* Security Group
- VPC 내 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상의 방화벽
- 서브넷 수준이 아닌 인스턴스 수준에서 작동하기 때문에 각 인스턴스를 서로 다른 보안그룹으로 지정할 수 있음
- 기본적으로 모든 인바운드 트래픽을 거부하고 모든 아웃바운드 트래픽을 허용
- 인스턴스당 최대 5개의 보안그룹을 설정할 수 있음
- 보안그룹의 가장 큰 특성은 이른바 'Stateful'로 인바운드 트래픽과 아웃바운드 트래픽에 별도의 규칙을 지정할 수 있는 것
- 예를 들어 인바운드에는 HTTP(80) 포트가 허용되어 있으나 아웃바운드에 없는 경우 HTTP 트래픽이 '외부에서 들어왔다가 나갈 때' 전혀 지장이 없음
- 허용 규칙만 존재하며 거부 규칙이 존재하지 않음
- Source IP, Protocol, Port 등을 설정할 수 있음
- 설정 변경시 즉시 적용됨

* Network ACL
- 서브넷 내부와 외부의 트래픽을 제어하기 위한 가상 방화벽으로 네트워크 스위치의 ACL과 역할이 같음
- 서브넷의 가상 방화벽이기 때문에 서브넷에 속한 모든 인스턴스가 영향을 받음
- 기본적으로 모든 인바운드와 아웃바운드 트래픽을 허용함
- 하나의 ACL은 다수의 서브넷과 연결될 수 있으며, 하나의 서브넷은 하나의 ACL만 연결됨
- Network ACL의 가장 큰 특징은 'Stateless'로서 인바운드 규칙과 아웃바운드 규칙이 서로 영향을 줌
- 예를 들어 인바운드에는 HTTP(80) 포트가 허용되어 있으나 아웃바운드에 없는 경우, HTTP 트래픽이 '외부에서 들어왔다가 나갈 때' 아웃바운드 통신이 되지 않음
- 허용과 거부 모두 가능
- Security Group과 달리 우선순위 값이 존재하며 가장 작은 값이 가장 높은 우선순위를 가지고 우선순위부터 순서대로 적용됨
- 설정 변경시 즉시 적용됨

* Security Group vs Network ACL
- Security Group은 'Stateful', Network ACL은 'Stateless'
- Security Group은 허용만 가능, Network ACL은 허용 및 거부 가능
- Security Group은 규칙 리스트에 있는 것 중 적용, Network ACL은 우선순위에 따라 우선 규칙 적용
- Security Group은 인스턴스의 가상 방화벽, Network ACL은 서브넷의 가상 방화벽

* VPC Peering
- 두 VPC 간의 트래픽을 전송하기 위한 기능
- Source VPC와 다른 리전의 VPC를 Destination으로 선택하여 Peering 요청을 보낸 후, 수락시 Peering 가능
- 요청과 수락이 필요한 이유는 다른 계정의 VPC도 연결 가능하기 때문
- Peering 생성 후 라우팅 테이블에 해당 Peering을 집어넣으면 통신 시작
- VPC Peering은 Transit Routing 불가(Transit Routing : 2개의 VPC가 한 개의 중간다리 VPC를 통해 통신하는 것)

* Transit Gateway
- On-Premise와 VPC를 연결하는데 사용되는 Gateway
- Direct Connect와 같은 전용선 서비스와 Site-to-Site VPN 또한 이 Transit Gateway를 통해 VPC를 연결함
- Virtual Private Gateway는 한 개의 VPC만을 연결할 수 있지만 Transit Gateway는 다수의 VPC를 연결할 수 있음

* VPC Endpoint
- VPC 내 리소스(EC2 등)와 비VPC 서비스(S3, CloudWatch, CodeDeploy 등)와의 통신시, 외부 인터넷을 거치지 않고 아마존 내부 백본 네트워크를 통해 연결하는 방법
    - S3, CodeDeploy 등의 서비스는 Region 내에는 존재하지만 VPC에는 존재하지 않는 공인 IP로 존재하는 서비스로 정의할 수 있음
- 외부 인터넷 통신이 불가능한 환경의 서브넷(Private Subnet)에서 아마존의 여러 서비스를 연결할 수 있음
- VPC 엔드포인트에는 Interface Endpoint, Gateway Endpoint 두 종류가 존재
- Interface Endpoint는 목적지가 공인 IP가 아닌 사설 IP로 설정되며 Gateway Endpoint는 목적지에 대해 라우팅 테이블을 지정할수 있음(ex. pl-abcdef)
- Gateway Endpoint는 S3와 Dynamo DB만 설정 가능

* Site-to-Site VPN
- AWS의 IPSec VPN 서비스
- 이 VPN을 통해 AWS와 On-Premise의 VPN을 연결하는 것이 가능
- 고객 측 공인 IP를 뜻하는 Customer Gateway와 AWS 측 게이트웨이인 Transit Gateway(혹은 Virtual Private Gateway) 생성 후 터널을 생성하면 사용 가능
- 반드시 터널 쪽으로 라우팅을 생성해야 함

* Direct Connect
- AWS의 전용선 서비스
- 표준 이더넷 광섬유 케이블을 이용하여 케이블 한쪽을 사용자 내부 네트워크의 라우터에 연결하고 다른 한 쪽을 Direct Connect 라우터에 연결하여 내부 네트워크와 AWS VPC를 연결함
- VPN보다 더 안전하고 빠른 속도를 보장받고 싶을 때 사용
- AWS Region <-> Direct Connect Location <-> Customer