = 921.51 USD

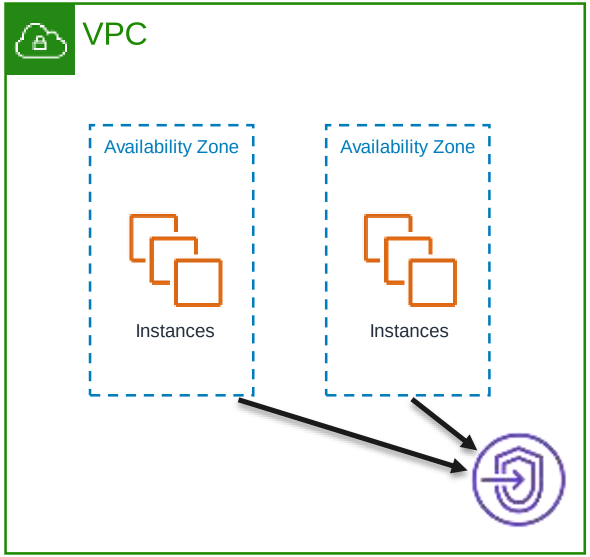
10240 GB x 0.085 USD per GB = 870.40 USD

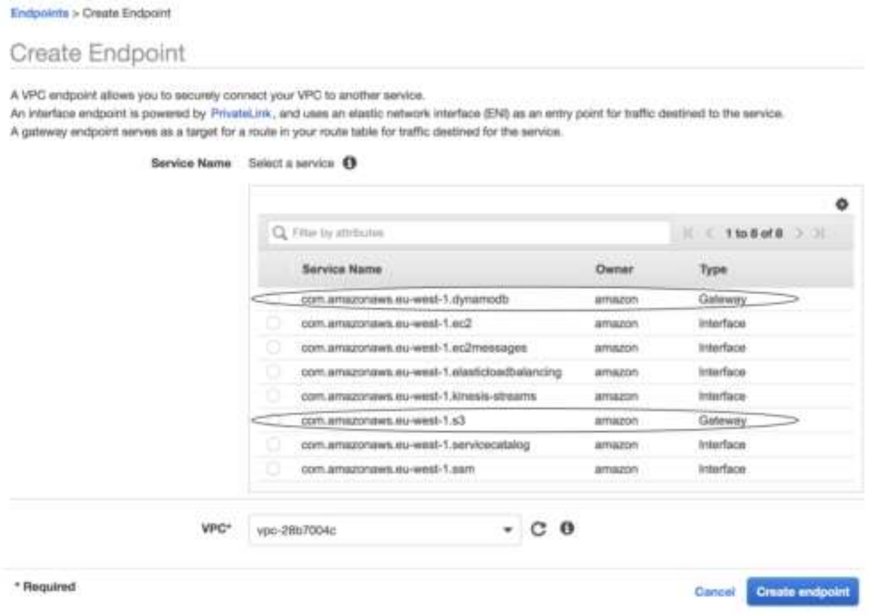
Data Transfer cost (monthly): 1,791.91 USD

AWS Endpoints Services



AWS Endpoints Services





Create Endpoint

A VPC endpoint allows you to securely connect your VPC to another service.
An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.
A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

Service Name Select a service

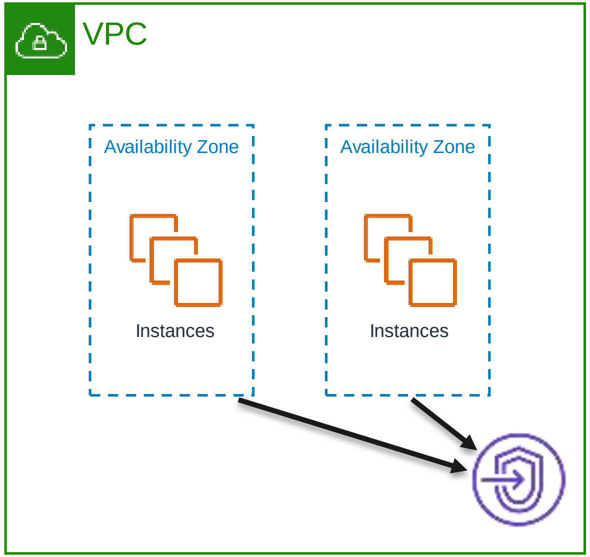
Filter by attributes
1 to 8 of 8

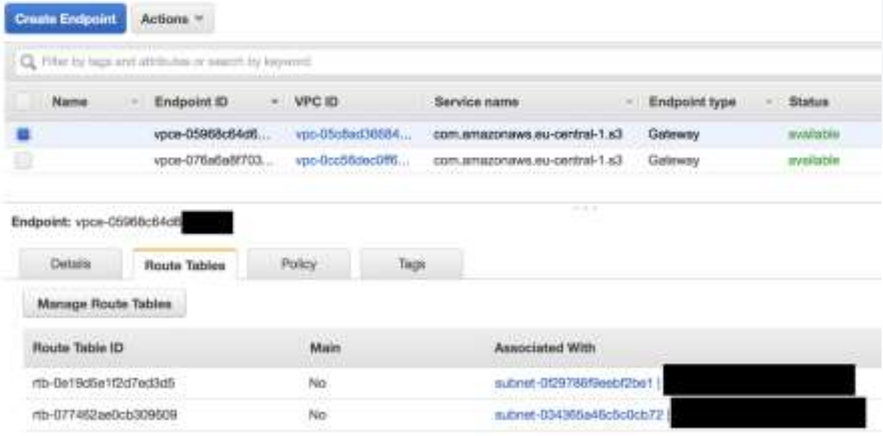
	Service Name	Owner	Type
	com.amazonaws.eu-west-1.dynamodb	amazon	Gateway
○	com.amazonaws.eu-west-1.ec2	amazon	Interface
○	com.amazonaws.eu-west-1.ec2messages	amazon	Interface
○	com.amazonaws.eu-west-1.elasticloadbalancing	amazon	Interface
○	com.amazonaws.eu-west-1.kinesis-streams	amazon	Interface
	com.amazonaws.eu-west-1.s3	amazon	Gateway
○	com.amazonaws.eu-west-1.servicecatalog	amazon	Interface
○	com.amazonaws.eu-west-1.sam	amazon	Interface

VPC* vpc-28b7004c

* Required

AWS Endpoints Services



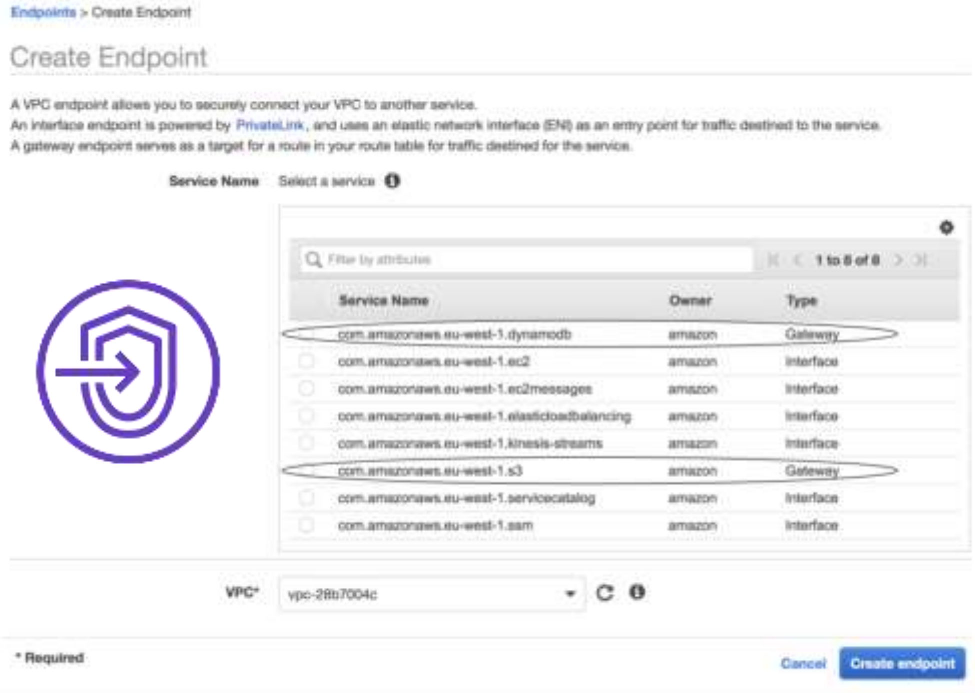


	Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status
■		vpce-05968c64d8...	vpc-05c6ad36684...	com.amazonaws.eu-central-1.s3	Gateway	available
□		vpce-076a6a8f703...	vpc-0cc56dec0f6...	com.amazonaws.eu-central-1.s3	Gateway	available

Endpoint: vpce-05968c64d8[redacted]

Route Table ID	Main	Associated With
rtb-0e19d6e1f2d7ed3d5	No	subnet-0f29786f9eebf2be1 | [redacted]
rtb-077462ae0cb309509	No	subnet-034365a46c5c0cb72 | [redacted]

AWS Endpoints Services



Endpoints > Create Endpoint

Create Endpoint

A VPC endpoint allows you to securely connect your VPC to another service.
An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.
A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

Service Name Select a service

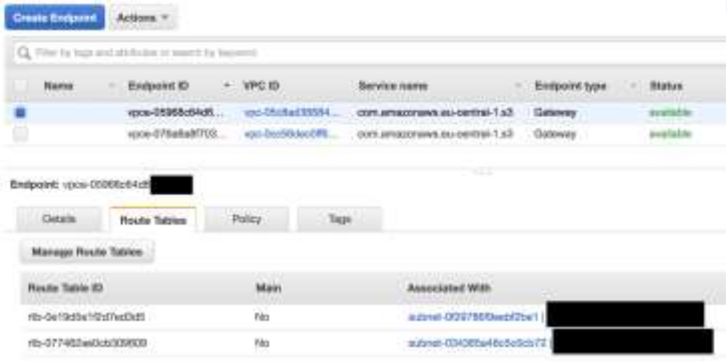
Filter by attributes 1 to 8 of 8

	Service Name	Owner	Type
○	com.amazonaws.eu-west-1.dynamodb	amazon	Gateway
○	com.amazonaws.eu-west-1.ec2	amazon	Interface
○	com.amazonaws.eu-west-1.ec2messages	amazon	Interface
○	com.amazonaws.eu-west-1.elasticloadbalancing	amazon	Interface
○	com.amazonaws.eu-west-1.kinesis-streams	amazon	Interface
○	com.amazonaws.eu-west-1.s3	amazon	Gateway
○	com.amazonaws.eu-west-1.servicecatalog	amazon	Interface
○	com.amazonaws.eu-west-1.ssm	amazon	Interface

VPC* vpc-28b7004c

* Required

Cancel Create endpoint



Create Endpoint Actions

Filter by tags and attributes or search by keyword

	Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status
☑		vpce-05968c64d6...	vpc-05c8ad33594...	com.amazonaws.eu-central-1.s3	Gateway	available
□		vpce-07ba8a8f703...	vpc-0cc58dec0f8...	com.amazonaws.eu-central-1.s3	Gateway	available

Endpoint: vpce-05068c64d6[redacted]

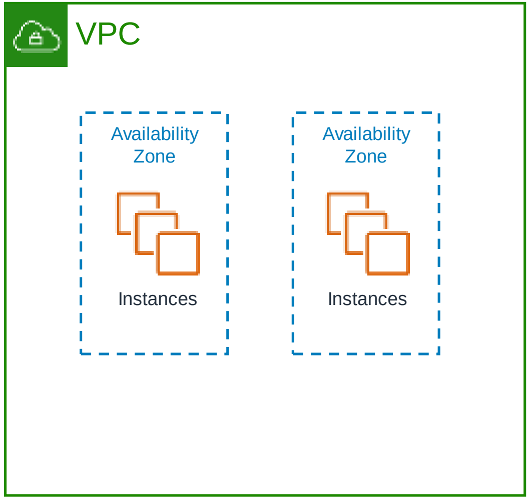
Details | Route Tables | Policy | Tags

Manage Route Tables

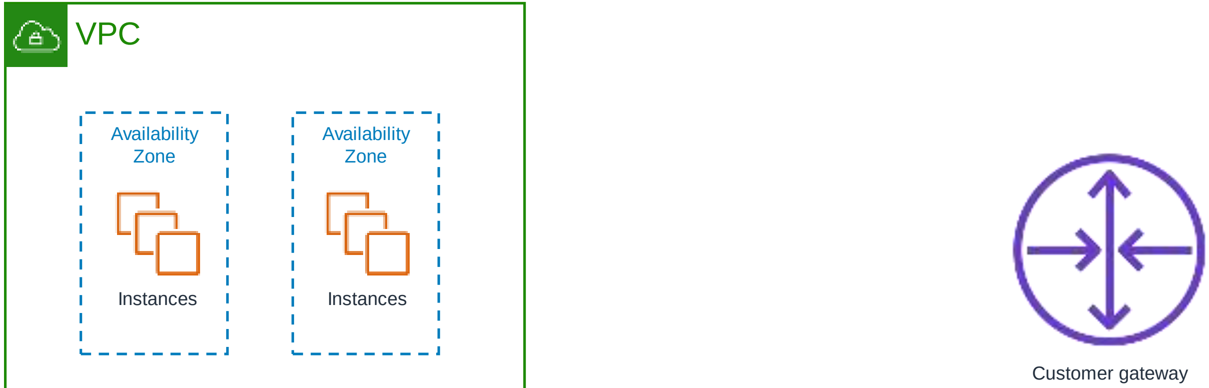
Route Table ID	Main	Associated With
rtb-0e19d3e1f2d7ed0d5	No	subnet-0f2978f0aebf2be1 | [redacted]
rtb-077482ae0cb309809	No	subnet-03406ba46c5c0cb72 | [redacted]

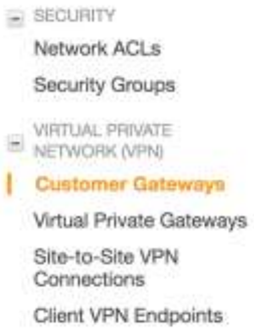
AWS Site-to-Site VPN

AWS Site-to-Site VPN



AWS Site-to-Site VPN




SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

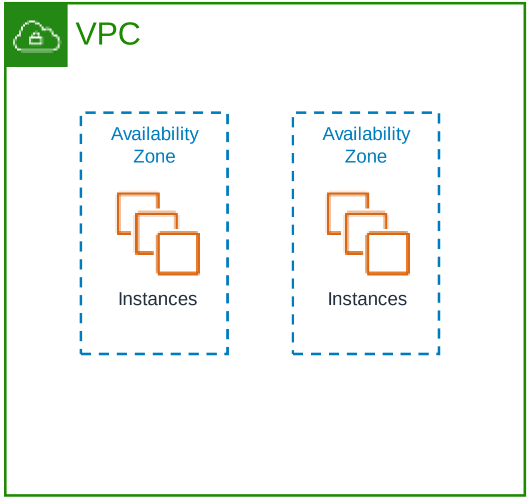
Customer Gateways

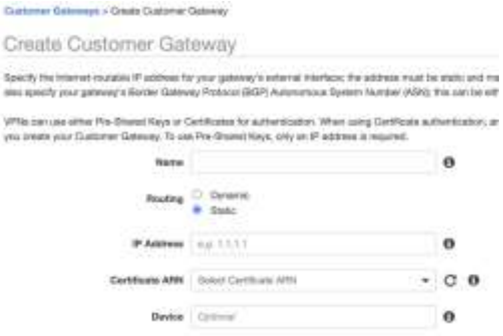
Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

AWS Site-to-Site VPN





Customer Gateways > Create Customer Gateway

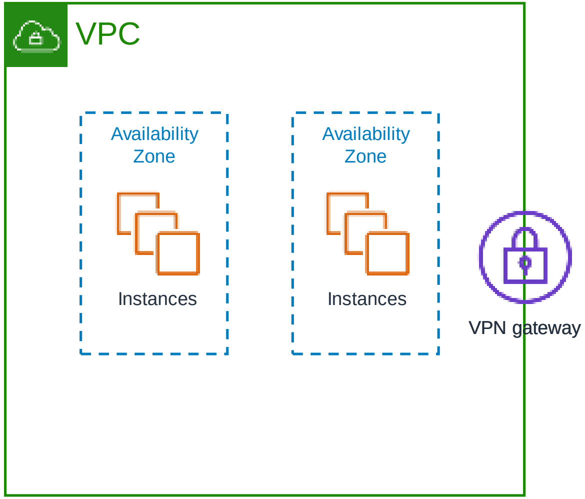
Create Customer Gateway

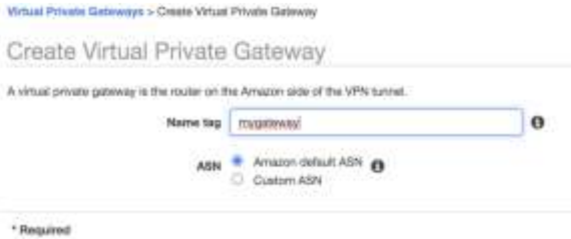
Specify the Internet-routable IP address for your gateway's external interface; the address must be static and ma
also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be eit

VPNs can use either Pre-Shared Keys or Certificates for authentication. When using Certificate authentication, ar
you create your Customer Gateway. To use Pre-Shared Keys, only an IP address is required.

Name	
Routing	○ Dynamic ● Static
IP Address	e.g. 1.1.1.1
Certificate ARN	Select Certificate ARN
Device	Optional

AWS Site-to-Site VPN




Virtual Private Gateways > Create Virtual Private Gateway

Create Virtual Private Gateway

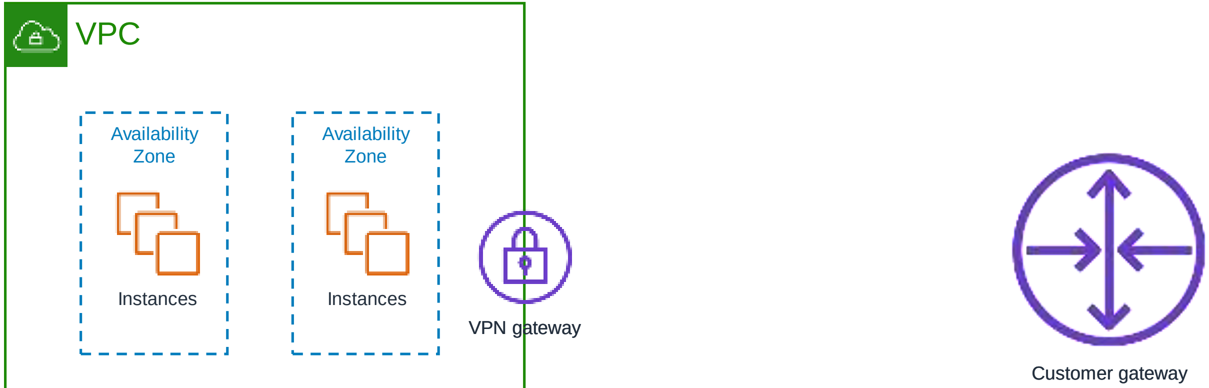
A virtual private gateway is the router on the Amazon side of the VPN tunnel.

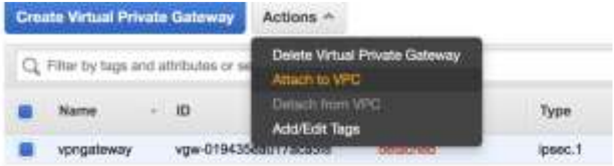
Name tag: mygateway

ASN: ● Amazon default ASN ○ Custom ASN

* Required

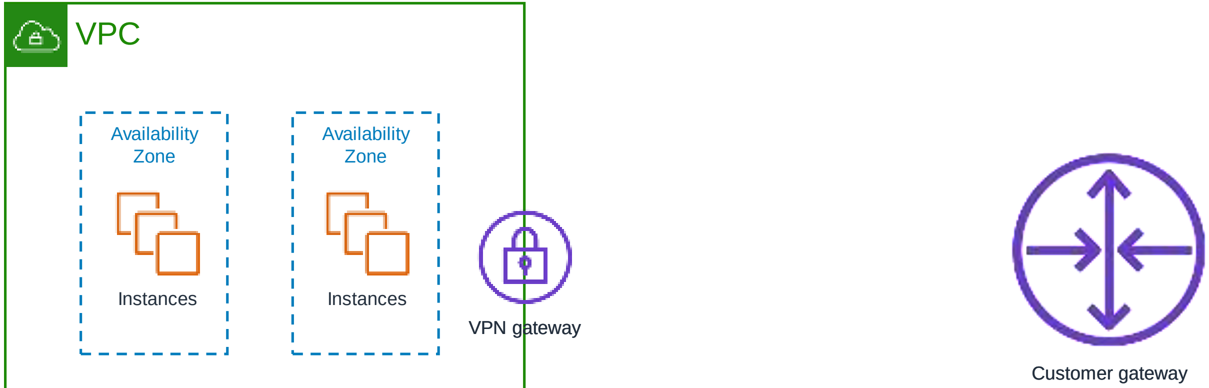
AWS Site-to-Site VPN

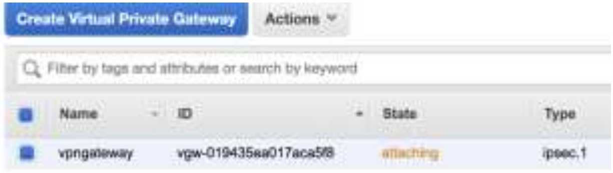



Create Virtual Private Gateway
Actions
Delete Virtual Private Gateway
Attach to VPC
Detach from VPC
Add/Edit Tags
Filter by tags and attributes or se

Name	ID		Type
vpngateway	vgw-019435[illegible]	[illegible]	ipsec.1

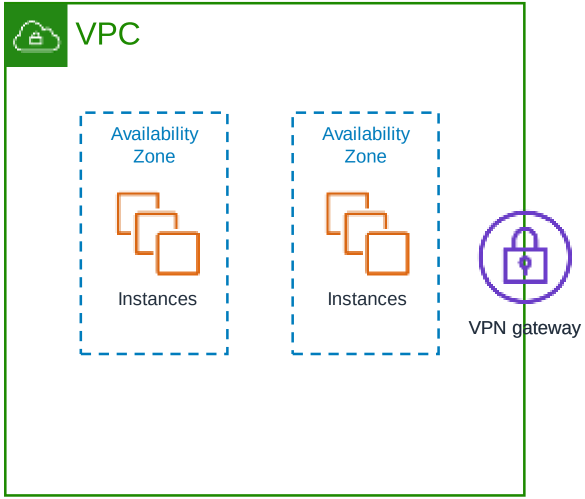
AWS Site-to-Site VPN

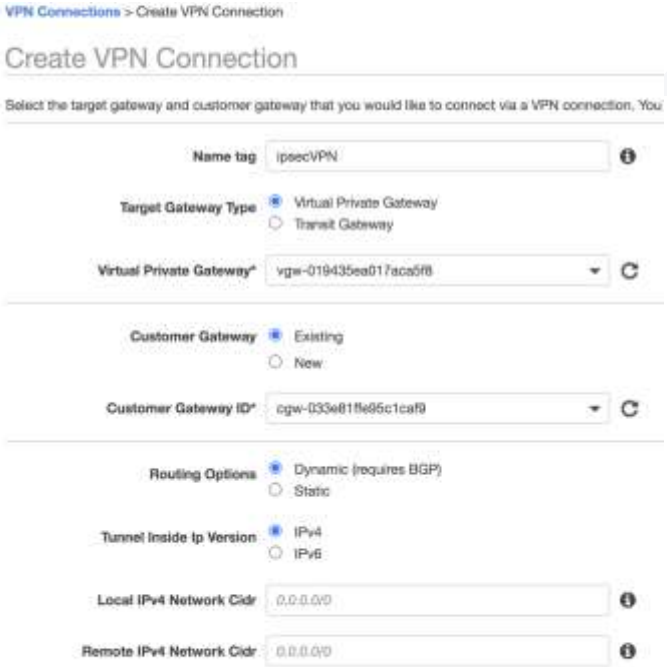



Create Virtual Private Gateway
Actions
Filter by tags and attributes or search by keyword

	Name	ID	State	Type
■	vpngateway	vgw-019435aa017aca5f8	attaching	ipsec.1

AWS Site-to-Site VPN





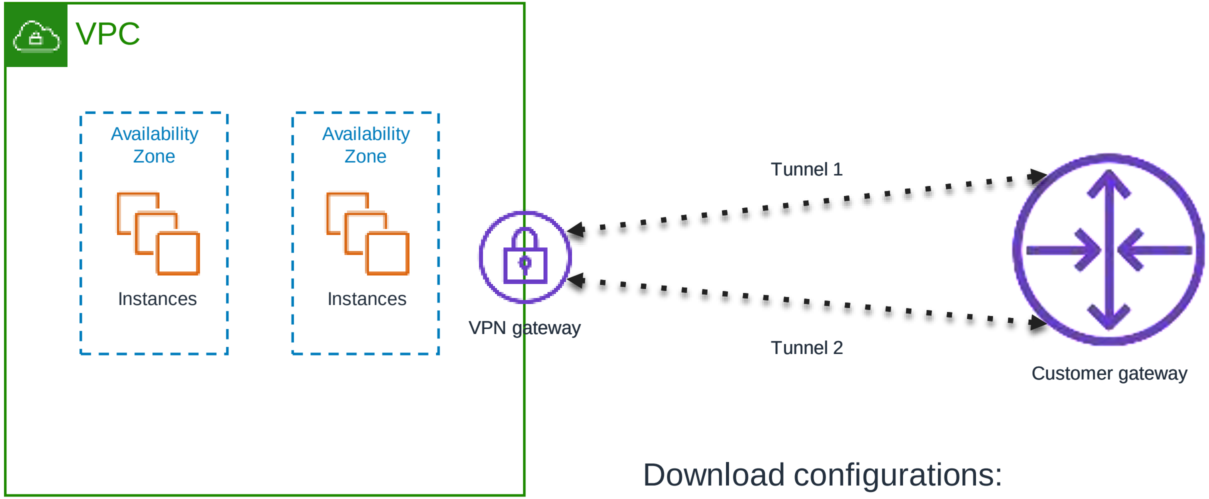
VPN Connections > Create VPN Connection

Create VPN Connection

Select the target gateway and customer gateway that you would like to connect via a VPN connection. You

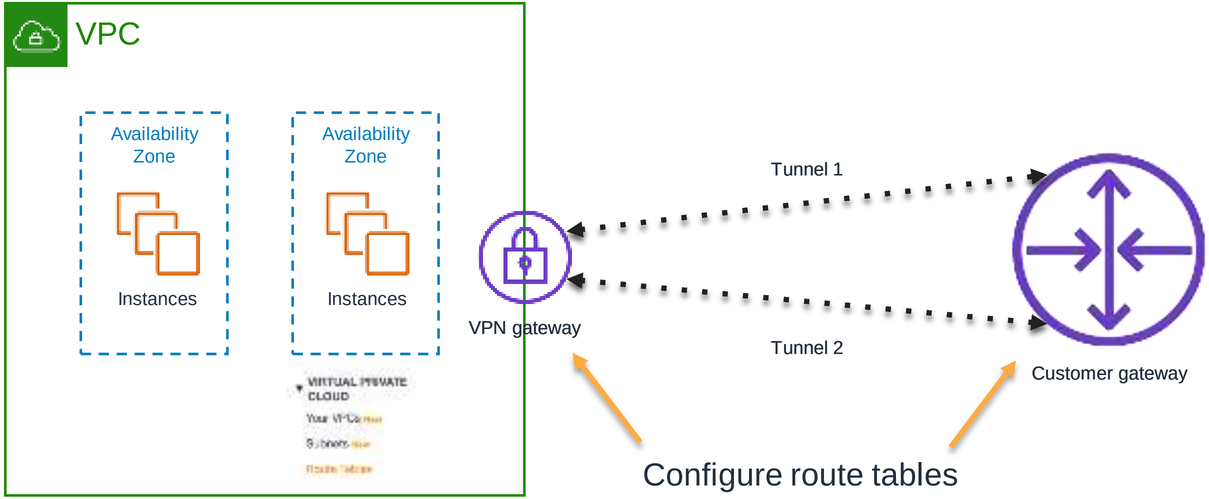
Name tag	ipsecVPN
Target Gateway Type	● Virtual Private Gateway ○ Transit Gateway
Virtual Private Gateway*	vgw-019435ea017aca5f8
Customer Gateway	● Existing ○ New
Customer Gateway ID*	cgw-033e81ffe85c1caf9
Routing Options	● Dynamic (requires BGP) ○ Static
Tunnel Inside Ip Version	● IPv4 ○ IPv6
Local IPv4 Network Cidr	0.0.0.0/0
Remote IPv4 Network Cidr	0.0.0.0/0

AWS Site-to-Site VPN



Download configurations:
- Cisco
- Juniper
- Mikrotik
- etc

AWS Site-to-Site VPN

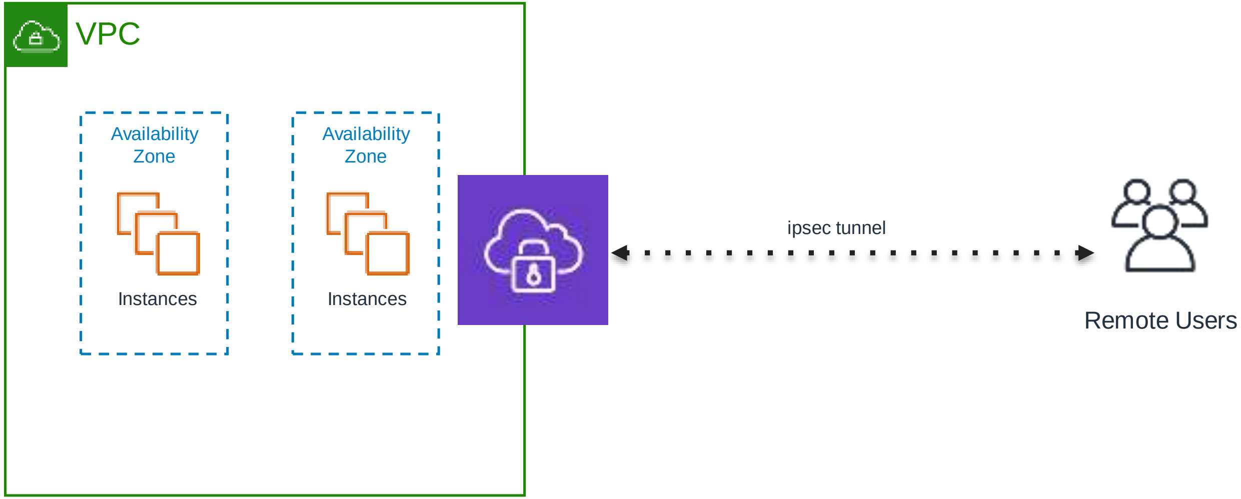


Configure route tables

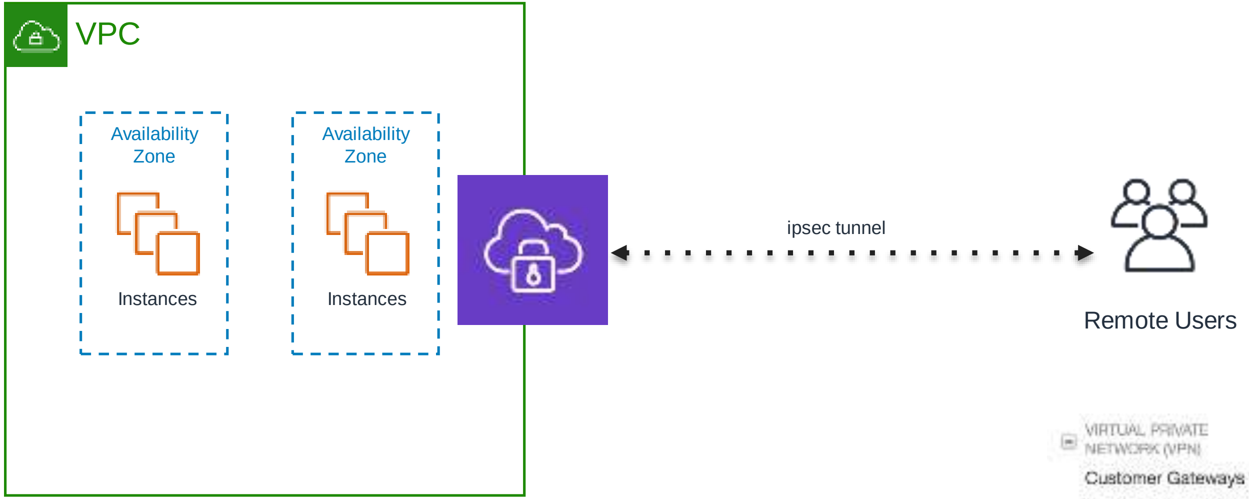
- Static
- Dynamic routing (BGP)

AWS Client VPN

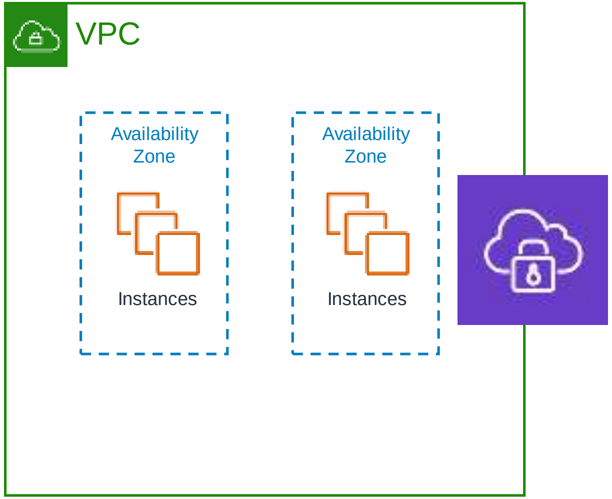
AWS Client VPN

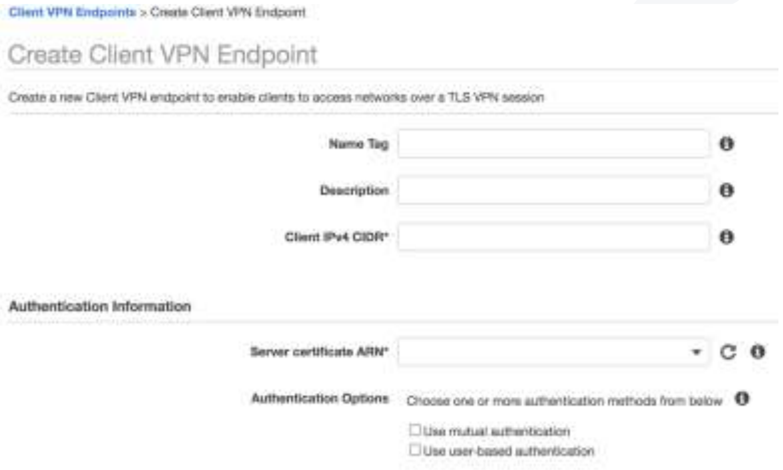


AWS Client VPN



AWS Client VPN





Client VPN Endpoints > Create Client VPN Endpoint

Create Client VPN Endpoint

Create a new Client VPN endpoint to enable clients to access networks over a TLS VPN session

Name Tag

Description

Client IPv4 CIDR*

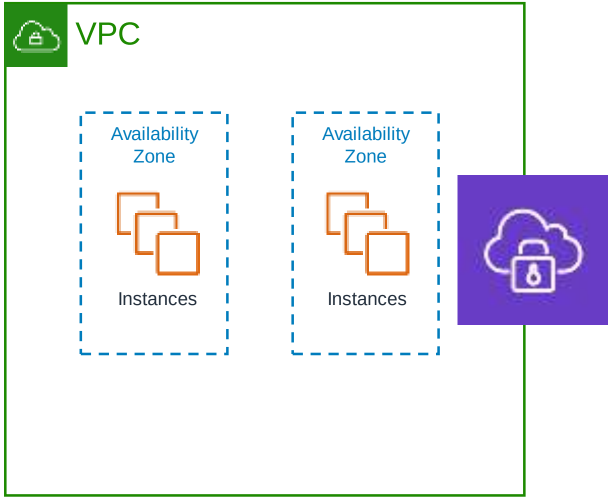
Authentication Information

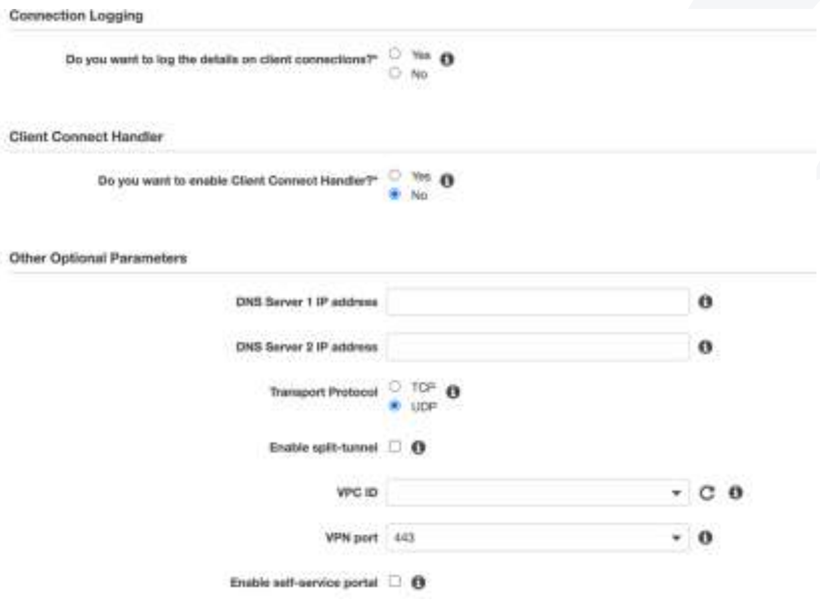
Server certificate ARN*

Authentication Options: Choose one or more authentication methods from below

☐ Use mutual authentication
☐ Use user-based authentication

AWS Client VPN





Connection Logging

Do you want to log the details on client connections?* ○ Yes ○ No

Client Connect Handler

Do you want to enable Client Connect Handler?* ○ Yes ● No

Other Optional Parameters

DNS Server 1 IP address

DNS Server 2 IP address

Transport Protocol ○ TCP ● UDP

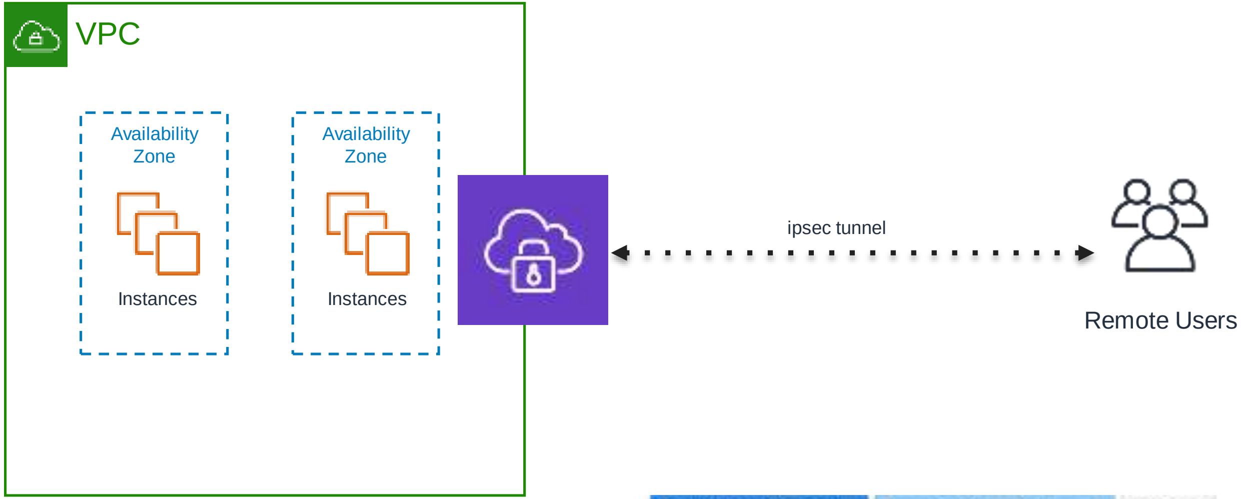
Enable split-tunnel □

VPC ID

VPN port 443

Enable self-service portal □

AWS Client VPN



Create Client VPN Endpoint
Download Client Configuration
Actions
Filter by tags and attributes or search by keyword

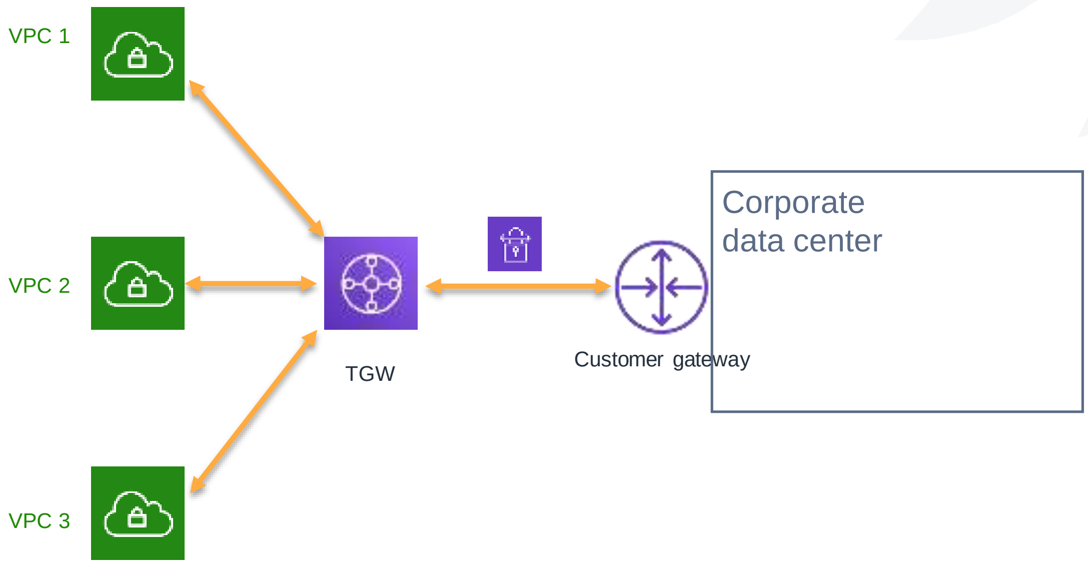
https://aws.amazon.com/vpn/client-vpn-download/

AWS Transit Gateway

A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks.

Andersen

AWS Transit Gateway



VPC 1

VPC 2

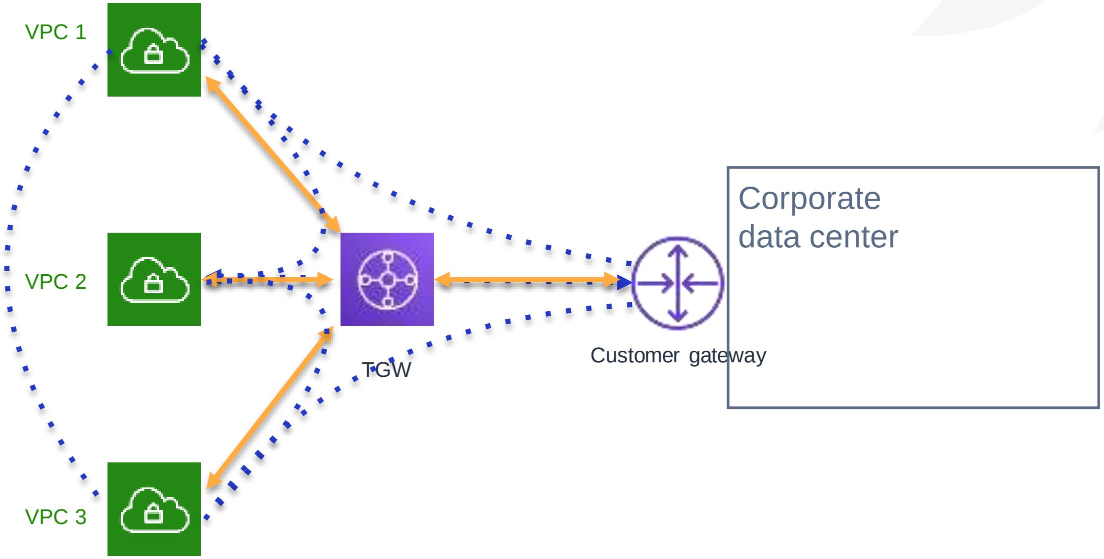
VPC 3

TGW

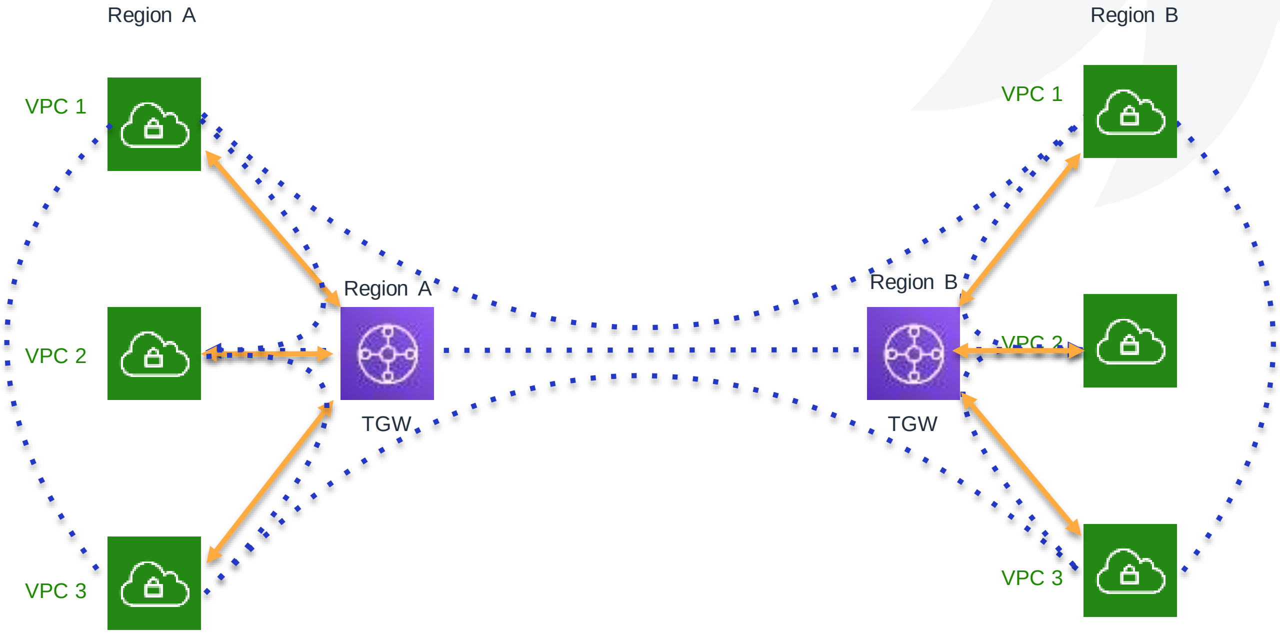
Customer gateway

Corporate data center

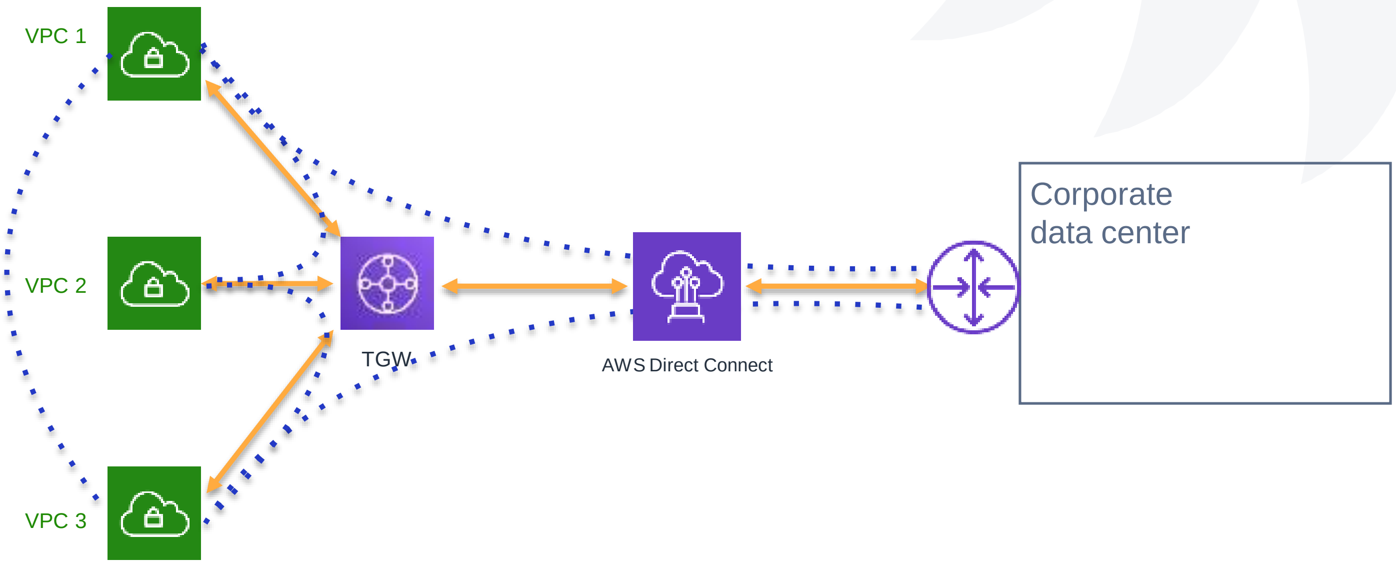
AWS Transit Gateway



AWS Transit Gateway



AWS Transit Gateway



Andersen

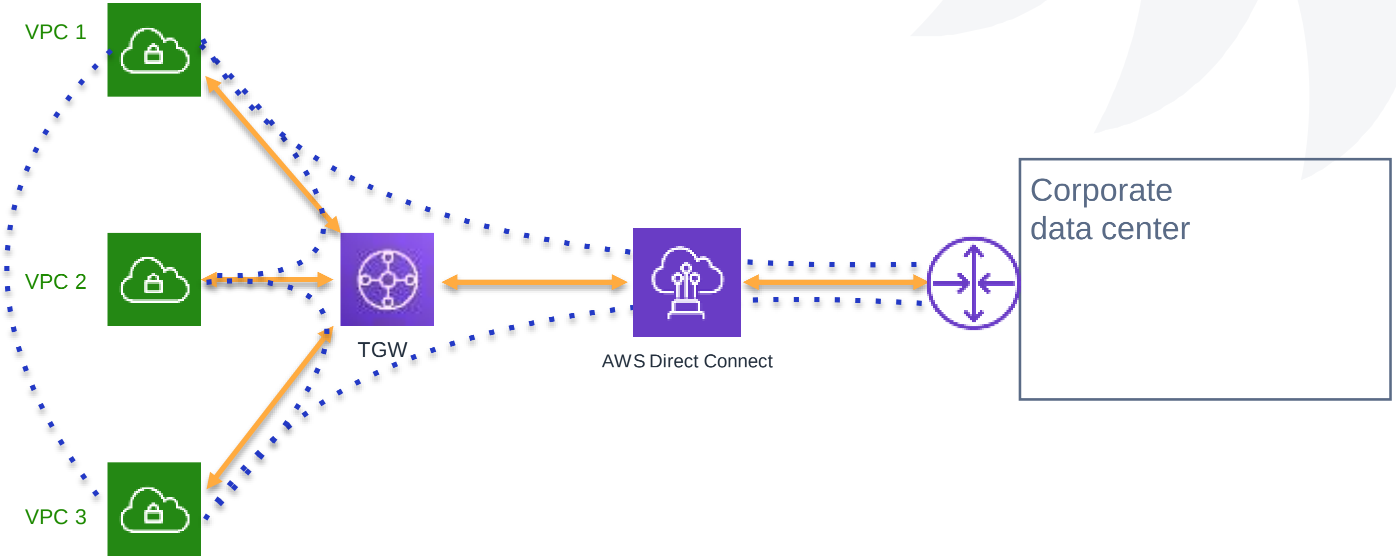
AWS Direct Connect

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable.

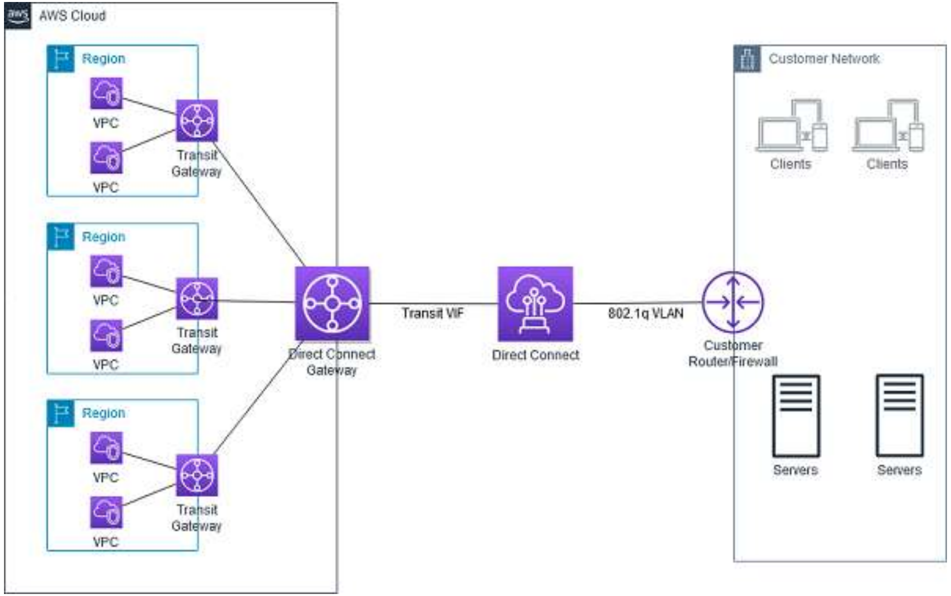
Work with VIFs:

- Public VIF (connection for public resources)
- Private VIF (connection to private resources)
- Transit VIF (for transit routing only)

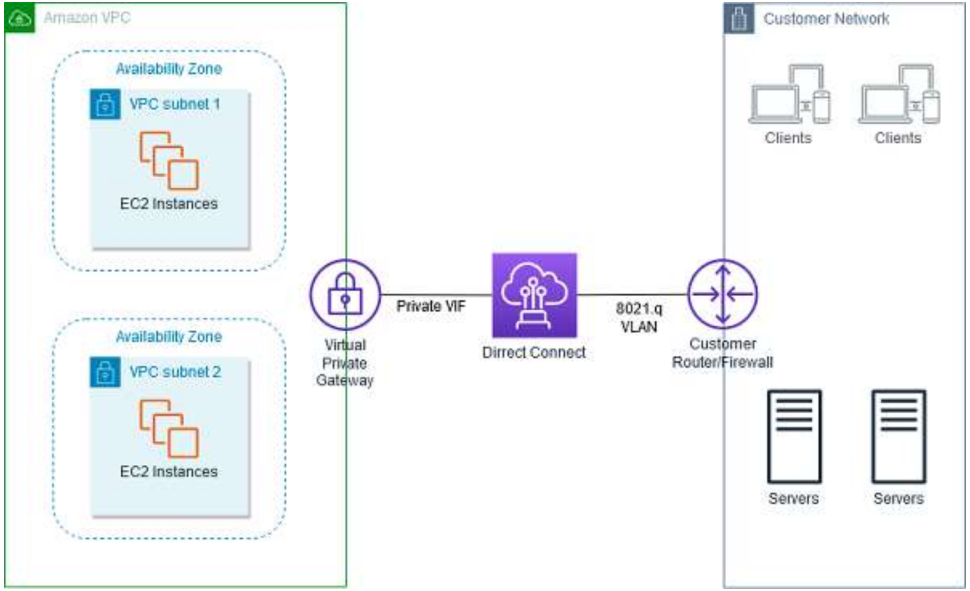
AWS Direct Connect



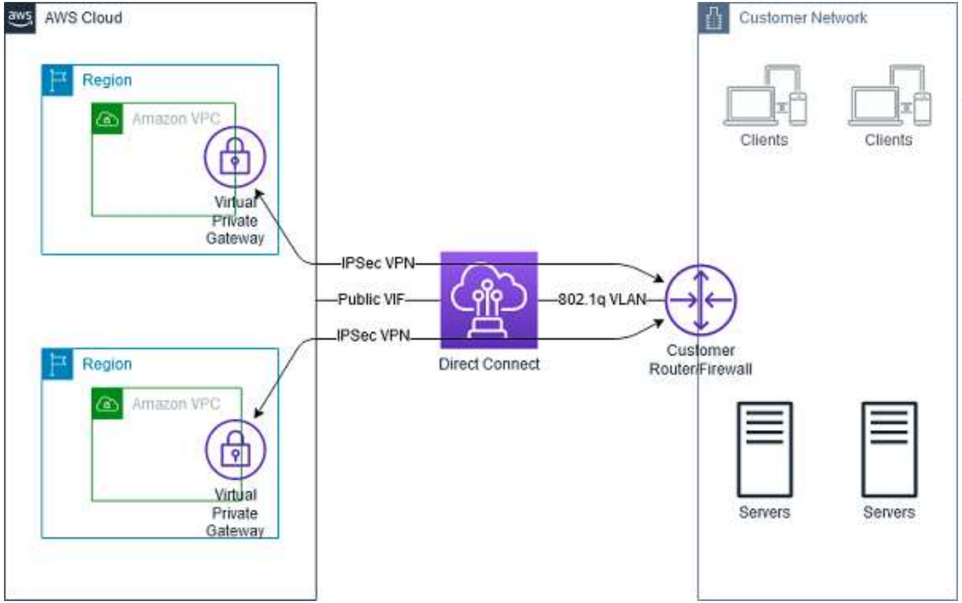
AWS Direct Connect



AWS Direct Connect



AWS Direct Connect



AWS Direct Connect

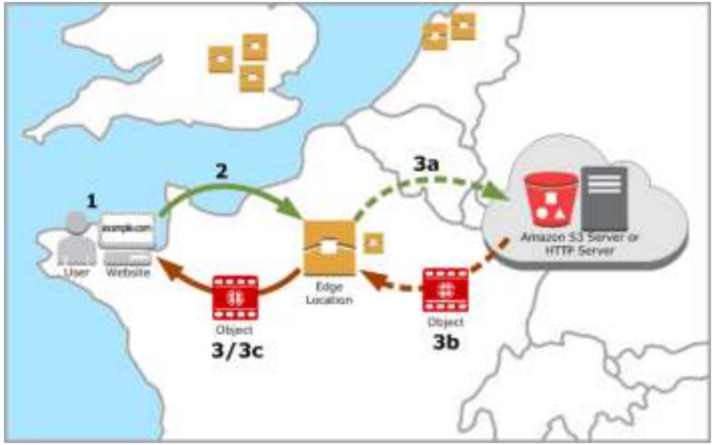
Benefits:

- Dedicated connectivity
- Security
- High bandwidth

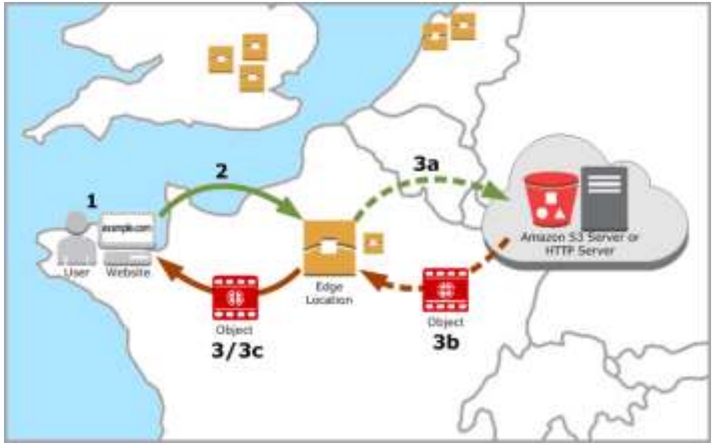
AWS CloudFront

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations.

AWS CloudFront



AWS CloudFront



Web Distribution: Typically used for websites
RTMP: Used for media streaming like Videos.

AWS Route53

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. You can use Route 53 to perform three main functions in any combination:

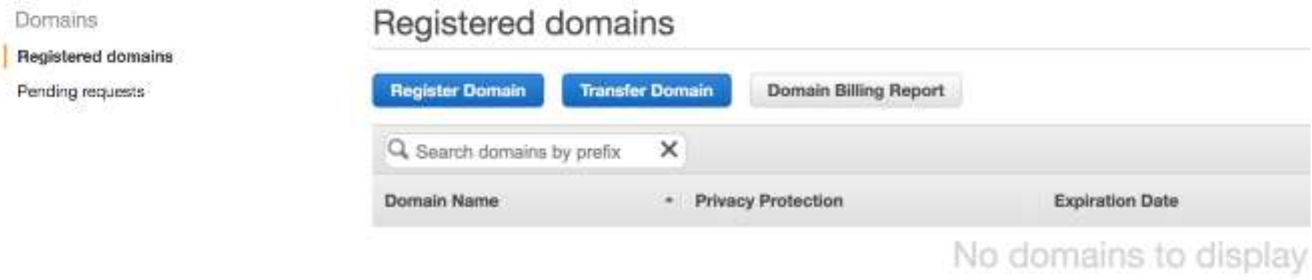
- Domain registration
- DNS routing
- Health checking.

AWS Route53

- Domain registration

AWS Route53

- Domain registration



Domains

Registered domains

Pending requests

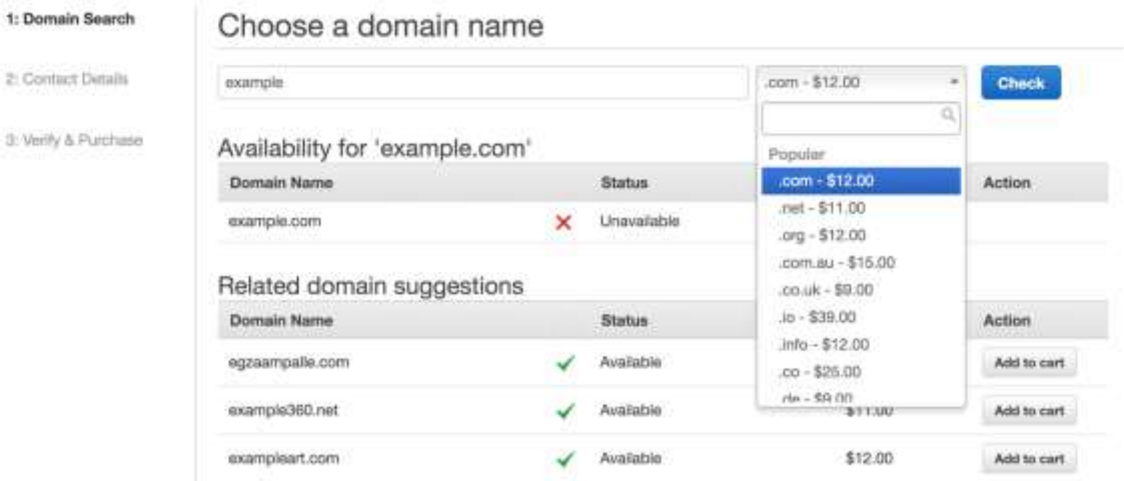
Registered domains

Domain Name	Privacy Protection	Expiration Date

No domains to display

AWS Route53

- Domain registration



1: Domain Search

2: Contact Details

3: Verify & Purchase

Choose a domain name

example | .com - $12.00 | Check

Availability for 'example.com'

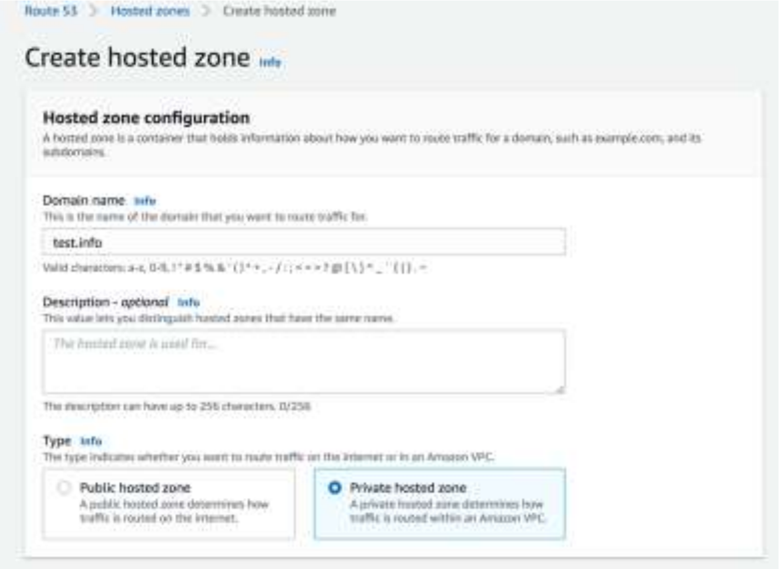
Domain Name		Status		Action
example.com	✗	Unavailable		

Related domain suggestions

Domain Name		Status		Action
egzaampalle.com	✓	Available		Add to cart
example360.net	✓	Available	$11.00	Add to cart
exampleart.com	✓	Available	$12.00	Add to cart

AWS Route53

- Hosted zones



Route 53 > Hosted zones > Create hosted zone

Create hosted zone Info

Hosted zone configuration

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name Info

This is the name of the domain that you want to route traffic for.

test.info

Valid characters: a-z, 0-9, ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } . ~

Description - *optional* Info

This value lets you distinguish hosted zones that have the same name.

The hosted zone is used for...

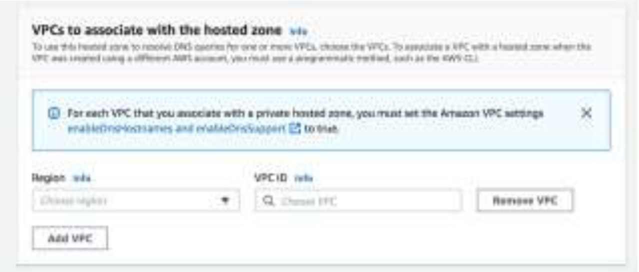
The description can have up to 256 characters. 0/256

Type Info

The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

○ Public hosted zone
A public hosted zone determines how traffic is routed on the internet.

● Private hosted zone
A private hosted zone determines how traffic is routed within an Amazon VPC.



VPCs to associate with the hosted zone Info

To use this hosted zone to resolve DNS queries for one or more VPCs, choose the VPCs. To associate a VPC with a hosted zone when the VPC was created using a different AWS account, you must use a programmatic method, such as the AWS CLI.

For each VPC that you associate with a private hosted zone, you must set the Amazon VPC settings enableDnsHostnames and enableDnsSupport to true.

Region Info: Choose region ▼

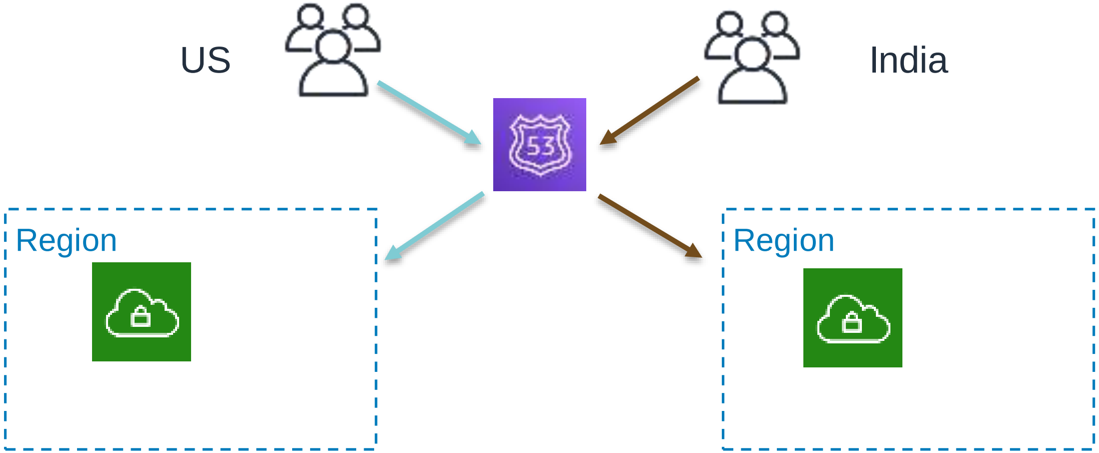
VPC ID Info: Choose VPC

AWS Route53

- DNS routing
  - Geographical routing
  - Failover routing
  - Latency based routing
  - Weight based routing

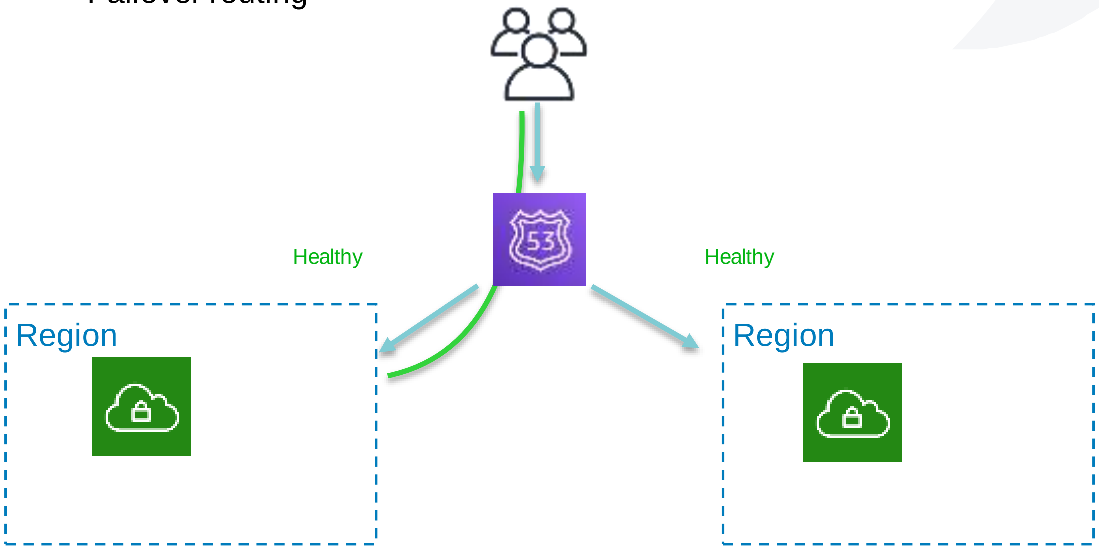
AWS Route53

- Geographical routing



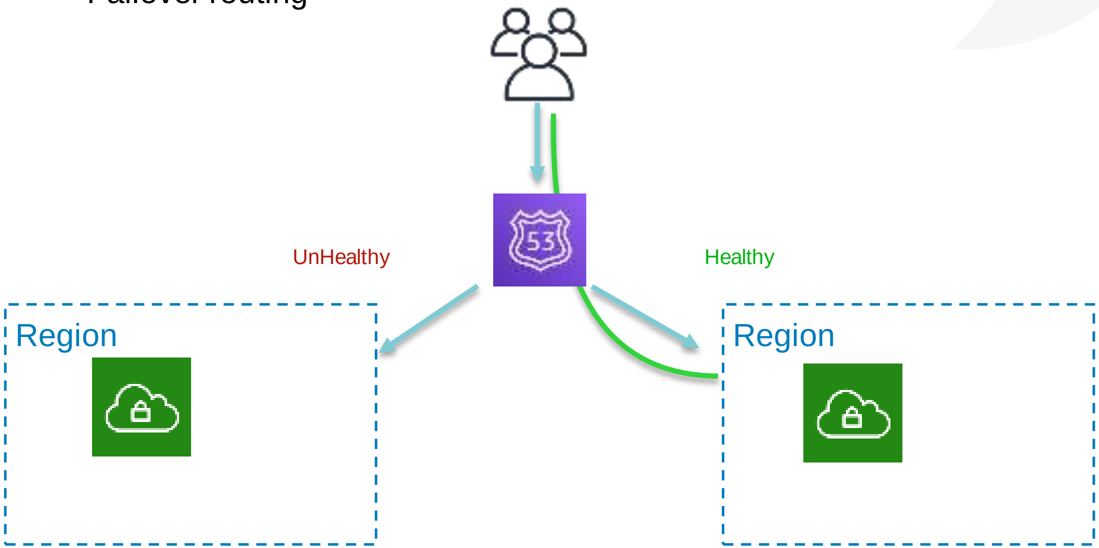
AWS Route53

- Failover routing



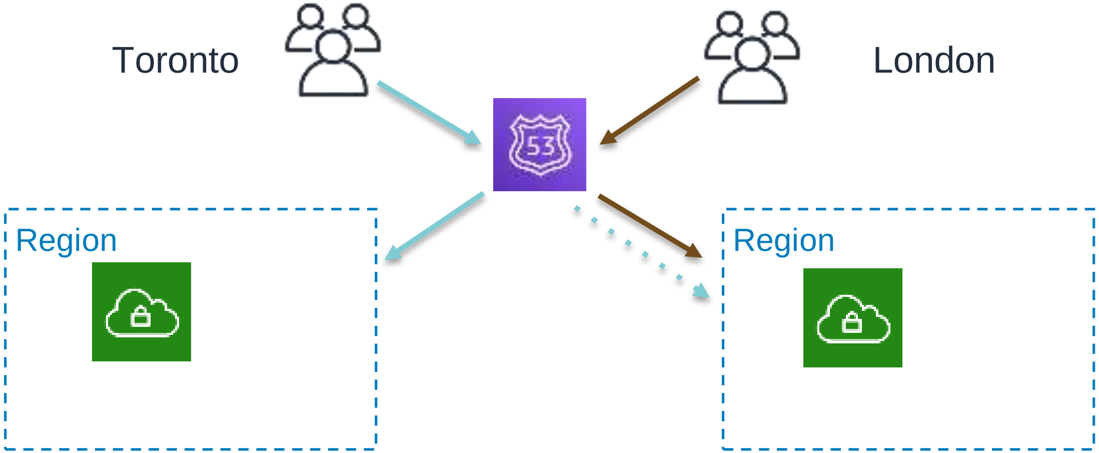
AWS Route53

- Failover routing



AWS Route53

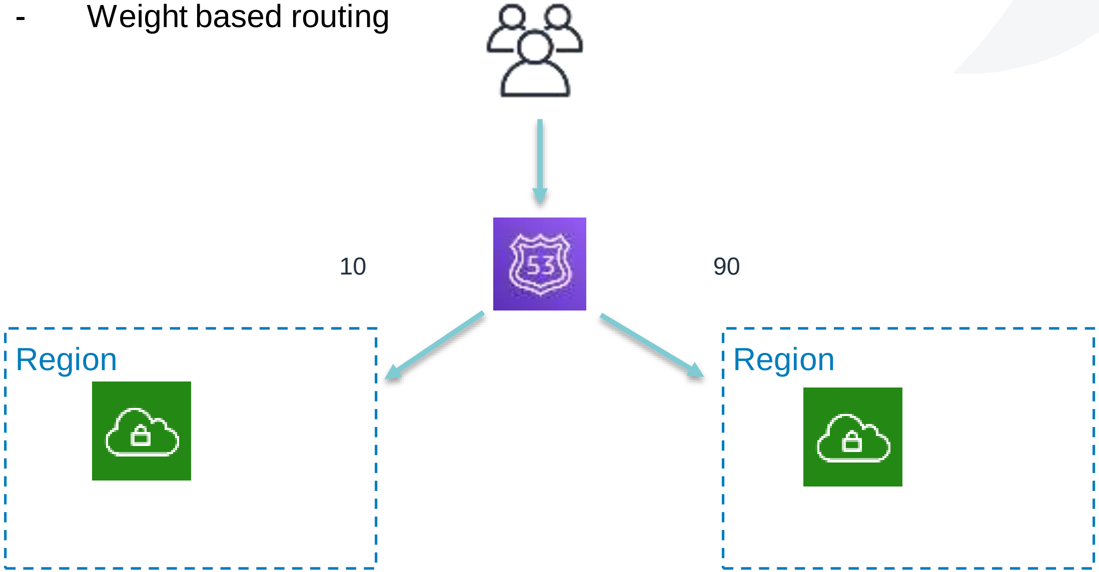
- Latency based routing



The Route 53 DNS servers decide, based on network conditions of the past couple of weeks, which instances in which regions should serve particular users

AWS Route53

- Weight based routing



Andersen

THANK YOU!