Networking - VPC

Uday Manchanda

September 17, 2021

1 CIDR, Private vs Public IP

- CIDR - classless inter-domain routing
- Used for SG rules or networking in general
- Define an IP address range. EX: 0.0.0.0/0 = all ip addresses
- Two components: base ip (xx.xx.xx.xx) and subnet mask (/y)
- base ip represents an ip contained in the range
- subnet masks defines how many bits can change in the IP

1.1 Subnet Masks

- allows part of the underlying IP to get additional next values from the base IP
- /32 allows for 1 IP = 2^0
- /31 allows for 2 IP = 2^1
- /30 = 4 IP = 2^2
- /29 = 8, /28 = 16, /16 = 65,536
- /y = 2^{32-y}
- /32 = no IP can change, /24 = last IP number can change, /16 = last two IP numbers can change, etc
- 192.168.0.0/24 = 192.168.0.0 - 192.168.0.255
- 192.168.0.0/16 = 192.168.0.0 - 192.168.255.255
- 134.56.78.123/32 = 134.56.78.123
- Private IP ranges: 10.0.0.0/8 (big networks), 172.16.0.0/12 (default AWS), 192.168.0.0/16 (home networks)

2 VPC

- VPC = virtual private cloud
- Can have multiple VPCs in a region (max 5)
- Max CIDR per VPC is 5. For each CIDR:
  - Min size is /28 = 16 IPs
  - Max is /16 = 65526 IPs
- Since the VPC is private, only the private IP ranges are allowed

2.1 Default VPC

- All new accounts have a default VPC
- New instances are launched into the default VPC if no subnet is specified
- Default VPC have internet connectivity and all instances have a public IP
- Also get public and private DNS name

2.2 VPC Peering

- connect 2 VPCs privately using the AWS network
- makes them behave as if they were in the same network
- must not have overlapping CIDR
- is not transitive. if A and B are connected, and B and C are connected, A and C are not connected
- can do vpc peering with another aws account
- must update route tables in each VPCs subnets to ensure instances can communicate
- can reference a SG of a peered VPC (for cross account)

2.3 VPC Endpoints

- meant for you to access AWS services within a private network
- via a NACL
- no need to setup all the infrastructure
- two types of endpoints

  - interface: provisions an ENI as an entry point - most AWS services
  - gateway: provisions a target and must be used in a route table (S3, DynamoDB)

- if there are issues: check DNS setting resolution in VPC or check route tables

2.4 VPC Flow Logs

- help you capture information about ip traffic going to your interfaces
- VPC flow logs, subnet flow logs, and ENI flow logs
- data can go to S3/CW logs

3 Subnet

- tied to specific AZs
- 5 IPs are reserved in each subnet (first 4 and last one)
- If you need 29 IP addresses for EC2 instances you can't choose a subnet size of /27 (32 IP) since 5 IPs are reserved
- Need at least 64 IPs, so go for /26

4 Internet Gateways and Route Tables

- Help our VPC instances connect with the internet
- created separately from VPC
- One VPC can only be attached to one IGW and vice versa
- also a NAT for the instances that have a public ipv4
- do not allow internet access on their own, must edit route tables
- if you want an ec2 to have access to the internet
  - edit route table to point to the gateway for a specific IP range
  - ec2 will then get routed directly into the gateway

5 NAT Instances

- allows instances in the private subnets to connect to the internet
- network address translation
- must be launched in a public subnet
- must have elastic IP attached
- route table must be configured to route traffic from private subnets to NAT instance

6 NAT Gateways

- AWS managed NAT, higher bandwidth, better availability, no administration
- created in a specific AZ, cannot be used by an instance in that subnet (only from other subnets)
- requires IGW
- no need to manage SG

6.1 NAT Gateway with High Availability

- resilient within a single AZ
- must create multiple NAT Gateways in multiple AZs for fault tolerance
- no cross AZ failover needed because if a AZ goes down it doesn't need NAT

7 DNS Resolution Options and R53 Private Zones

- DNS resolution in VPC
  - enableDnsSupport - default true
  - enableDnsHostname - default false
- if you use custom DNS domain names in a private zone in r53, you must set both these attributes to true

8 NACL and Security Groups

- NACL = network access control list (subnet level)
- incoming requests are first evalulated by the NACL inbound rules and then the SG inbound rules

- SGs are stateful. so if an inbound rule allows traffic the outbound does as well.
- NACLs are stateless. so if an inbound rule allows traffic the outbound does not necessarily.
- outgoing requests are first evaluated by the outbound rule on the SG and then the outbound rule on the NACL
- they're like a firewall which control traffic from and to subnet
- default nacl allows everything inbound and outbound
- one nacl per subnet, new subnets are assigned default nacl
- nacl rules have a number, higher precedence have lower numbers.

9 Bastion Hosts

- Use to SSH into private instances
- bastion is in the public subnet which is then connected to all other private subnets
- bastion host should only have port 22 traffic from the IP you need

10 Site to Site VPN

- used if you have a corporate data center
- customer gateway on the corporate data center side
- vpn gateway on the vpc side
- site to site vpn links the two

10.1 Virtual Private Gateway

- VPN concentrator on the AWS side of the VPN connection
- VGW (virtual private gateway) is created and attached to the VPC from which you want to create the site to site VPN

10.2 Customer Gateway

- IP address:
  - use static, internet-routable IP address for you customer gateway device
  - if behind a NAT (with NAT-T), use the public IP of the NAT

11 Direct Connect and Direct Connect Gateway

- DX provides a dedicated private connection from a remote network to your VPC
- dedicated connection must be setup between your DC and AWS DX locations
- Set up Virtual private gateway on VPC
- use direct connect gateway to connect to one or more VPCs in different regions (same acct)
- Connection types
  - Dedicated connections - physical ethernet port dedicated to customer, connection requests are made to AWS first and completed by AWS DX partners
  - Hosted Connections - connection requests are made via AWS DX partners

12 Egress Only Internet Gateway

- egress = outgoing
- similar to NAT but for ipv6
- all ipv6 addresses are public
- gives ipv6 instances access to internet but won't be directly reachable by the internet

13 AWS Private Link

- aka vpc endpoint services
- expose services in your VPC to other VPCs. most scalable and secure way

14 Transit Gateway

- for having transitive peering between thousands of VPC and on-premises, hub and spoke (star) connection
- no need to peer the VPCs individually