#CIDR – Classless Inter-Domain Routing

无类别域间路由：一个用于给用户分配IP地址以及在互联网上有效地路由IP数据包的对IP地址进行归类的方法。

Graphical user interface, text, application

Description automatically generated

Private IP can only allow certain values

#Defult VPC Overview

Create a private VPC--- CIDR ---- Add subnet

#Subnet – Ipv4

AWS reserve 5 IP address in each Subnet

\*\*\*\*If you need 29 IP address for EC2 instance, you can’t choose a Subnet of size /27 ( 32/IP) ,32-5 < 29

You need ad least 64 Ips.

#Internet Gateways & Route Tables（网关与路由表）

Gateway = 网关

VPC can only have one internet gateway attached

NAT Instance – Network Address Translation

Graphical user interface, text, application

Description automatically generated

#NAt Instance VS NAT Gateway

NAT Gateway disabling source check destination,highly available.Text

Description automatically generated

#DNS Resolution in VPC

DNS –域名系统，DNS（Domain Name Server，域名服务器）是进行域名(domain name)和与之相对应的IP地址(IP address)转换的服务器。

Enable Dnssupport :(DNS Resolution setting)

Enable dnsHostname:=(DNS Hostname setting)

\*\*\* When you do have private Route 53 zones, had have it resole within your vpc.

#Network ACLs & Security Group

!!!!The difference between them.

For network ACL, this is stateless, both inbound rule and outbound rule will be evaluated;

Diagram

Description automatically generated

Network ACLs:

Text

Description automatically generatedTable

Description automatically generated

#VPC peering

从AWS的介绍来看，VPC Peering是一种在区域间共享资源或为实现地理冗余性而复制数据的简单经济且安全的方式；

Connect two VPC

Must update route tables in each VPC’s subnets to ensure instances can communicate.

#VPC Endpoints:

1. Interface
2. Gateway

When run the commands, select the region.

#VPC Flow logs

VPC流日志（Flow Logs）可以捕获经过你的VPC的网络流量（入向和出向），Flow Logs的日志数据保存在Amazon CloudWatch Logs中。 创建了Flow Logs后，你可以在Amazon CloudWatch Logs中查看和检索其数据。

How do you analyze Flow logs?

Athena.

#Bastion Hosts

堡垒主机是网络上专门设计和配置为抵御攻击的专用计算机。

Bastion Host security group must be tightened.

#Sute to Sute VPN

Customer Gateway：

IP address:

Use static, internet-routable IP address for your customer gateway devidce,

If behind a CGW behind NAT(with NAT -T),use the public IP address of the NAT

#Direct Connect(DX)

#Direct Connect Resiliency

High resiliency good for critical workloads

#Egress only internet gateway

Is for IPv6 only

#AWS Private Link(VPC endpoint services)

The most safety way to **expose the service**

these two services have a Gateway endpoint (remember it), all the other ones have an interface endpoint (powered by Private Link - means a private IP)

**No cost for using Gateway Endpoint**

**IPV4 cannot be disabled for your VPC and subnets**

**If you cannot launch an instance an instance in your subnets, it’s not because it cannot acquire an IPv6, because there are no available IPv4 in your subnet, solution, create a new IPV4 CIDR in your subnet.**