Data Protection VPC

VPC

default VPC : all subnet has route out to IE
모든서브넷인터넷연결 . 모든EC2주소
each EC2 has pub & private IP주소

VPC 생성시 Custom VPC
IGW는 하나VPC에 할당,
autoassign IP 설정을 Enable하여 EC2의 IP주소를 하면 (By default 하는)

logical Datacenter /w Route table, NACL, Security Group

1 subnet = 1 AZ

10.0.0.0/24
- 10.0.0.0 네트워크주소
- 10.0.0.1 VPC router
- 10.0.0.2 DNS서버
- 10.0.0.3 예약 reserved
- 10.0.0.255 브로드캐스팅

(AWS는 Broadcasting지원안함)

256 − 5 = 251개 주소만 이용가능

Load Balancer

반드시 must have 2개이상의 AZ in VPC to have load balancer.

- TLS/SSL termination on Loadbalancer
  : 로드밸런서가 암복호화담당 → ⊕ offloads the process 등 비용절감 cost effective
  HTTPS이용 / Application LB
- TLS/SSL termination on EC2
  종단간보안 End to End Encryption, TCP이용, NWT/classic LB

VPC peering

VPC 여러개서로연결하는것
private IP이용 / STAR configuration
1:1 연결 (방사형불가능)
(NO TRANSITIVE)

VPC Flow log는 같은계정의 peering만가능

VPC Flow Logs ★

Flow logs are stored using cloudwatch Logs

Flow(VPC) Log기 기록되지않는것들
- DNS (AWS) 트래픽
- metadata instance
- windows license activation트래픽
- DHCP request 트래픽
- reserved IP주소 2 VPC라우터로의 트래픽

- 같은계정의 peered된 VPC만 log가능
- can't tag a flow log 태깅불가능
- 한번 생성되면, can't change the config 변경불가능

NAT & Bastion

NAT : provides Internet traffic to Private subnet's EC2

Bastion : Jump server (SSH/RDP) for administration to securely access to "

NAT instance VS NAT G/W

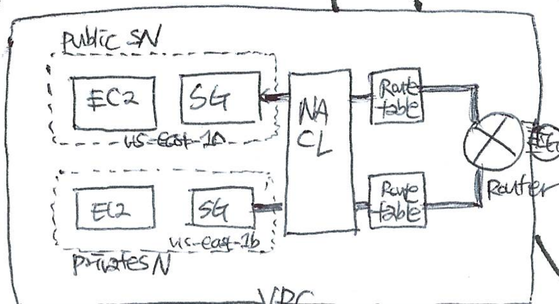
Private subnet의 EC2가 OS 패치 등을 해야할때 필요한 옵션

NAT instance ★

- Disable src / dst check
- Behind security groups
- must be in public subnet
- must have a route out of private SN to NAT instance
- 인스턴스 종류에 따라 가용성이 다름
- 가용성 높이는 방법 : 멀티 subnet 멀티 AZ, autoscaling, a script for automate failover

NAT G/W

- 가용성 높은, more secure
- 터널링 안해도, AWS manage
- auto scaling automatically up to 10Gbps
- no need to disable src / dst check
- 멀티AZ로 redundancy
- NAT 할당은 AZ 다면 안됨
- no association /w SG



Public SN의 EC2가 Private SN의 EC2로 ssh가 가능한 이유는 EC2의 S.G가 ssh를 allow했기 때문

NACL VS Security Group

NACL

- Default NACL allow all, 특정 IP주소막기
- Custom NACL's default ✱ All Traffic Deny
- 각각의 subnet은 NACL과 연결되어 (아니면 자동으로 default NACL)
- 한개 이상의 Subnet : 1개 NACL / Support Allow & DENY
- Stateless. (inbound / outbound) rules needed
- allow ephemeral ports for outbound rules
- 오버한 (규칙)가 적은 숫자 순서대로. 100 > 200 순서대로 / 2nd layer defense

Security Group

- Stateful (인바운드만설정해도 O.K)
- automatic apply to outbound rules
- only support allow rules
- 1 layer of defense

VPC Endpoint

AWS의 서비스들과 연결할 수 있게 프라이빗 / privately connect from VPC to AWS SVC

interface endpoint / G/W endpoint

- 인터페이스 endpoint : Elastic net interface /w private IP주소 이용 (타깃서비스이용)
- 게이트웨이 endpoint : gateway you specify as a target for a route in a route table. (S3, DynamoDB)

Custom DNS SVR /w VPC

- AWS DNS SVR
  used one of IP주소 10.0.0.2
- VPC생성시 자동으로 Amazon DNS사용설정
- DNS resolution setting, uncheck it (disable AWS DNS 서버)
- create new DHCP option sets & custom DNS