샘플 페이지입니다.

01. VPC (Virtual Private Cloud)

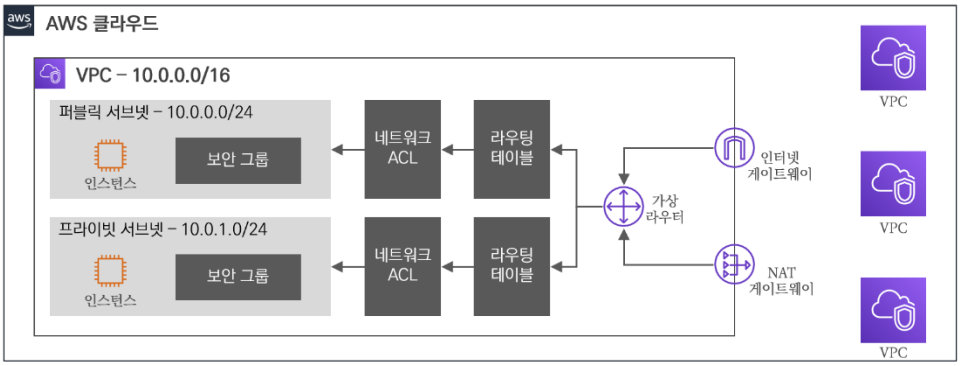
1.1 VPC 란?

1.1.1 VPC 정의

VPC는 Virtual Private Cloud의 약자로 AWS 클라우드 내 논리적으로 독립된 섹션을 제공하여, 사용자가 정의한 가상 네트워크상에서 다양한 AWS 리소스를 실행할 수 있게 지원합니다. 한마디로 **독립된 가상의 클라우드 네트워크**라 볼 수 있습니다.

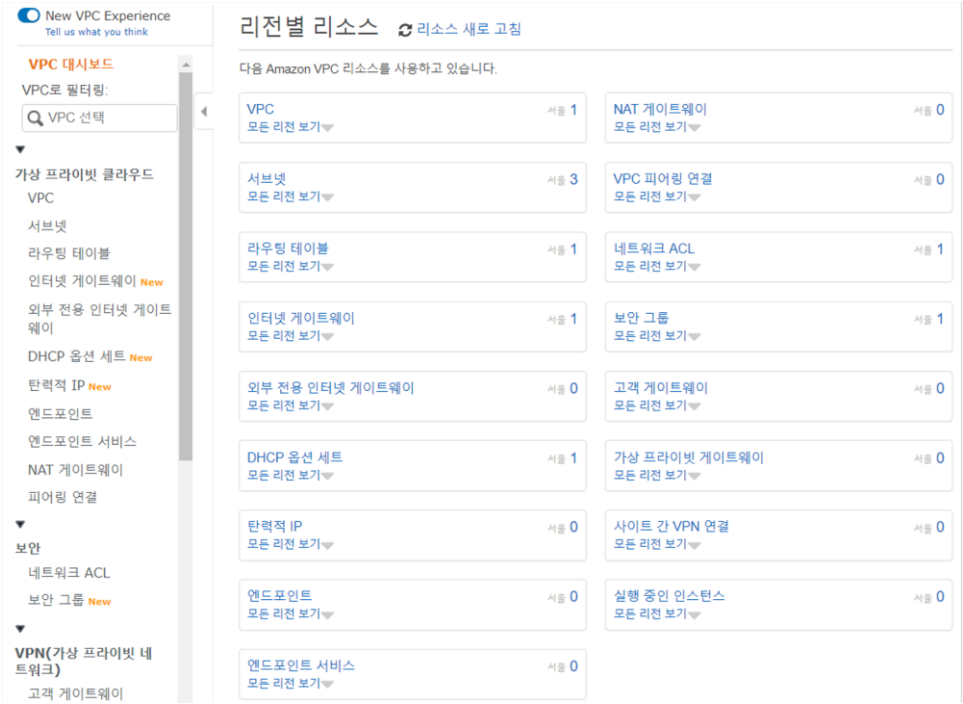
AWS 클라우드 서비스는 사용자에 따라 네트워크 환경을 직접 설계를 할 수 있다는 특징을 가지고 있습니다. 2011 년 8 월에 AWS VPC가 최초 정식 서비스되어, 사용자는 VPC 내에 IP 대역, 인터페이스, 서브넷, 라우팅 테이블, 인터넷 게이트웨이, 보안 그룹, 네트워크 ACL 등을 생성하고 제어할 수 있습니다.

[그림 1-1-1] VPC 도식화



[그림 1-1-1]과 같이 AWS 클라우드 내에 VPC를 생성하여 사용자 기반에 다양한 리소스를 생성하고 제어할 수 있습니다.

[그림 1-1-2] VPC 리소스 정보



AWS 콘솔에서 VPC 대시보드Dashboard에 접근하면 다양한 VPC 리소스들을 확인해 볼 수 있습니다. 네트워크의 기본적인 개념과 VPC 내에 생성되는 AWS 리소스 요소 중 주요 사항에 대해서는 3 절에서 하나씩 설명하도록 하겠습니다.

1.1.2 VPC 종류

VPC 는 사용자의 관여에 따라 기본 VPC Default VPC와 사용자 VPC Custom VPC로 나누어 질 수 있습니다. 기본 VPC 는 리전별로 1 개씩 생성이 되어 있으며 기본 VPC 내에 AWS 리소스가 미리 정해져 있습니다. 반면에 사용자 VPC 는 사용자 정의에 의해 수동으로 AWS 리소스를 생성하고 제어할 수 있습니다.

[표 1-1-1] 기본 VPC와 사용자 VPC 차이

구분	기본 VPC	사용자 VPC
생성 주체	AWS	사용자
AWS 리소스	정해진 리소스 미리 생성	수동으로 생성
리전 별 생성 수	1 개	최대 5 개 (기본값)

기본 VPC는 별도의 작업 없이 기본적인 클라우드 네트워크를 제공하지만, 향후 실습을 진행할 때는 사용자 VPC 를 통해 원하는 환경에 맞게 구성을 할 것입니다. 기본 VPC 의 개념 정도만 이해하고 넘어가시길 바랍니다.

1.2 VPC 특징

확장성

클라우드 기반에 손쉽게 VPC 자원을 생성하고 삭제가 가능하며, 설정 및 관리에 편의성을 제공합니다.

보안

인스턴스 레벨과 서브넷 레벨에서 인바운드 Inbound 및 아웃바운드 Outbound 필터링을 수행할 수 있도록 보안 그룹과 네트워크 ACL을 제공하여 보안을 강화할 수 있습니다.

사용자 중심

VPC 내 리소스에 대해 사용자가 원하는 대로 손쉽게 제어할 수 있으며, 네트워크 지표 및 모니터링 툴을 활용하여 사용자에게 높은 가시성을 제공합니다.

제약 사항

전통적인 네트워크 환경에서 사용가능 했던 기능이 제한되어 있거나 일부분만 사용 가능하여 기술적 제약(브로드캐스트, 멀티캐스트, IP 기반 Failover 프로토콜(VRRP, HSRP) 등) 이 따르게 됩니다.

[참고 사항]

물론 위에서 나열한 제약 사항들은 AWS에서 지속적인 기능 추가로 개선해 나가고 있습니다.

02. 기본 네트워크 개념 이해

AWS의 가상 클라우드 네트워크인 VPC에 대한 리소스 소개에 앞서 기본적인 네트워크 개념에 대해 간략하게 짚고 넘어가겠습니다.

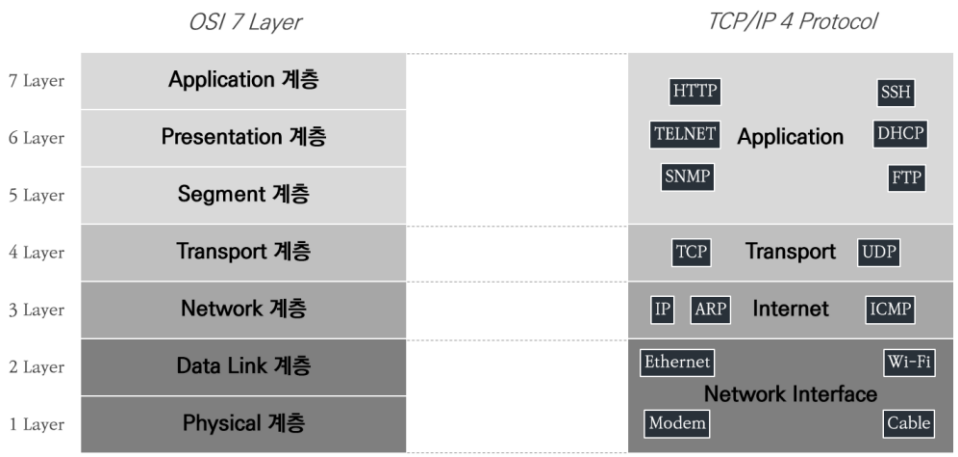
2.1 OSI 7 레이어 모델

2.1.1 OSI 7 레이어 모델 개념

OSI 7 레이어 모델은 국제표준화기구 ISO, International Organization for Standardization에서 개발한 모델로 복잡한 네트워크 동작 과정을 7 개의 계층으로 나누어 네트워크 통신 흐름을 한눈에 알아보고 이해할 수 있게 도와주는 역할을 합니다. 계층별로 하위 계층의 기능을 이용하고 상위 계층으로 기능을 제공하는 상하 관계를 맺고 있습니다.

2.1.2 OSI 7 레이어 계층 설명

[그림 2-1-1] OSI 7 레이어와 TCP/IP 프로토콜 간 계층별 비교



[그림 2-1-1]은 OSI 7 레이어의 계층별 구분과 함께 TCP/IP 프로토콜 간 계층별 비교를 보여주고 있습니다. 우선 TCP/IP 프로토콜이란 네트워크를 통해 통신하는데 쓰이는 통신 규약의 모음을 말합니다. OSI 7 레이어 계층별로 TCP/IP 의 어떤 프로토콜이 해당하는지 확인해 볼 수 있습니다. OSI 7 레이어 계층별로 간략하게 정의해 보면 아래와 같습니다.

1 Layer – Physical 계층

Physical 계층은 물리 계층으로 네트워크의 하드웨어 전송 기술을 말합니다. 물리적인 링크의 연결, 유지, 해제를 담당합니다.

2 Layer – Data Link 계층

Data Link 계층은 Physical 계층에서 송수신되는 정보의 오류와 흐름을 관리하여 데이터의 전달을 수행하는 역할을 합니다.

OSI 1 계층과 OSI 2 계층을 TCP/IP 프로토콜 상 Network Interface 계층으로 분류하며, 해당 계층에는 Ethernet, Wi-Fi, 물리적인 케이블 등이 포함됩니다.

3 Layer – Network 계층

Network 계층의 핵심은 데이터를 목적지까지 빠르고 안전하게 전달(라우팅)하기 위한 것으로 여러 노드를 거칠 때마다 최적의 경로를 찾아주는 역할을 합니다.

OSI 3 계층을 TCP/IP 프로토콜 상 Internet 계층으로 분류하며, 해당 계층에는 IP, ARP, ICMP 등의 프로토콜이 포함됩니다.

4 Layer – Transport 계층

Transport 계층은 전송 계층으로 종단의 사용자 간 데이터를 통신을 다루는 최상위 계층으로 데이터 전달의 유효성과 효율성을 보장받습니다.

OSI 4 계층을 TCP/IP 프로토콜 상에서도 Transport 계층으로 분류하며, 해당 계층에는 TCP, UDP 등의 프로토콜이 포함됩니다.

5 Layer – Session 계층

Session 계층은 종단의 사용자 간의 응용 프로세스 통신을 관리하기 위한 방법을 제공합니다. 데이터의 통신을 위한 논리적인 연결을 말합니다.

6 Layer – Presentation 계층

Presentation 계층은 데이터의 형식상 차이에 대해 송/수신자간 이해할 수 있는 형태로 데이터를 표현하는 기능을 담당합니다. 데이터의 암호화 및 압축 등을 수행합니다.

7 Layer – Application 계층

Application 계층은 응용 프로세스와 직접 연계하여 실제 응용 프로그램을 사용하게 하는 계층입니다.

OSI 5~7 계층을 TCP/IP 프로토콜 상 Application 계층으로 분류하며, 해당 계층에는 HTTP, SSH, FTP, DHCP 등이 포함됩니다.

2.2 IP와 서브넷마스크

2.2.1 IP 개념

IP는 Internet Protocol의 약자로 인터넷상의 네트워크 자원들을 구분하는 고유한 주소입니다. 참고로 IP는 앞서 설명 드린 OSI 7 레이어에서 3 계층에 해당합니다. IP 주소는 버전에 따라 IP 버전 4[IPv4]와 IP 버전 6[IPv6]로 구분 지을 수 있습니다.

[표 2-2-1] IPv4와 IPv6 차이

구분	IPv4	IPv6
주소 길이	32bit	128bit
표기 방법	8 비트씩 4 개의 파트로 10 진수 표현 예) 39.118.188.233	16 비트씩 8 개의 파트로 16 진수 표현 예) 2002:0221:ABCD:CDEF:0000:0000:FFFF:1234
주소 개수	약 43 억개	약 43 억 × 43 억 × 43 억 × 43 억

[표 2-2-1]과 같이 IPv4 와 IPv6 는 구조적으로 다른 형태로 표기되며 가용 숫자도 큰 차이를 보입니다. 물론 IPv4와 IPv6 간 차이는 많은 요소가 있지만 간략하게 구조의 차이 정도만 이해하고 넘어가시길 바랍니다. 예전부터 IPv4는 가용 숫자의 문제와 효율성 문제가 제기되고 있고 이에 IPv6 가 문제에 대해 진보된 특성을 보이지만, 여전히 IPv4 를 주로 쓰이고 있습니다. 본 책에서 다루고 있는 대부분의 실습과 이론은 IPv4 기준으로 쓰였음을 알려드립니다.

2.2.2 퍼블릭 IP와 프라이빗 IP

기본적으로 네트워크의 통신 용도에 따라 퍼블릭 네트워크와 프라이빗 네트워크로 구분을 지을 수 있습니다. 퍼블릭 네트워크는 실제 인터넷 구간으로 통신하는 공공 네트워크이며, 프라이빗 네트워크는 인터넷 구간이 아닌 내부적으로 통신하는 사설 네트워크입니다. 이러한 퍼블릭 네트워크와 프라이빗 네트워크가 사용하는 IPv4 주소 대역이 지정되어 있습니다.

퍼블릭 IP (공인 IP)

인터넷 구간의 통신 대상을 식별하기 위해 ISP(Internet Service Providor: 인터넷 서비스 공급자)에서 제공하는 IP 주소입니다. 해당 퍼블릭 IP는 전 세계의 인터넷 구간에서 유일한 주소를 갖습니다.

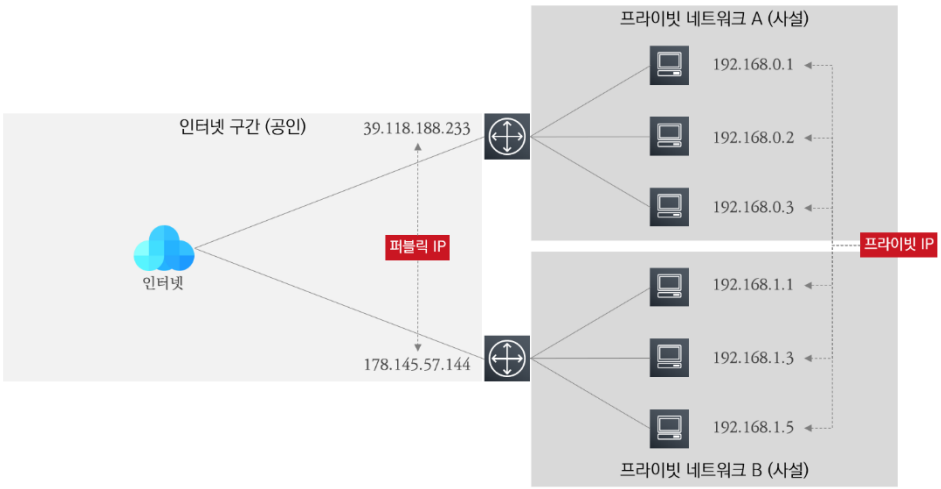
프라이빗 IP (사설 IP)

일반 가정이나 회사 등의 독립된 네트워크에서 사용하는 내부 IP 주소입니다. 해당 프라이빗 IP는 프라이빗 네트워크 관리자에 의해 할당되며, 독립된 네트워크상에서 유일한 주소를 갖습니다. 그리고 프라이빗 IP 주소를 통해 외부 인터넷 구간과 통신이 불가능합니다.

이러한 프라이빗 IP 주소는 아래와 같이 3가지 대역(Class)으로 고정되어 있습니다.

- Class A: 10.0.0.0 ~ 10.255.255.255
- Class B: 172.16.0.0 ~ 172.31.255.255
- Class C: 192.168.0.0 ~ 192.168.255.255

[그림 2-2-1] 퍼블릭 IP와 프라이빗 IP 도식화



[그림 2-2-1]을 통해 퍼블릭 IP와 프라이빗 IP의 차이를 확인해 볼 수 있습니다.

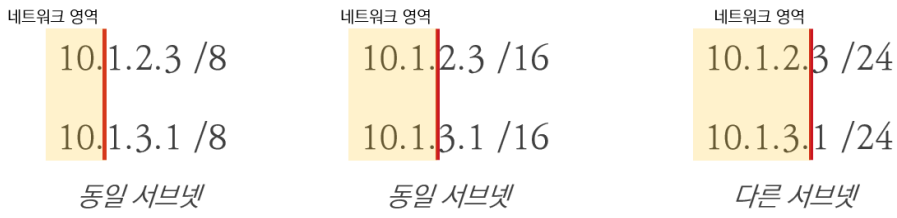
2.2.3 서브넷과 서브넷 마스크

먼저 서브넷이란 부분적인 네트워크를 의미합니다. 모든 네트워크망이 거대한 하나의 망으로 이루어진 형태는 아닙니다. 네트워크망에서 서브넷을 통해 부분적인 네트워크망으로 나누어지고 서로 연결되어 있습니다. [그림 2-2-1]을 다시 보면 사설 네트워크 A와 사설 네트워크 B는 서로 다른 네트워크로 나뉘어 있습니다. 즉, 서로 간에 서브넷으로 분리된 부분 네트워크망입니다.

그렇다면 이렇게 나누어진 서브넷은 서로 간에 어떻게 구분을 할 수 있을까요? 이때 사용되는 것이 서브넷 마스크입니다. 서브넷 마스크는 IP 주소에 네트워크 ID와 호스트 ID를 구분하는 기준값입니다. 네트워크 ID는 서브넷을 식별하는 영역이고, 호스트 ID는 서브넷에서 대상을 식별하는 영역입니다. 즉, 동일한 서브넷에 속한 IP 주소의 네트워크 ID의 값은 모두 동일하며 호스트 ID를 통해 개별 구분합니다. 서브넷 마스크는 IPv4와 마찬가지로 32bit 구조이며, 이진수 값이 1인 영역이 네트워크 ID, 0인 영역이 호스트 ID입니다. (비트 값은 연속성을 취하고 있습니다)

예를 들면 서브넷 마스크는 이진수로 11111111.11111111.11111111.00000000 형태로 표현될 수 있습니다. 물론 이진수로 표현하는 것보다 255.255.255.0 처럼 10진수로 표현하거나 /24로 프리픽스 Prefix 형태로 표현을 합니다. (/24는 1의 개수, 네트워크 ID의 비트 수입니다)

[그림 2-2-2] 서브넷 마스크를 통한 서브넷 구분



[그림 2-2-2]는 보편적으로 많이 쓰이는 프리픽스를 통해 2개의 IP가 동일한 서브넷인지 다른 서브넷인지 보여주고 있습니다. 참고로 /8은 8bit가 네트워크 영역으로 10진수 첫 번째 자리가 네트워크 영역입니다. 이렇게 네트워크 영역을 구분하고 서로 비교하여 동일 서브넷인지 아

닌지 판단할 수 있습니다. 10.0.0.0/8, 10.1.0.0/16, 10.1.1.0/24 와 같이 표기하는 방법을 **IP CIDR**Classless Inter Domain Routing 표기법이라 합니다.

[참고 사항]

위와 같이 /8, /16, /24에서 세부적으로 서브넷팅을 할 수 있습니다만, 서브넷과 서브넷 마스크와 IP CIDR가 무엇인지 정도만 이해하고 넘어가길 바랍니다.

2.3 TCP와 UDP 그리고 포트 번호

2.3.1 TCP와 UDP

TCP 와 UDP 는 OSI 7 레이어 중 4 계층에 사용되는 대표적인 전송 프로토콜입니다. TCP 와 UDP는 신뢰성 있는 전송의 여부에 따라 차이를 두고 있습니다.

[표 2-3-1] TCP와 UDP의 차이

구분	TCP	UDP
OSI 모델	4 계층(전송 계층)	4 계층(전송 계층)
연결	연결 지향성	비연결 지향성
신뢰성	신뢰성 보장	신뢰성 보장하지 않음
순서	데이터 순서 보장	데이터 순서 보장하지 않음
제어	혼잡 제어, 흐름 제어 제공	혼잡 제어, 흐름 제어 제공하지 않음
속도	상대적으로 느림	상대적으로 빠름
서비스	HTTP, SSH, FTP 등	DNS, DHCP 등

[표 2-3-1]과 같이 TCP 는 종단 간의 연결을 맺고 연결이 이루어지면 신뢰성 있는 전송을 보장하는 프로토콜로 그로 인해 UDP 보다 상대적으로 느린 통신이 이루어집니다. 대표적인 서비스로 HTTP, SSH, FTP 등의 연결성과 신뢰성이 필요한 서비스가 있습니다.

반대로 UDP 는 종단 간의 연결 없이 통신이 이루어지며 신뢰성 있는 전송을 보장받을 수 없습니다. 연결이나 제어를 위한 작업이 없기 때문에 TCP 보다 상대적으로 빠른 통신이 이루어집니다. 대표적인 서비스로 DNS, DHCP 등이 있습니다.

2.3.2 포트 번호

위의 설명과 같이 TCP 와 UDP 의 특성에 따라 제공되는 응용 프로그램 서비스가 있습니다. 이런 서비스를 구분할 때 포트 번호를 통해 구분할 수 있습니다. IANA 라는 단체에서 TCP 와 UDP 의 포트 번호 범위를 정의하고 있으며, 범위에 따라 크게 3 가지로 구분 지을 수 있습니다.

- 잘 알려진 포트(Well-Known Port): 0~1023
- 등록된 포트(Registered Port): 1024~49151
- 동적 포트(Dynamic Port): 49152~65535

예를 들어 TCP 의 포트 번호 80 은 HTTP 서비스로 예약된 잘 알려진 포트이며, UDP 의 포트 번호 53 은 DNS 서비스로 예약된 잘 알려진 포트를 의미합니다.

2.4 DHCP (Dynamic Host Configuration Protocol)

2.4.1 DHCP 개념

DHCP Dynamic Host Configuration Protocol 는 동적으로 IPv4 주소를 일정 기간 임대를 하는 프로토콜입니다. 해당 DHCP 는 UDP 프로토콜을 사용하며, 포트 번호 67 과 68 을 사용하여 동작합니다. 네트워크상 호스트가 IPv4 주소를 할당할 때 수동으로 지정할 수도 있고, DHCP 를 통해 자동으로 지정할 수도 있습니다. IP 주소를 임대하는 개념하에 임대 시간 Lease Time 이 존재하며 임대 시간이 만료되면 반환하거나 갱신을 수행합니다.

2.4.2 DHCP 절차

DHCP 는 중앙집중형 서버/클라이언트 방식으로 동작합니다. 즉, DHCP 서버가 존재하고 네트워크 호스트가 클라이언트가 되어 서버에게 IP 할당을 요청하는 구조입니다.

[그림 2-4-1] DHCP 동작 절차

[그림 2-4-1]과 같이 DHCP 는 4 단계의 절차를 통해 동적으로 IP 를 할당 받을 수 있습니다.

- DHCP Discover: DHCP 클라이언트에서 DHCP 서버를 찾기 위한 메시지
- DHCP Offer: DHCP 서버에서 할당할 IP 주소와 임대 시간을 알림
- DHCP Request: DHCP 클라이언트에서 DHCP 서버로 할당받은 IP 를 요청
- DHCP Ack: DHCP 서버에서 최종적으로 할당 IP 를 승인하여 알림

2.5 DNS (Domain Name System)

2.5.1 DNS 개념

DNS Domain Name System는 도메인 네임을 제공하기 위한 기술입니다. 여기서 도메인 네임이란 IP 주소의 복잡한 주소 체계를 해소하기 위해 문자 형태로 구성된 이름입니다. 예를 들어 구글 서버에 대한 주소는 IP 형태로 구성되어 있겠지만, 우리는 google.com 이라는 문자 형태로 접근을 합니다. 즉, google.com 이라는 것이 도메인 네임이며 google.com 과 IP 주소를 매핑하여 제공하는 기술이 DNS 입니다. 해당 DNS 는 UDP 프로토콜을 사용하며, 포트 번호 53 을 사용하여 동작합니다.

[참고 사항]

DNS에 대한 상세 정보는 '**5장 부하 분산**' 파트에 '**Route 53**' 부분에서 자세히 다루고 있습니다. 지금은 개념적인 부분만 설명하고 넘어가겠습니다.

2.6 라우팅 (Routing)

2.6.1 라우팅 개념

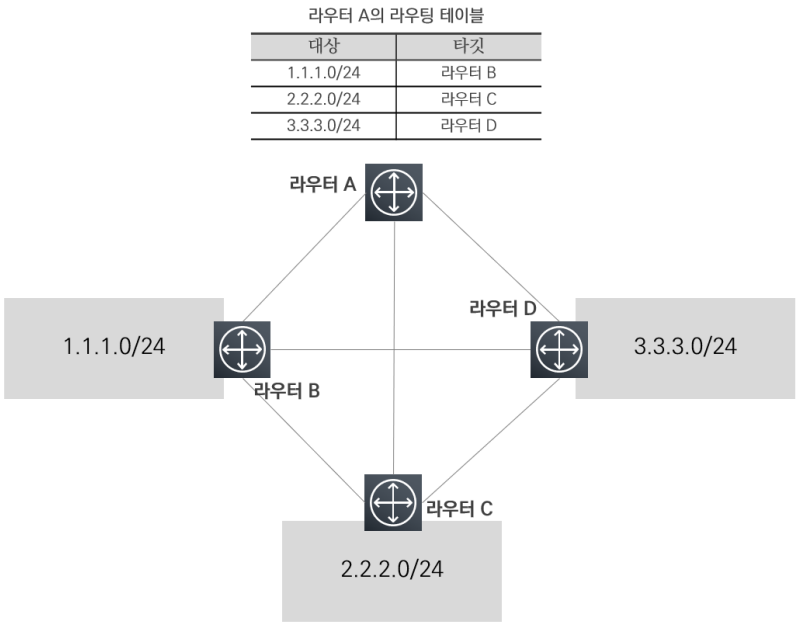
라우팅이란 네트워크 통신을 수행할 때 거쳐 가는 경로를 잡아 주는 OSI 7 Layer 에서 3 계층인 Network 계층의 핵심적인 기능을 수행합니다.

위에서 설명했듯이 네트워크는 여러 개의 서브넷으로 이루어져 있으며, 목적지 IP 로 향할 때 여러 노드를 거쳐서 통신이 되고 있습니다. 복잡하게 연결된 네트워크망에서 최적의 경로를 잡아 통신하는 것이 바로 라우팅입니다. 네트워크 입장에서 최적의 라우팅을 통해 안정적이고 빠른 통신을 하는 것은 중요한 지향점입니다.

2.6.2 라우터와 라우팅 테이블

이렇게 라우팅을 수행하는 장비를 라우터라 하며, 해당 라우터는 라우팅 테이블을 통해 경로를 파악하고 원하는 목적지 대상으로 데이터를 전달합니다.

[그림 2-6-1] 라우터와 라우팅 테이블



[그림 2-6-1]과 같이 네트워크망에서 라우터는 라우팅 테이블을 통해 목적지 IP가 어느 경로로 향하는지 기록하고 해당 경로로 데이터를 전달합니다.

03. VPC 리소스 소개

3.1 서브넷 (Subnet)

3.1.1 서브넷 개념

서브넷 Subnet 의 일반적인 개념은 네트워크 영역을 부분적으로 나눈 망으로 정의할 수 있습니다. 클라우드 환경의 VPC 에서도 서브넷을 통해 네트워크를 분리하여 나눌 수 있습니다.

[그림 3-1-1] 서브넷 도식화

[그림 3-1-1]과 같이 VPC 내에 서브넷을 통해 네트워크망을 분리하고 있는 모습입니다. 추가로 알아두셔야 할 것은 서브넷의 IP 대역은 VPC 의 IP 대역에 속해 있어야 하며, 서브넷은 1 개의 가용 영역에 종속되어야 합니다. AWS 에서는 서브넷에 할당할 수 있는 IP 대역에서 미리 예약되어 있는 IP 주소가 있습니다. 이러한 예약된 IP 주소들은 AWS 자원에게 할당할 수 없습니다.

AWS에서 서브넷의 IP 대역마다 예약된 IP 주소

서브넷 IP 대역에서 첫번째에서 네번째까지 IP 주소는 예약되어 있습니다. 그리고 마지막 IP 주소도 예약되어 있습니다.

예를 들어 서브넷에 할당할 IP 대역이 10.0.0.0/24 이라면 10.0.0.0~10.0.0.255 중에서
첫번째 주소: 10.0.0.0 ➔ 네트워크 주소
두번째 주소: 10.0.0.1 ➔ AWS VPC 가상 라우터 주소
세번째 주소: 10.0.0.2 ➔ AWS DNS 서버 주소
네번째 주소: 10.0.0.3 ➔ 향후 새로운 기능에 활용할 주소
마지막 주소: 10.0.0.255 ➔ 네트워크 브로드캐스트 주소

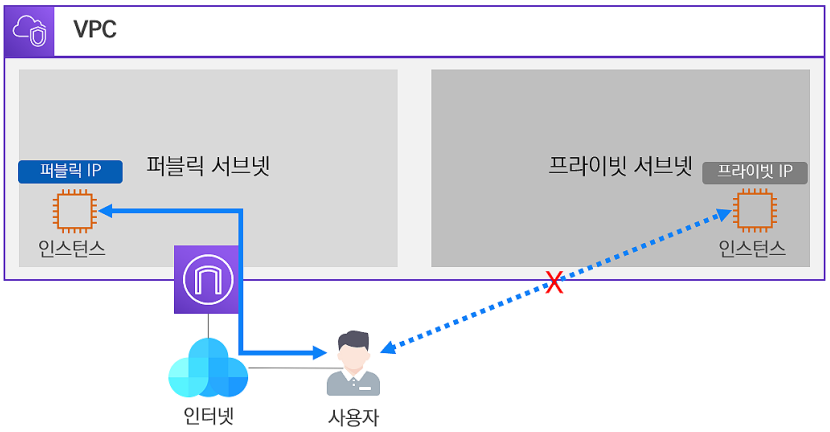
[참고 사항]

기본적으로 예약된 IP 주소를 고려하여 생성해야 합니다. 특정 서비스에 대해 IP 주소가 부족하면 문제가 발생할 수 있어, 어느 정도 여유를 두고 생성하는 것을 권장합니다.
그리고, VPC 내 여러 서브넷이 존재할 경우 첫번째 서브넷의 세번째 주소를 DNS 서버 주소로 사용합니다. 나머지 서브넷의 세번째 주소는 AWS에서 예약되어 있습니다.

3.1.2 퍼블릭 서브넷과 프라이빗 서브넷

서브넷은 크게 퍼블릭 서브넷과 프라이빗 서브넷으로 나눌 수 있습니다. 퍼블릭 서브넷은 공인 네트워크 개념으로 외부 인터넷 구간과 직접적으로 통신을 할 수 있는 공공 네트워크입니다. 반면에 프라이빗 서브넷은 사설 네트워크 개념으로 외부 인터넷 구간과 직접적인 통신을 할 수 없는 폐쇄적인 네트워크입니다.

[그림 3-1-2] 퍼블릭 서브넷과 프라이빗 서브넷



[그림 3-1-2]와 같이 퍼블릭 서브넷은 퍼블릭 IP 를 가지고 인터넷 게이트웨이를 통해 외부 인터넷 구간의 사용자와 통신이 가능하나, 프라이빗 서브넷은 프라이빗 IP 만 가지고 있어 자체적으로 외부 인터넷 구간의 사용자와 통신이 불가능합니다.

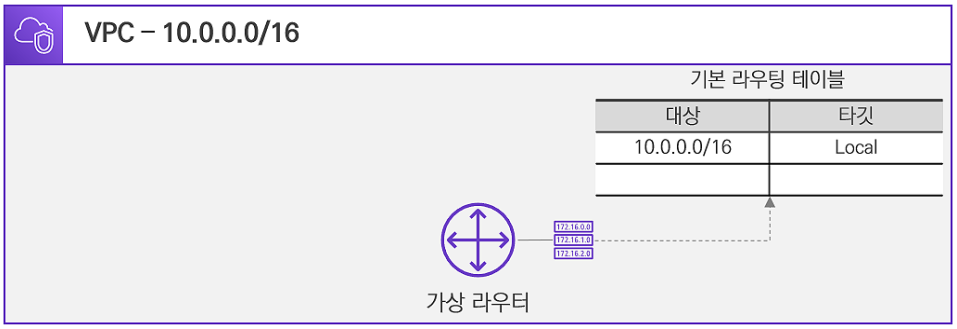
[참고 사항]

프라이빗 서브넷은 원론적으로는 외부 인터넷 구간과 통신이 불가능하지만, 프라이빗 IP를 퍼블릭 IP로 변환해 주는 NAT 게이트웨이가 있으면 통신이 가능합니다.

3.2 가상 라우터와 라우팅 테이블

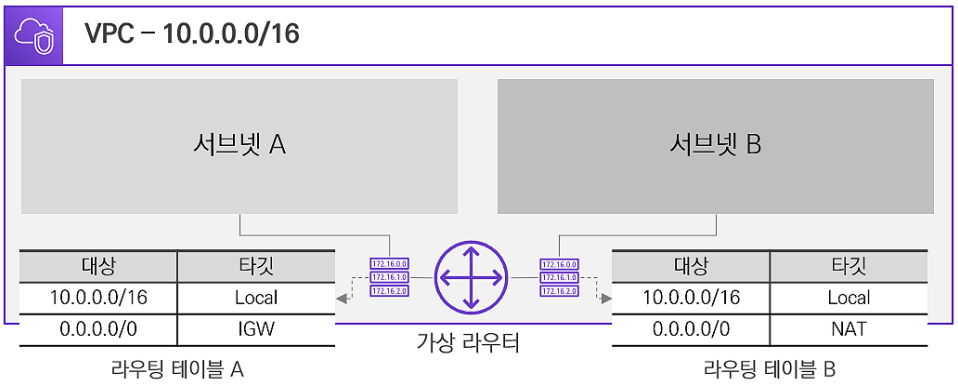
VPC 를 생성하면 자동으로 가상 라우터가 생성됩니다. 이 가상 라우터는 라우팅 테이블을 가지고 있어 목적지 네트워크로 라우팅하여 통신합니다.

[그림 3-2-1] 가상 라우터와 라우팅 테이블



[그림 3-2-1]과 같이 10.0.0.0/16 대역의 VPC 를 생성하면, 자동으로 가상 라우터가 생성됩니다. 가상 라우터는 최초에 기본 라우팅 테이블을 보유하고 있으며 로컬 네트워크에 대한 라우팅 경로만 잡혀 있습니다. 여기서 로컬 네트워크는 VPC 의 자체 대역으로 VPC 내에 생성된 서브넷은 라우팅 테이블의 로컬 네트워크에 의해 통신이 가능합니다.

[그림 3-2-2] 서브넷 당 라우팅 테이블 매핑



[그림 3-2-2]와 같이 가상 라우터에서는 서브넷별로 라우팅 테이블을 매핑을 시켜 줄 수 있습니다. 기본 라우팅 테이블을 사용할 수도 있지만, 새로운 라우팅 테이블을 생성하고 매핑하여 서브넷 당 개별적인 라우팅 테이블을 가질 수 있습니다.

3.3 인터넷 게이트웨이

인터넷 게이트웨이는 VPC와 인터넷 간의 논리적인 연결입니다. 간략하게 VPC에서 인터넷 구간으로 나가는 관문이라고 생각할 수 있습니다. 이러한 인터넷 게이트웨이는 VPC 당 1개만 생성할 수 있습니다. 인터넷 게이트웨이를 통해 외부 인터넷 구간으로 통신할 수 있는 대상은 퍼블릭 IP 를 사용하는 퍼블릭 서브넷 내의 자원입니다. 이러한 퍼블릭 서브넷은 자신의 라우팅 테이블에 외부 인터넷 구간으로 나가는 타깃을 인터넷 게이트웨이로 지정해 주어야 합니다.