NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Coaching - Virtual Private Cloud

Cloud Infrastructure Engineering

Nanyang Technological University & Skills Union - 2022/2023

VPC Overview

You are not expected to know this in-depth but this is an important concept in Cloud.

Summary:

- Explore VPC, Subnets, Internet Gateways & NAT Gateways
- Explore Security Groups, Network ACL (NACLs) & VPC Flow Logs
- VPC Peering & VPC Endpoints
- Site-to-Site VPN & Direct Connect
- Transit Gateway

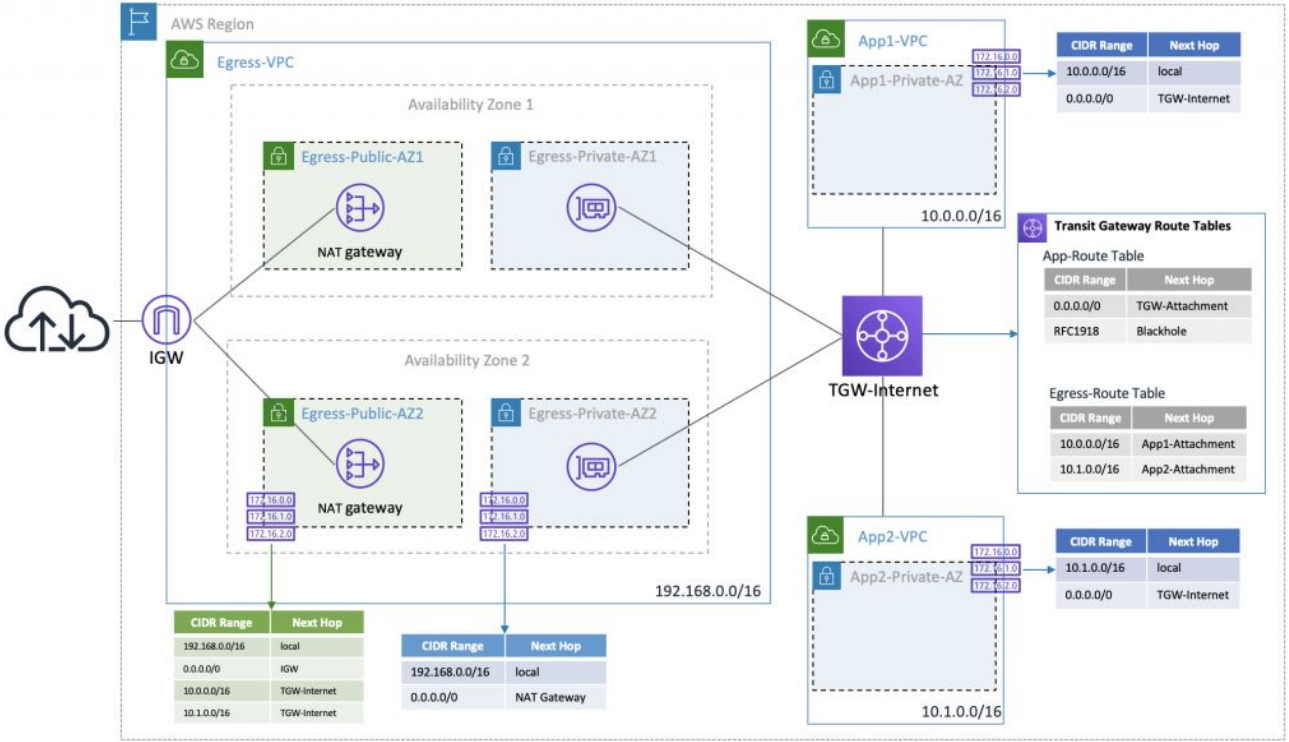
VPC

Amazon Virtual Private Cloud (Amazon VPC) enables you to **launch AWS resources into a virtual network** that you've defined.

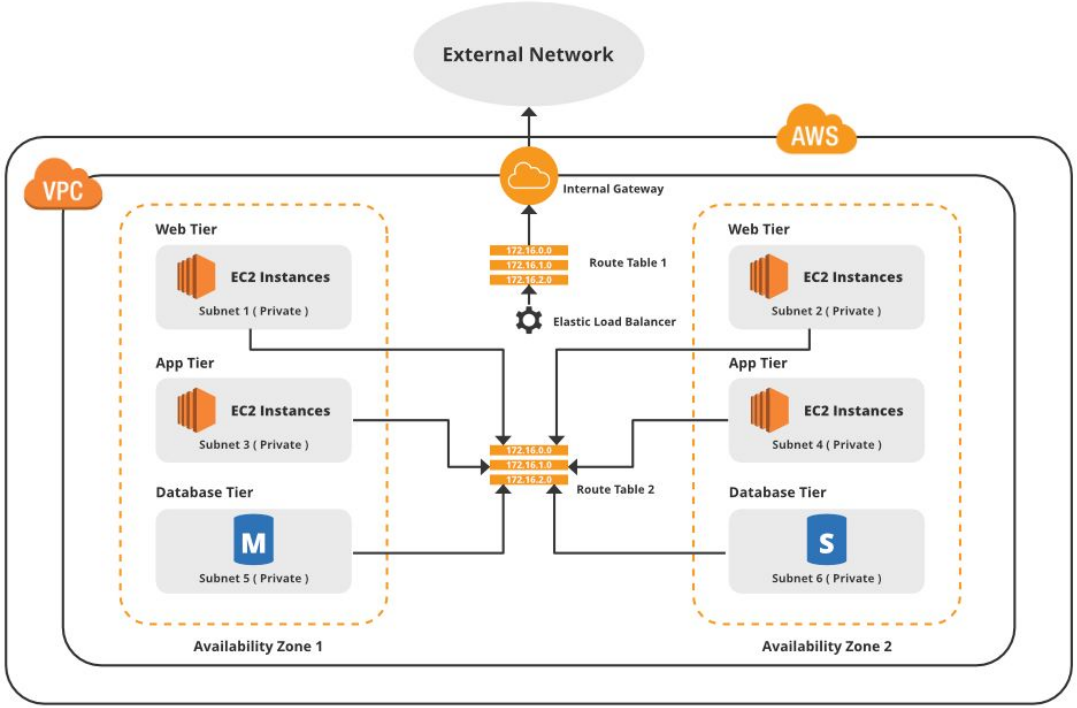
This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

A VPC is **region-specific but multi-AZ**

VPC - Complex


AWS Region
Egress-VPC
Availability Zone 1
Egress-Public-AZ1
NAT gateway
Egress-Private-AZ1
Availability Zone 2
Egress-Public-AZ2
NAT gateway
Egress-Private-AZ2
IGW
192.168.0.0/16
App1-VPC
App1-Private-AZ
10.0.0.0/16
App2-VPC
App2-Private-AZ
10.1.0.0/16
TGW-Internet
Transit Gateway Route Tables
App-Route Table
Egress-Route Table
CIDR Range
Next Hop
192.168.0.0/16 local
0.0.0.0/0 IGW
10.0.0.0/16 TGW-Internet
10.1.0.0/16 TGW-Internet
192.168.0.0/16 local
0.0.0.0/0 NAT Gateway
10.0.0.0/16 local
0.0.0.0/0 TGW-Internet
0.0.0.0/0 TGW-Attachment
RFC1918 Blackhole
10.0.0.0/16 App1-Attachment
10.1.0.0/16 App2-Attachment
10.1.0.0/16 local
0.0.0.0/0 TGW-Internet

VPC - Simple


External Network
AWS
VPC
Internal Gateway
Web Tier
EC2 Instances
Subnet 1 (Private)
172.16.0.0
172.16.1.0
172.16.2.0
Route Table 1
Elastic Load Balancer
Web Tier
EC2 Instances
Subnet 2 (Private)
App Tier
EC2 Instances
Subnet 3 (Private)
App Tier
EC2 Instances
Subnet 4 (Private)
172.16.0.0
172.16.1.0
172.16.2.0
Route Table 2
Database Tier
M
Subnet 5 (Private)
Database Tier
S
Subnet 6 (Private)
Availability Zone 1
Availability Zone 2

VPC - Creating

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

- (●) VPC only
- ( ) VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

my-personal-vpc-1

IPv4 CIDR block Info

- (●) IPv4 CIDR manual input
- ( ) IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.20.4.0/32

IPv6 CIDR block Info

- (●) No IPv6 CIDR block
- ( ) IPAM-allocated IPv6 CIDR block
- ( ) Amazon-provided IPv6 CIDR block
- ( ) IPv6 CIDR owned by me

Tenancy Info

Default

Default VPC

AWS will provide you with a default VPC, but it is good practice to create custom VPCs for your applications.

Why?

Security - You can leverage the **enhanced security options** in Amazon VPC to provide **more granular access to and from the Amazon EC2** instances in your virtual network.

Greater Control - You define your own network space, and **control how your network and the Amazon EC2 resources inside your network are exposed** to the Internet.

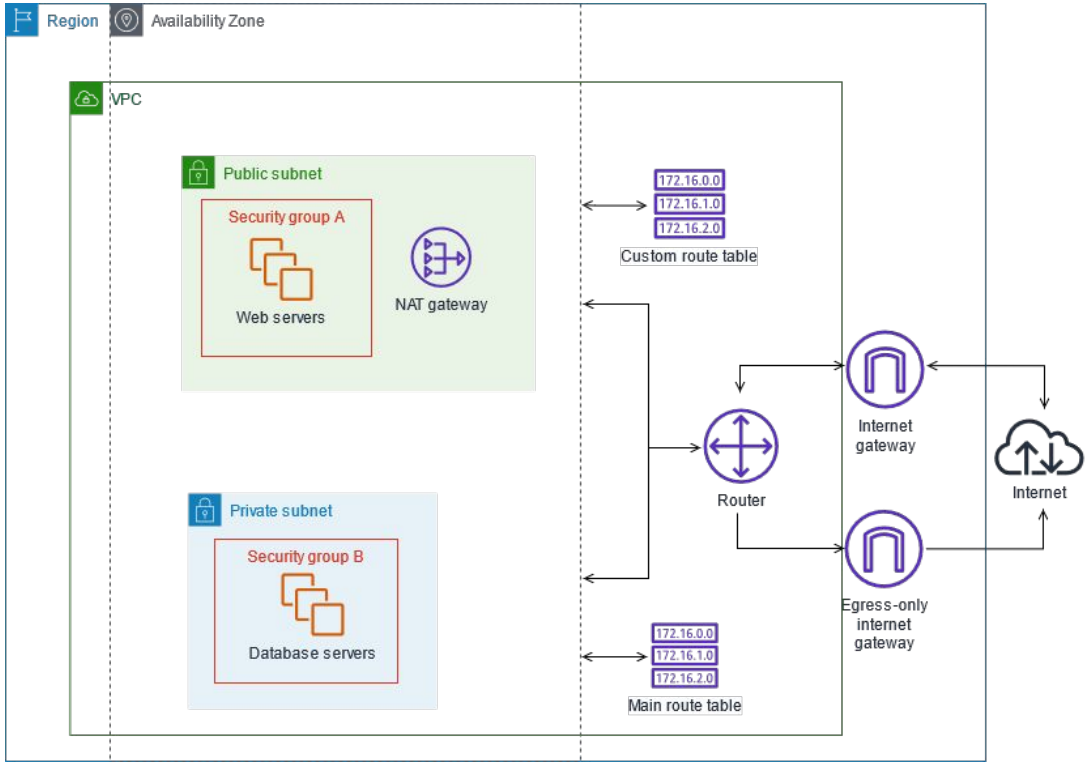
Subnets

A subnet is a range of IP addresses in your VPC.

A subnet must reside in a **single Availability Zone**.

After you add subnets, you can deploy AWS resources in your VPC.

Subnets

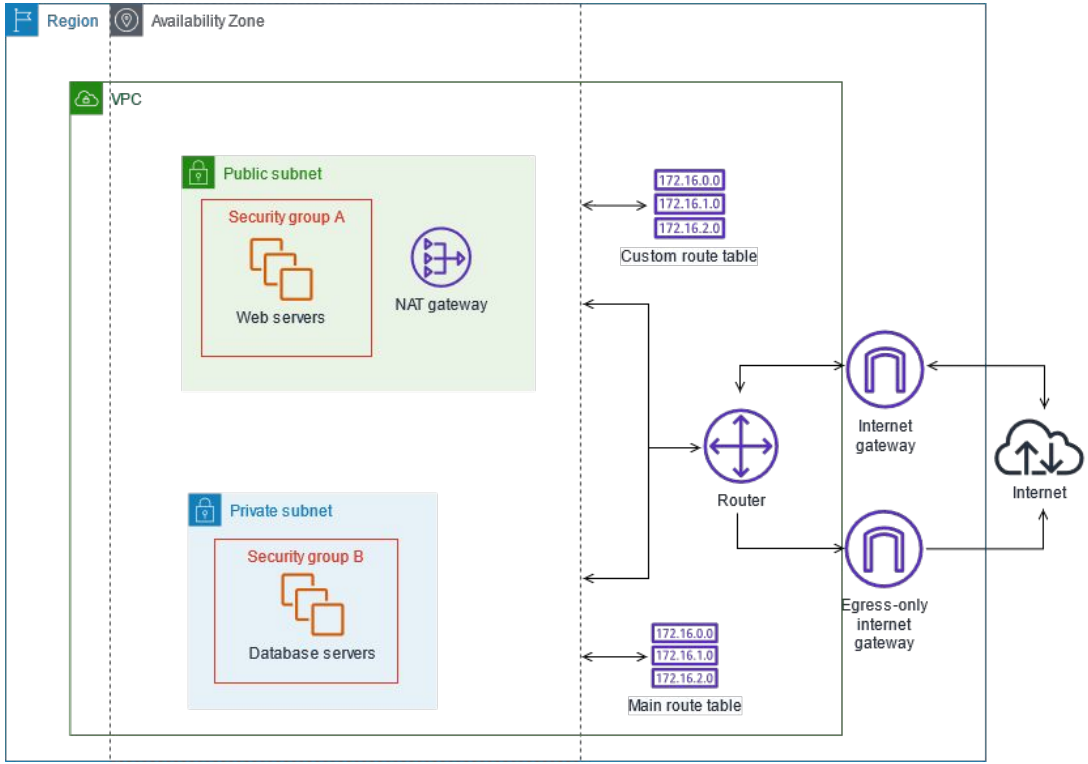

Region
Availability Zone
VPC
Public subnet
Security group A
Web servers
NAT gateway
172.16.0.0
172.16.1.0
172.16.2.0
Custom route table
Internet gateway
Router
Internet
Private subnet
Security group B
Database servers
Egress-only internet gateway
172.16.0.0
172.16.1.0
172.16.2.0
Main route table

Subnets

Public Subnet - The instances in the public subnet can send outbound traffic directly to the internet.

Private Subnet - The instances in the private subnet can't send outbound traffic directly to the internet. Instead, the instances in the private subnet can access the internet by using a **network address translation (NAT) gateway** that resides in the public subnet

Subnets


Region
Availability Zone
VPC
Public subnet
Security group A
Web servers
NAT gateway
172.16.0.0
172.16.1.0
172.16.2.0
Custom route table
Internet gateway
Router
Internet
Private subnet
Security group B
Database servers
Egress-only internet gateway
172.16.0.0
172.16.1.0
172.16.2.0
Main route table

Subnets

Public Subnet - Web Servers, Application Servers

Private Subnet - Database Servers, Private Compute Instances

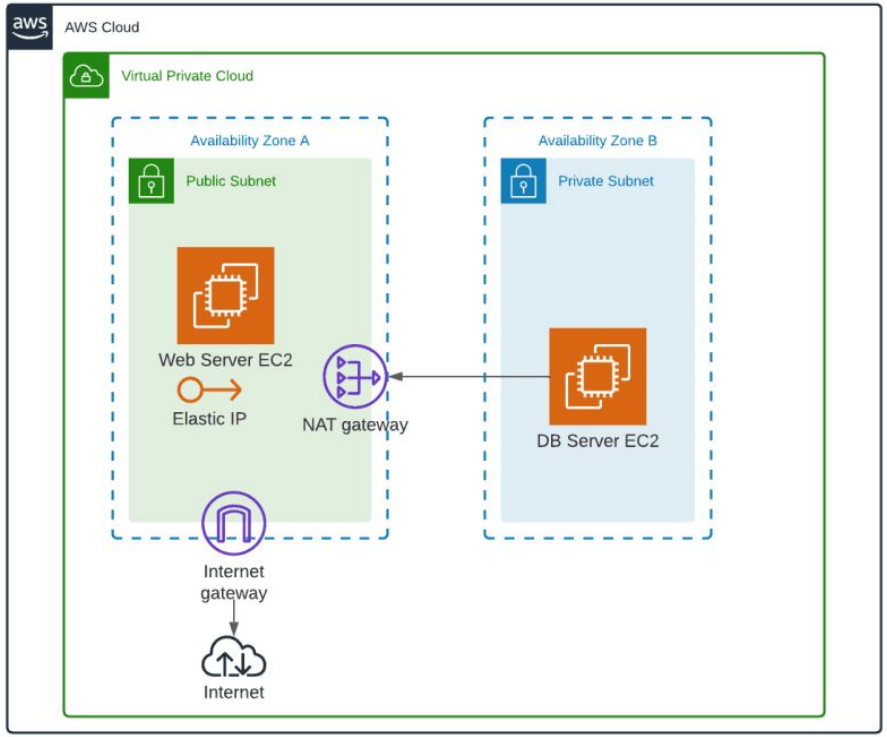
Internet & NAT Gateway

Internet Gateways **helps our VPC instances connect with the internet**

*** Public Subnets have a route to the internet gateway

NAT Gateways (AWS-managed) & NAT Instances (self-managed) **allow your instances in your Private Subnets to access the internet while remaining private**

Internet & NAT Gateway



Network ACL & Security Groups

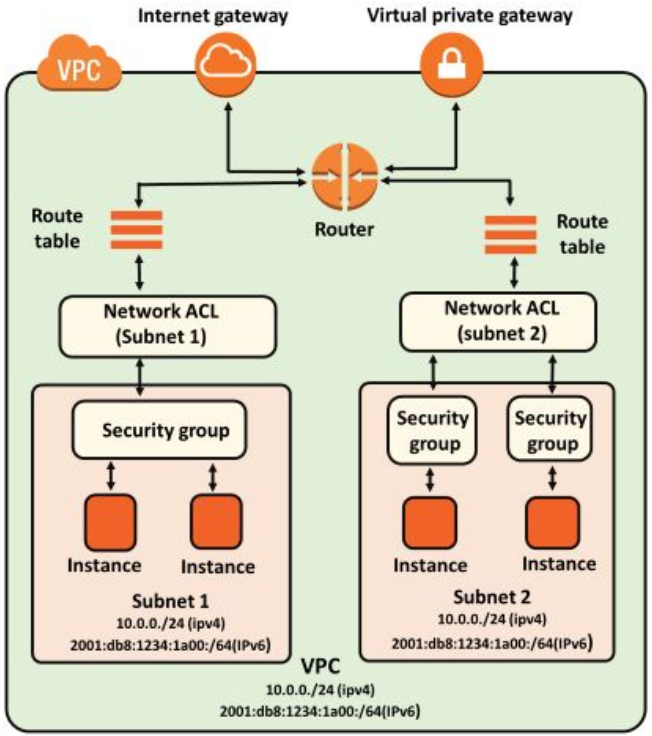
NACL (Network ACL)

- A **firewall** which controls traffic from and to subnet
- Can have **ALLOW** and **DENY** rules
- Are attached at the Subnet level
- Rules only include IP addresses

Security Groups

- A firewall that controls traffic to and from an ENI / an EC2 Instance
- Can have only ALLOW rules
- Rules include IP addresses and other security groups

Network ACL & Security Groups



Network ACL & Security Groups

NACL

Summary | Inbound Rules | Outbound Rules | Subnet Associations | Tags

Network ACL ID: acl-3bc28741
Associated with: 6 Subnets
Default: yes
VPC: vpc-c3b6aeb8

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

View: All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

View: All rules

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Summary | Inbound Rules | Outbound Rules | Subnet Associations

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-4ec11e29	172.31.0.0/20	-
subnet-bf6c0cf5	172.31.16.0/20	-
subnet-494a9715	172.31.32.0/20	-
subnet-93ae369c	172.31.48.0/20	-
subnet-576a8769	172.31.64.0/20	-
subnet-899c42a7	172.31.80.0/20	-

Network ACL & Security Groups

Create Security Group | Actions

Filter by tags and attributes or search by keyword

1 to 3 of 3

Name	Group ID	Group Name	VPC ID	Description
RDS Databases	sg-2805c95e	Periscope_DBs	vpc-2ccc1557	Test Group for testing conne…
RDS SSH Tunnels (EC2)	sg-3124e847	Periscope_Inbound	vpc-2ccc1557	Rules for connecting to the S…
Default Group	sg-77856b01	default	vpc-2ccc1557	default VPC security group

Security Group: sg-3124e847

Description | Inbound | Outbound | Tags

Edit

Type	Protocol	Port Range	Source	Description
All traffic	All	All	54.236.224.46/31	Periscope IP
All traffic	All	All	107.23.195.228/30	Periscope IP

Network ACL & Security Groups

Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (therefore, you don't have to rely on users to specify the security group)

VPC Flow Logs

Capture information about IP traffic going into your VPC & services

Helps you **monitor & troubleshoot VPC issues**, including:

- Connectivity between subnets to internet
- Connectivity between subnets to subnets
- Connectivity between internet to subnets

VPC Flow logs data can be pushed to **S3** or **CloudWatch**

VPC Flow Logs

AWS Services Edit

Dashboard
Alarms
ALARM
INSUFFICIENT
OK
Billing
Logs
Metrics
Selected Metrics
EBS
EC2

Log Groups > Streams for MyFirstFlowLog > Events for eni-30076669-all

Filter

Date/Time: 2015/06/08 16 : 43 : 02 Local (GMT-07:00)

Event Data

```
2 493062987015 eni-30076669 107.170.242.27 172.31.8.238 123 123 17 1 76 1433806982 1433807038 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 107.170.242.27 123 123 17 1 76 1433806982 1433807038 ACCEPT OK
2 493062987015 eni-30076669 79.33.7.58 172.31.8.238 54517 23 6 3 180 1433807174 1433807218 REJECT OK
2 493062987015 eni-30076669 71.6.135.131 172.31.8.238 15314 21379 6 1 40 1433807224 1433807278 REJECT OK
2 493062987015 eni-30076669 172.31.8.238 108.61.56.35 123 123 17 1 76 1433807281 1433807338 ACCEPT OK
2 493062987015 eni-30076669 108.61.56.35 172.31.8.238 123 123 17 1 76 1433807281 1433807338 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 23.226.142.216 123 123 17 1 76 1433807350 1433807398 ACCEPT OK
2 493062987015 eni-30076669 188.138.1.218 172.31.8.238 40082 26 6 1 40 1433807350 1433807398 REJECT OK
2 493062987015 eni-30076669 23.226.142.216 172.31.8.238 123 123 17 1 76 1433807350 1433807398 ACCEPT OK
2 493062987015 eni-30076669 50.116.38.167 172.31.8.238 123 123 17 1 76 1433807411 1433807458 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 50.116.38.167 123 123 17 1 76 1433807411 1433807458 ACCEPT OK
2 493062987015 eni-30076669 107.170.242.27 172.31.8.238 123 123 17 1 76 1433807529 1433807579 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 107.170.242.27 123 123 17 1 76 1433807529 1433807579 ACCEPT OK
2 493062987015 eni-30076669 116.211.0.90 172.31.8.238 46373 8080 6 1 40 1433807648 1433807699 REJECT OK
2 493062987015 eni-30076669 222.122.52.157 172.31.8.238 58354 22 6 3 180 1433807894 1433807999 REJECT OK
2 493062987015 eni-30076669 199.217.117.85 172.31.8.238 5064 5060 17 1 443 1433807944 1433807999 REJECT OK
2 493062987015 eni-30076669 107.170.242.27 172.31.8.238 123 123 17 1 76 1433808069 1433808119 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 107.170.242.27 123 123 17 1 76 1433808069 1433808119 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 108.61.56.35 123 123 17 1 76 1433808310 1433808359 ACCEPT OK
```

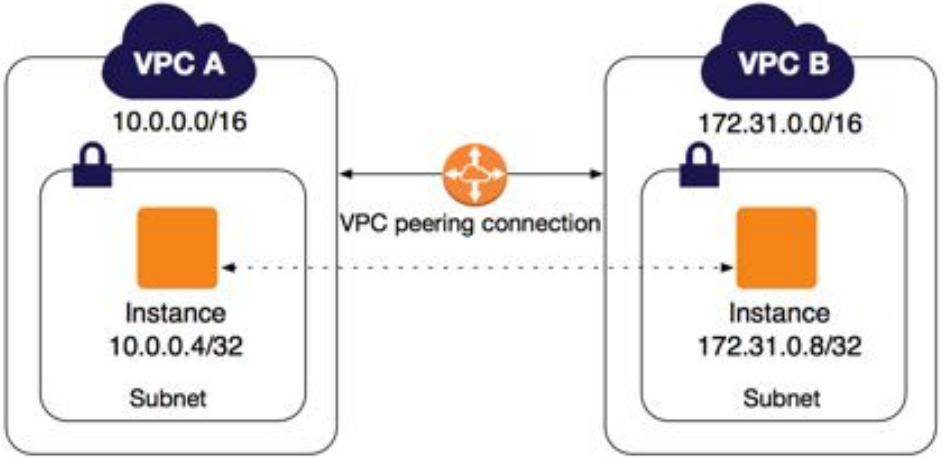
VPC Peering

Allows you to connect two VPCs privately in AWS

Must not have overlapping CIDR or IP Address Range

VPC Peering connection needs to be established for all VPCs needed to communicate with one another

VPC Peering


VPC A
10.0.0.0/16
Instance
10.0.0.4/32
Subnet
VPC peering connection
VPC B
172.31.0.0/16
Instance
172.31.0.8/32
Subnet

VPC Endpoints

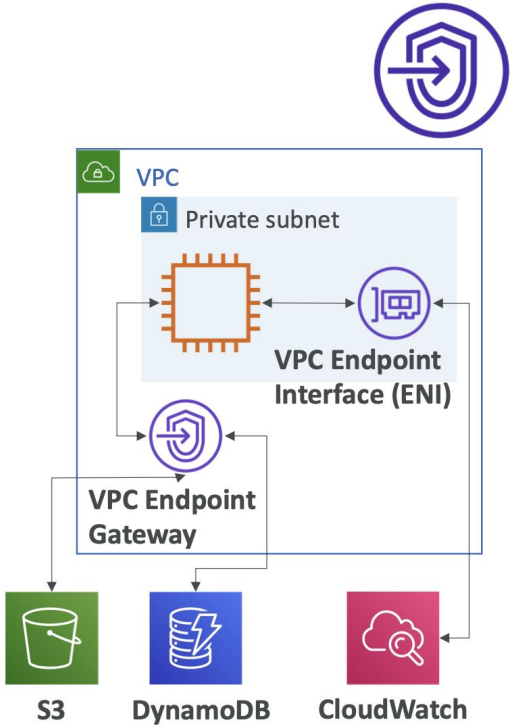
Allows you to connect to internal AWS services using a private network instead of the public internet network

Gives you better security control & lower latency to access these services

VPC Endpoint Gateway: S3 & DynamoDB

VPC Endpoint Interface: Everything else

VPC Endpoints



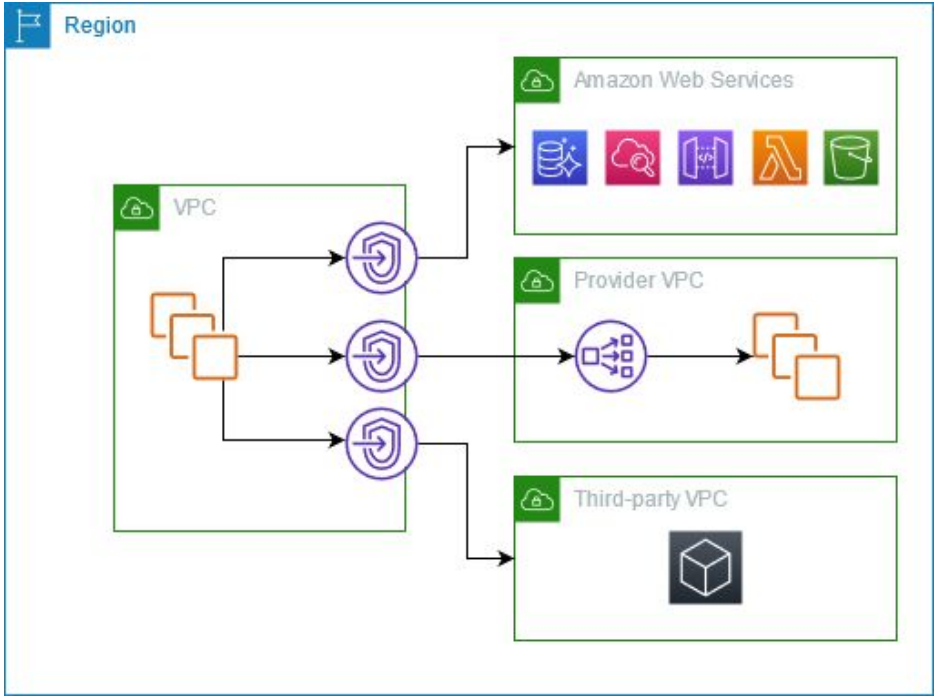
PrivateLink

Most secure & scalable way to expose a service to 1000s of VPCs

Does not require VPC peering, internet gateway, NAT, route tables…

Requires a network load balancer (Service VPC) and ENI (Customer VPC)

PrivateLink



Site-to-Site VPN & Direct Connect

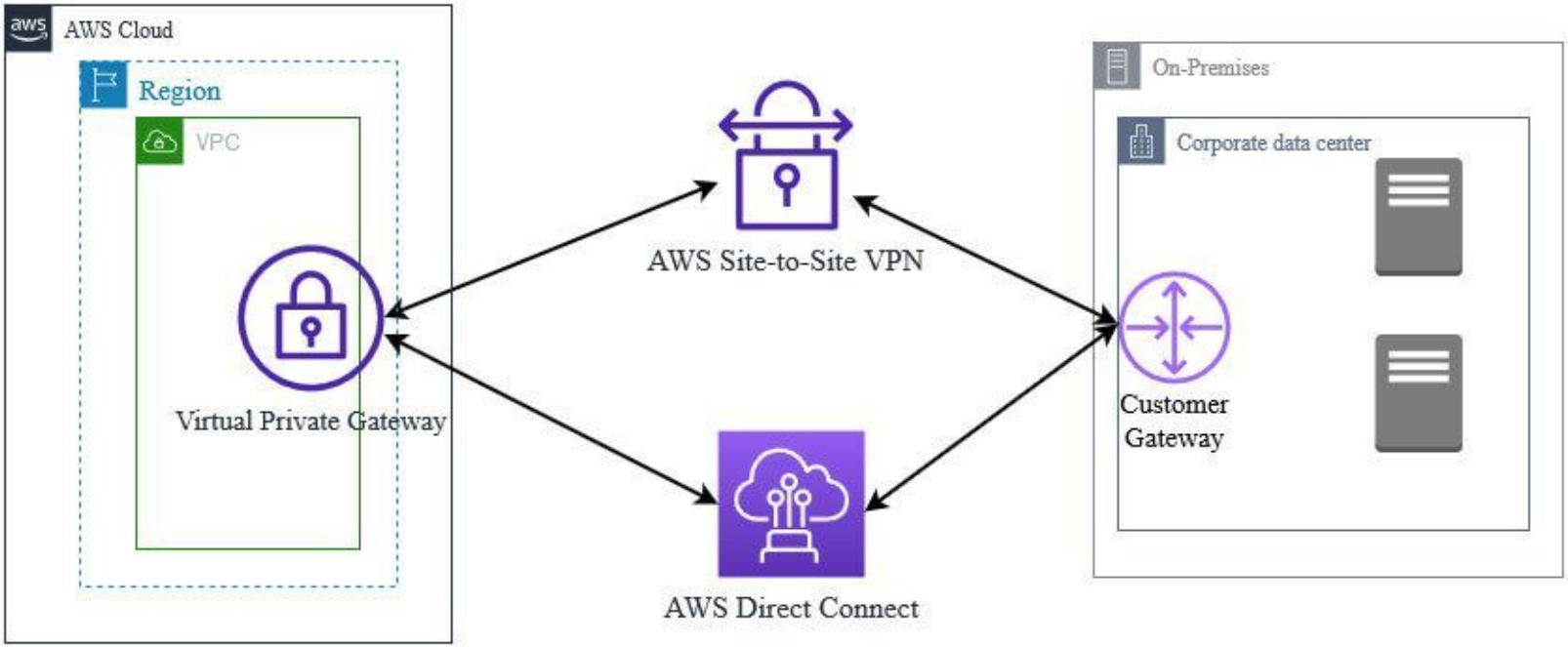
Site to Site VPN

- Connect an on-premises VPN to AWS
- The connection is automatically encrypted
- Goes over the **public internet**

Direct Connect (DX)

- Establish a physical connection between on-premises and AWS
- The connection is **private, secure and fast**
- Goes over a private network
- Takes at least a month to establish

Site-to-Site VPN & Direct Connect



Transit Gateway

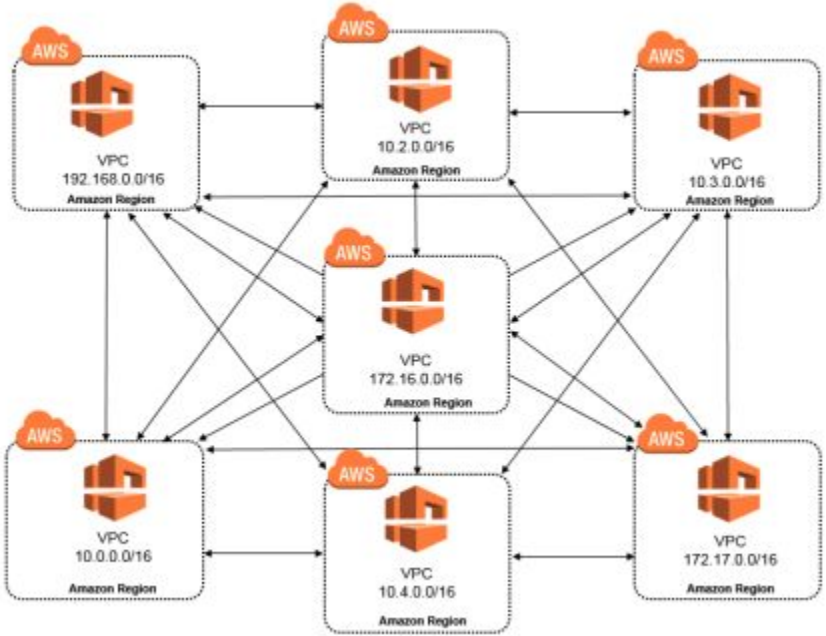
Imagine having to manage peering between thousands of VPCs…

It is much easier to use Transit Gateway to **enable transitive peering** between thousands of VPC and on-premises, **hub-and-spoke (star) connection**

One single Gateway can provide this connectivity

Works with Direct Connect Gateway, VPN connections

Transit Gateway



Transit Gateway