* Introduction to AWS Security Group
- 인스턴스의 방화벽과 같은 역할을 함
- Stateful : 'Status'가 저장되므로 외부에서 온 요청과 그에 대한 응답은 인바운드만을, 내부에서 나간 요청과 그에 대한 응답은 아웃바운드의 영향을 받음
- 인스턴스당 최대 5 개의 Security group 적용 가능
    - 5 개 모두 적용됨
- 변경사항은 즉시 적용됨
- Outbound rule 은 기본적으로 '모두 허용'
    - 접속하고자 하는 주체가 인스턴스이므로 막을 이유가 없음
- 허용 규칙만이 존재함
- 인스턴스 자체에 적용되는 것이 아닌 인스턴스의 Elastic Network Interface 에 적용됨

* Security Group and Network ACL
- Security Group 과 달리 Network ACL 은 Stateless
- Network ACL 은 'Status'에 대한 이해가 없으므로 어느 트래픽이든 인바운드, 아웃바운드 모두 적용
- Network ACL 을 새롭게 생성시 인바운드,아웃바운드 모두 거부 상태

* Instance Metadata
- EC2 에 대한 정보
- Security group 은 EC2 인스턴스 자체를 보호하는 방화벽이기에 Metadata 까지 보호하지 않음
- 인스턴스 OS 단에서 보호 수단을 강구해야 함

* Virtual Private Gateway(VGW)
- 리전당 최대 5 개까지 생성 가능
- VPC 에 장착됨
- 기본적으로 가용성이 보장됨
- VGW 생성시 자동으로 Routing table 에 추가됨

* VPC Endpoint to connect AWS Public Service
- VPC 내 Resource 들이 Non-VPC Resource 혹은 API 와 통신하기 위한 목적
- AWS 의 Public Service 를 Internet Gateway 가 아닌 Amazon Private Network 를 통해 이동하게 하는 서비스
- PrivateLink 로 구동되는 Interface Endpoint 와 Gateway Endpoint 로 나뉘며 S3 와 DynamoDB 만이 Gateway Endpoint 를 사용

- VPC Interface Endpoint 생성시 지정한 Subnet 마다 인터페이스가 생기며, 인터페이스를 통해 Non-VPC 서비스 접근
- VPC Gateway Endpoint 생성시 자동으로 Routing table 에 추가되며 Gateway 를 통해 Non-VPC 서비스 접근
- Interface Endpoint 의 경우 다음과 같은 설정 필요
    - Private DNS name enable 활성화를 설정하여 Private VPC Endpoint 를 통해서 접근하도록 해야 함
    - Security group 설정
    - Routing 설정 불필요
- Gateway Endpoint 의 경우 다음과 같은 설정/제한 사항 존재
    - VPC 에서 'DNS 확인'을 활성화해야 함
    - 엔드포인트에 지정된 서비스에 대한 아웃바운드 트래픽을 허용/거부하기 위해 ACL 아웃바운드 규칙에 AWS 접두사 목록을 사용할 수 없음, CIDR 블록으로 대체해야 함
    - 엔드포인트는 VPC 와 연결되는 엔드포인트가 동일한 리전에 있어야 함
    - IPv4 트래픽만 지원함
    - 엔드포인트는 VPC 외부로 확장되지 않음, VPN 연결, Peering 연결, Transit gateway, Direct connect 등을 통해 엔드포인트 서비스의 리소스와 연결할 수 없음

* AWS Web Application Firewall(WAF)
- API Gateway, Cloudfront 혹은 ALB 에 적용 가능
- API 를 통해 관리 가능
- 관리 규칙이 AWS 보안팀에 의해 지속적으로 최신화됨

* VPC Flow Logs
- AWS VPC 의 네트워크 인터페이스에서 송/수신되는 네트워크 트래픽 정보를 수집하여 CloudWatch Log 에 저장하는 기능
- 다음과 같은 작업에 활용 가능
    - 지나치게 제한적인 보안 그룹 규칙 진단
    - 인스턴스에 도달하는 트래픽 모니터링
    - 네트워크 인터페이스를 오가는 트래픽 방향 결정
- VPC Flow Logs 를 생성한 후 이를 CloudWatch Log 의 Log Group 에 연결해야 함
- VPC, Sunbet, EC2 에서 생성 가능
- 허용/거부된 트래픽 모두 확인가능
- 로그는 10 분마다 발행됨
- Flow Logs 는 생성 후 변경 불가능
- 실시간 확인이 아닌 기록을 확인하는 것
- IAM 을 통해 CloudWatch Logs 로의 전송을 허용하지 않을 수 있음

- 각 Elastic Network Interface 는 고유의 Log Stream 을 가짐
- Flow Logs 에 잡히지 않는 트래픽
    - AWS DNS Server 로 가는 트래픽
    - 윈도우 인스턴스 라이센스를 활성화하기 위한 트래픽
    - DHCP 트래픽
    - Default VPC router 의 예약 주소로 가는 트래픽