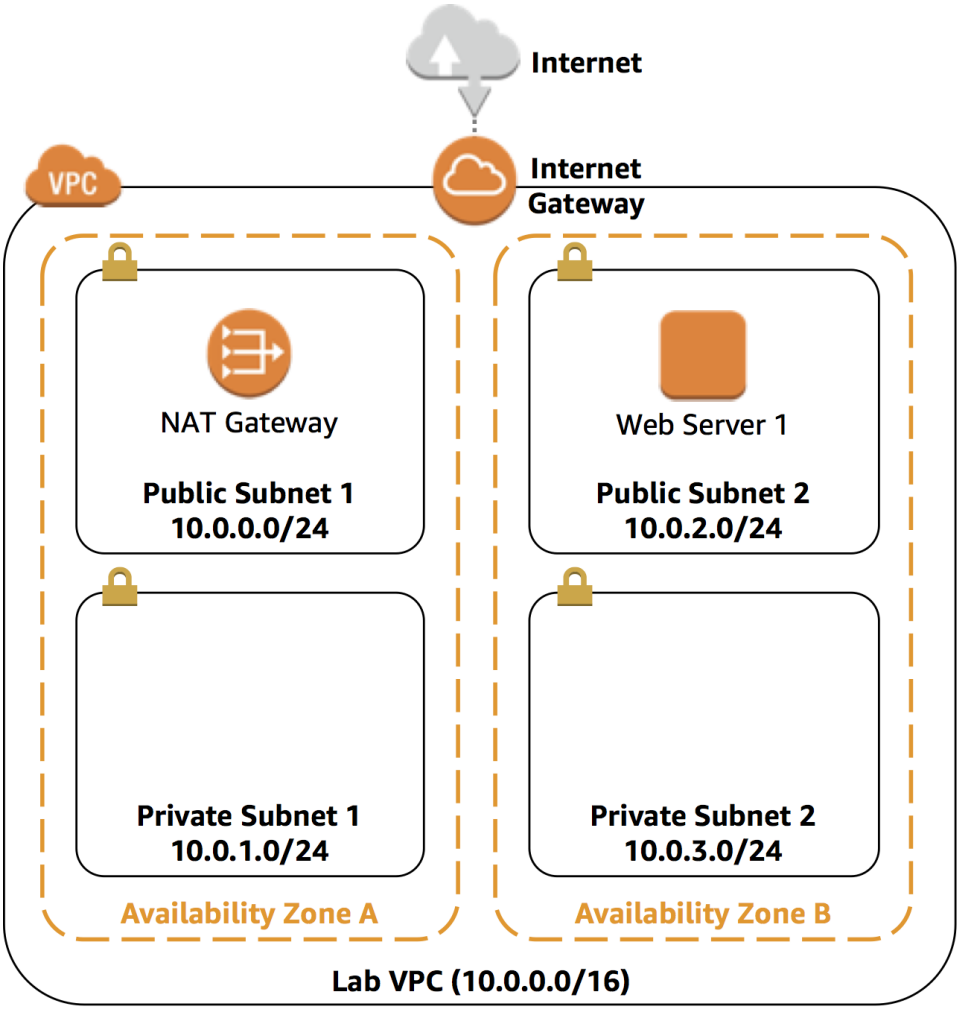
# 실습 1: VPC 구축 및 웹 서버 시작

본 실습 섹션에서는 Amazon Virtual Private Cloud(VPC)를 사용하여 자체 VPC를 생성하고, VPC에 구성 요소를 추가하여 사용자 정의된 네트워크를 구성합니다. EC2 인스턴스에 대한 보안 그룹을 생성합니다. 웹 서버를 실행하고 이를 VPC에서 시작하도록 EC2 인스턴스를 구성 및 사용자 정의합니다.

**Amazon Virtual Private Cloud(Amazon VPC)** 를 사용하면 사용자가 정의한 가상 네트워크에 AWS(Amazon Web Services) 리소스를 시작할 수 있습니다. 이 가상 네트워크는 AWS의 확장 가능한 인프라를 사용하는것에 대한 이점과 함께 귀하가 자체 데이터 센터에서 운영하는 기존 네트워크와 매우 유사합니다. 그리고 VPC는 여러 가용영역에 걸쳐 생성할 수 있습니다.

**시나리오**

본 실습에서는 다음과 같은 인프라를 구축합니다.




**Public Route Table**

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | Internet Gateway |

**Private Route Table**

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | NAT Gateway |

**목표**

본 실습을 완료하면 다음을 할 수 있습니다.

- VPC 생성
- 서브넷 생성
- 보안 그룹 구성
- VPC에서 EC2 인스턴스 시작

**소요 시간**

본 실습을 완료하는 데는 약 **45분** 정도가 소요됩니다.

## 사전작업

이 작업은 **Elastic IP**를 설정합니다.

1. **AWS Management Console**의 **Services** 메뉴에서 **EC2** 를 클릭합니다.
2. 좌측 패널에서 **Network & Security**아래 **Elastic IPs**를 클릭합니다.
3. 우측 상단의 **Allocate Elastic IP address**를 클릭합니다.
4. 아래에 있는 **Allocate** 버튼을 클릭합니다.

## 과제 1: VPC 생성

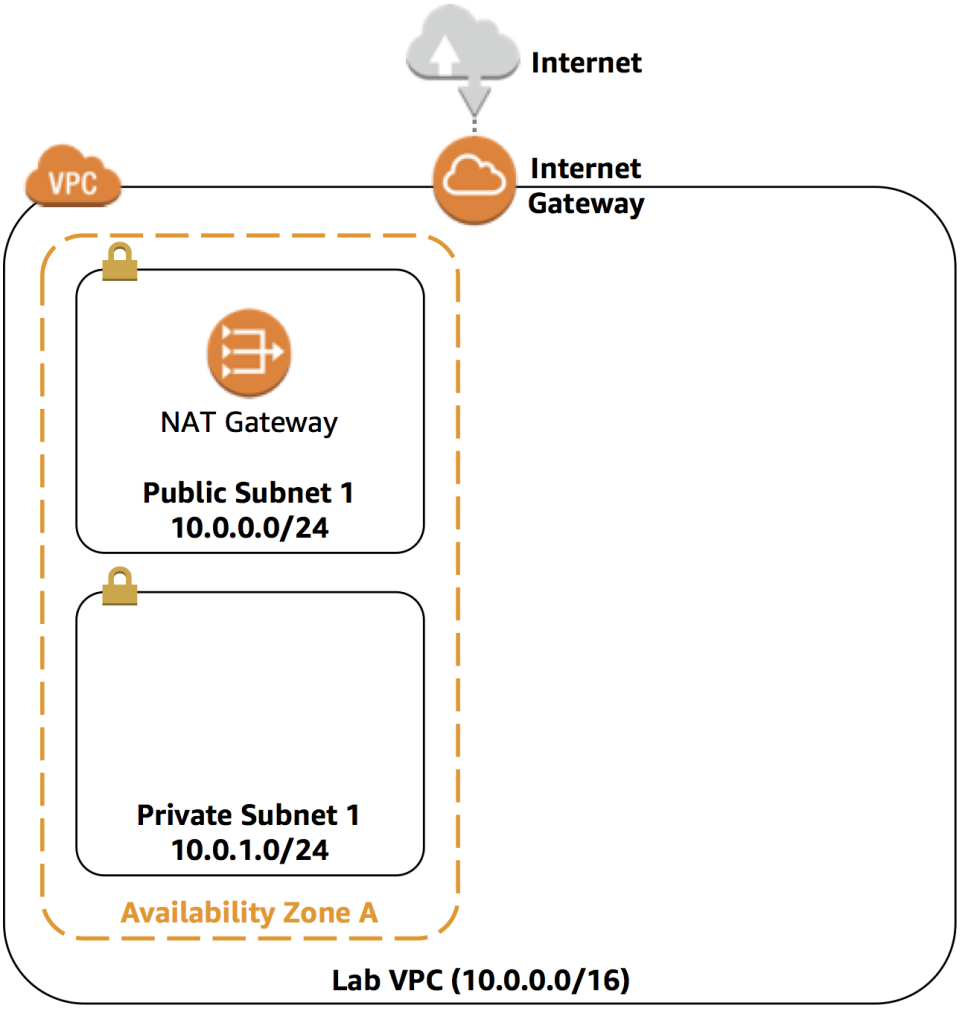
이 작업에서는 VPC 마법사를 사용하여 VPC 인터넷 게이트웨이와 단일 가용영역에 두 개의 서브넷을 생성하십시오. **Internet Gateway(IGW)** 는 VPC와 인터넷 인스턴스간의 통신을 허용하는 VPC 구성 요소입니다.

VPC를 생성한 후 **subnets** 을 추가할 수 있습니다. 각 서브넷은 모두 하나의 가용영역 내에 존재하며 영역을 확장할 수는 없습니다. 서브넷의 트래픽이 인터넷 게이트웨이로 라우팅되는 경우 서브넷은 **Public subnet** 으로 부르며. 서브넷에 인터넷 게이트웨이로의 경로가 없는 경우 서브넷은 **Private subnet** 라고 합니다.

또한 마법사는 Private subnet 의 EC2 인스턴스애게 인터넷 연결을 접속할 수 있도록 *NAT Gateway* 를 만들 것입니다.

1. **AWS Management Console**의 **Services** 메뉴에서 **VPC** 를 클릭합니다.
2. 콘솔 언어를 영어로 변경합니다. 화면 맨 왼쪽 아래 **Feedback(의견)** 바로 오른쪽에 언어를 확인합니다. **한국어** 로 되어 있다면 반드시 **English(US)** 로 변경하십시오. 이 실습 가이드는 **English** 를 기준으로 작성 되었습니다.
3. **Launch VPC Wizard** 를 클릭합니다.
4. 좌측 탐색 창에서 **VPC with Public and Private Subnets**를 클릭합니다.(두번째 옵션입니다.)
5. **Select** 를 클릭후 다음 설정을 구성합니다(나열되지 않은 설정은 무시).
   - **VPC name**: `Lab  VPC`를 입력합니다.
   - **Availability Zone**: *첫 번째* 가용 영역을 클릭합니다.
   - **Public subnet name**: `Public  Subnet  1`을 입력합니다.
   - **Availability Zone**: *첫 번째* 가용 영역을 클릭합니다.
     이것은 위에에 사용된 것과 동일합니다.
   - **Private subnet name**: `Private  Subnet  1`을 입력합니다.
   - **Elastic IP Allocation ID:** 비어있는 박스를 클릭하면 IPaddress가 표시되며, 그 IPaddress를 선택합니다.
6. **Create VPC** 를 클릭합니다.
7. 생성이 완료되면 **OK** 를 클릭합니다.

마법사가 VPC를 동일한 가용영역에 Public Subnet과 Private Subnet과 각 서브넷의 경로 테이블과 함께 구성을 하게 됩니다.




**Public Route Table**

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | Internet Gateway |

**Private Route Table**

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | NAT Gateway |

Public Subnet은 **10.0.0.0/24** 의 CIDR을 가지고 있으며, 이는 **10.0.0.x** 로 시작하는 모든 IP 주소를 포함하고 있음을 의미합니다.

Private Subnet은 **10.0.1.0/24** 의 CIDR을 가지고 있으며, 이는 **10.0.1.x**로 시작하는 모든 IP 주소를 포함하고 있음을 의미합니다.

## 과제 2: 추가 서브넷 생성

이 작업에서는 두 번째 가용영역에 두 개의 추가 서브넷을 생성합니다. 이는 여러 가용영역에서 리소스를 생성하여 *고가용(High Availability)* 를 제공하는 데 유용하게 됩니다.

8. 왼쪽 탐색 창에서 **Subnets** 를 클릭합니다.
9. **Create subnet** 을 클릭하고 다음 설정을 구성합니다.
   - **VPC**: **Lab VPC**를 클릭합니다.
   - **Name tag**: `Public Subnet 2`를 입력합니다.
   - **Availability Zone**: *두 번째* 가용 영역을 클릭합니다.
   - **IPv4 CIDR block**: `10.0.2.0/24`를 입력합니다.

이 서브넷은 **10.0.2.x**로 시작하는 모든 IP 주소를 갖게 됩니다.

10. **Create Subnet** 를 클릭 합니다.

또 다른 subnet을 생성합니다.

11. **Create subnet** 를 클릭한후 다음 설정을 구성합니다.

    - **VPC**: *Lab VPC* 를 클릭합니다.

- **Name tag**: `Private Subnet 2`를 입력합니다.
- **Availability Zone**: *두 번째* 가용 영역을 선택합니다.
  이것은 Public Subnet 2에서 사용된 것과 동일합니다.
- **CIDR block**: `10.0.3.0/24`를 입력합니다.

이 서브넷은 **10.0.3.x**로 시작하는 모든 IP 주소를 갖게 됩니다.

12. **Create Subnet** 를 클릭 합니다.

이제 Private Subnet의 리소스가 인터넷에 연결되지만 여전히 리소스를 비공개로 유지할 수 있도록 Private Subnet을 구성하여 NAT 게이트웨이로 인터넷 연결을 라우팅하십시오. 이것을 위해 *Route Table* 을 구성합니다.

*Route table* 은 네트워크 트래픽의 방향을 결정하는 데 사용되는 *Routes* 라는 규칙 집합을 포함합니다. VPC의 각 서브넷은 **Route table** 과 연결되어야 합니다. *Route table* 은 서브넷에 대한 라우팅을 제어합니다.

13. 왼쪽 탐색 창에서 **Route Tables** 를 클릭합니다.
14. 화면에서 **VPC ID** 필드에 **Lab VPC** 가 보이고(VPC ID 필드를 확장해야 보입니다.) **Main** 필드에 **Yes** 가 있는 라우팅 테이블을 선택 합니다.
15. 이 라우팅 테이블의 비어있는 **Name** 필드에 마우스를 올려놓으면 연필모양의 아이콘 이 보이며 이것을 클릭하고 `Private Route Table`을 입력한 다음 확인 표시 를 클릭하여 저장합니다.
16. 아래쪽 창에서 **Routes** 탭을 클릭합니다.
17. **Destination 은 0.0.0.0/0** 으로 설정되어 있고 **Target 은 nat-xxxxxxxx** 로 설정되어 있는지 확인합니다. 이 라우팅 테이블의 설정 의미는 프라이빗 서브넷에서 NAT Gateway로 트래픽을 라우팅하는 데 사용됩니다.
18. 오른쪽 **Subnet Associations** 탭을 클릭합니다.

이제 이 라우팅 테이블을 Private Subnet에 연결합니다.

19. **Edit subnet associations** 를 클릭합니다.
20. **Private Subnet 1** 및 **Private Subnet 2**를 선택 합니다.

*Subnet ID* 컬럼을 확장하면 Subnet name을 잘 보실 수 있습니다.

21. **Save**를 클릭합니다.

이제 Public Subnet에서 사용하는 라우팅테이블을 구성합니다.

22. 이번에는 VPC ID가 **Lab VPC** 이고 **Main** 에 **No**가 있는 라우팅 테이블을 선택 합니다.(다른 Subnet이 선택되어 있으면 선택을 제거합니다.)

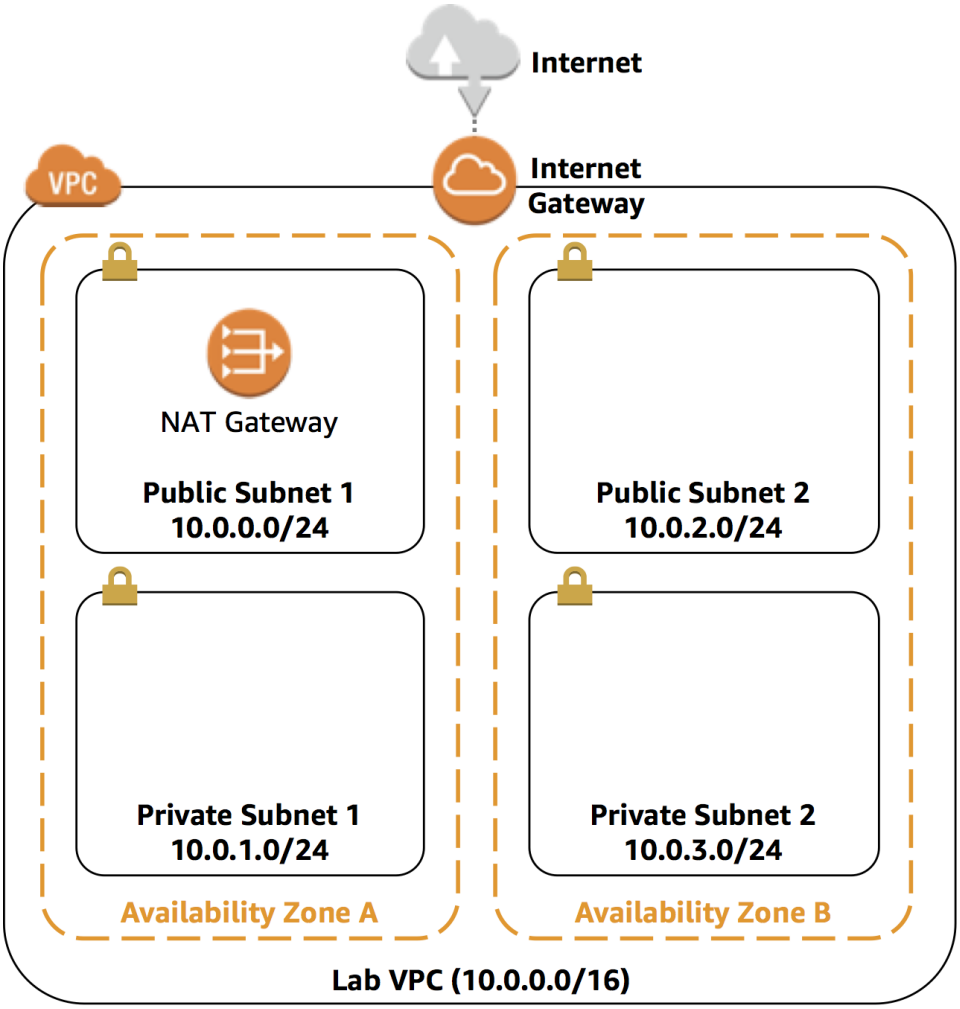
23. 이 라우팅 테이블의 **Name** 필드에 마우스를 올려놓으면 연필모양 의 아이콘이 보이며 이것을 클릭하고 `Public Route Table` 을 입력한 다음 확인 표시 를 클릭하여 저장합니다.

24. 아래쪽 창에서 **Routes** 탭을 클릭하고 **Destination 이 0.0.0.0/0** 이고, **Target 이 igw-xxxxxxxx** 로 설정되어 있는지 확인합니다. 이 라우팅 테이블은 퍼블릭 서브넷에서 인터넷으로 통신되도록 사용됩니다.

이제 이 라우팅 테이블을 Public Subnet에 연결합니다.

25. **Subnet Associations** 탭을 클릭한 다음 **Edit subnet associations** 를 클릭합니다.
26. **Public Subnet 1** 및 **Public Subnet 2** 를 선택 합니다.
27. **Save**를 클릭합니다.

이제 VPC에 두 개의 가용영역에서 Public 및 Private Subnet이 구성되었습니다.




**Public Route Table**

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | Internet Gateway |

**Private Route Table**

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | NAT Gateway |

## 과제 3: VPC 보안 그룹 생성

이 작업에서는 가상 방화벽 역할을 하는 VPC Security Group을 생성합니다. 인스턴스를 생성할 때 하나 이상의 보안 그룹을 인스턴스와 연결해야 하며 연결된 인스턴스로의 트래픽을 허용하는 규칙을 각 Security Group에 추가 해야 합니다.

28. 왼쪽 탐색 창에서 **Security Groups** 를 클릭합니다.
29. `Create security group` 를 클릭후 다음 설정을 구성합니다.
    - **Security group name**: `Web Security Group`을 입력합니다.
    - **Description**: `Enable HTTP access`를 입력합니다.
    - **VPC**: **Lab VPC** 를 클릭합니다.

이제 인바운드 웹 요청을 허용하는 규칙을 Security Group에 추가하십시오.

30. **Inbound rules** 세션에서 `Add rule` 을 클릭하고 다음을 구성합니다:

- **Type:** *HTTP*
- **Source:** *Anywhere-IPv4*
- **Description:** `Permit web requests`

31. 화면 맨 아래에 `Create security group` 버튼을 클릭합니다.

Amazon EC2 인스턴스를 시작할 때 다음 작업 에서 이 Security Group을 사용하십시오.

## 과제 4: 첫 번째 웹 서버 인스턴스 시작

이 작업에서는 Amazon EC2 인스턴스를 새 VPC에서 시작합니다. 웹 서버 역할을 수행하도록 인스턴스를 구성하십시오.

32. Services 메뉴에서 **EC2** 를 클릭합니다.
33. Launch instance 를 클릭합니다.

먼저 원하는 운영 체제가 포함된 _Amazon Machine Image(AMI)_를 선택하십시오.

34. **Amazon Linux 2 AMI** 가 있는 행에서 오른쪽에 Select 를 클릭합니다.

*Instance Type* 은 인스턴스에 할당된 하드웨어 리소스를 정의합니다.

35. **t3.micro** 를 선택합니다.(*Type* 컬럼을 확인합니다.)
36. Next: Configure Instance Details 을 클릭합니다.

이제 새 VPC의 Public Subnet에서 시작하도록 인스턴스를 구성하십시오.

37. 다음을 구성하십시오. **Network:** *Lab VPC*
    - **Subnet:** *Public Subnet 2* (Private이 아닙니다!)
    - **Auto-assign Public IP:** *Enable*
38. 아래 화면에서 **Advanced Details** 섹션을 확장합니다.
39. 다음 코드 복사하여 **User data** 상자에 입력합니다.

```
#!/bin/bash
# Install Apache Web Server and PHP
yum install -y httpd mysql php
# Download Lab files
wget https://us-west-2-tcprod.s3.amazonaws.com/courses/ILT-TF-100-TECESS/v4.7.16/lab
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

이 스크립트는 인스턴스가 처음 실행될 때 자동으로 실행됩니다. 스크립트는 PHP 웹 응용 프로그램을 로드하고 구성하게 되어 있습니다.

40. Next: Add Storage 를 클릭합니다.

Storage의 기본 설정을 그대로 사용합니다.

41. Next: Add Tags 를 클릭합니다.

태그를 사용하여 리소스를 식별할 수 있습니다. 태그를 사용하여 인스턴스에 이름을 할당하십시오.

42. Add Tag 를 클릭하고 다음 설정을 구성합니다.
    - **Key**: `Name`
    - **Value**: `Web Server 1`
43. Next: Configure Security Group 을 클릭합니다.

이전에 생성한 *Web Security Group* 을 사용하도록 인스턴스를 구성하십시오.

44. **Select an existing security group** 을 선택합니다.
45. **Web Security Group** 을 선택합니다.

이전 작업에서 생성한 Security Group입니다. 인스턴스에 대한 HTTP 액세스를 허용합니다.

46. **Review and Launch** 를 클릭합니다.
47. 포트 22를 통해 인스턴스에 연결할 수 없다는 *Warning* 메시지가 표시되면 **Continue** 를 클릭합니다.
48. 인스턴스 정보를 확인한 후 **Launch** 를 클릭합니다.
49. *Select existing key pair or create a new key pair* 의 팝업 화면이 보입니다. 이 화면은 keypair를 선택 하는 화면입니다. **I acknowledge...** 으로 시작하는 확인란을 선택합니다.
50. **Launch Instances** 를 클릭합니다. 그리고 이어서 화면아래 **View Instances** 를 클릭합니다.
51. **Web Server 1** 의 **Status Checks** 열에 *2/2 checks passed*가 표시될 때까지 기다립니다.

3~5분 정도 걸립니다. 오른쪽 상단 창에 있는 새로 고침 아이콘 을 30초 단위로 클릭하여 업데이트를 확인합니다.

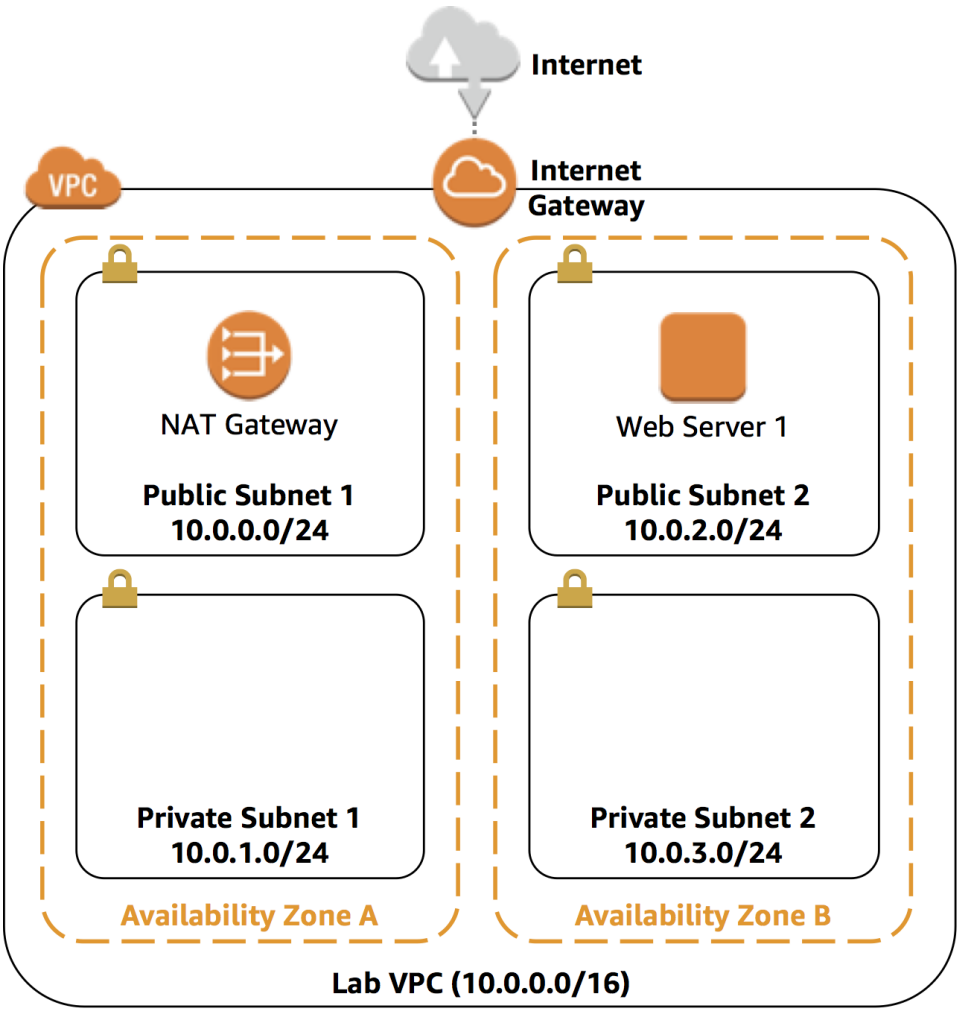
이제 EC2 인스턴스에서 실행 중인 웹 서버에 연결하십시오.

52. Web Server 1을 선택하고 **Details** 탭에서 **Public IPv4 address** 값을 복사합니다.
53. 새 웹 브라우저 창이나 탭에 위에서 복사한 **Public IPv4 address** 값을 붙여 넣고 **ENTER**를 누릅니다.

과제 3에서 *Web Security Group* 을 생성할 때 Http 포트만 허용했으므로, Http가 아닌 Https 포트를 사용하는 **open address** 링크를 클릭하지 않도록 주의합니다.

AWS 로고 및 인스턴스 메타데이터 값을 표시하는 웹 페이지가 보입니다.

구성된 전체 아키텍처:




**Public Route Table**

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | Internet Gateway |

**Private Route Table**

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | NAT Gateway |

# 실습 완료

축하합니다! 성공적으로 VPC를 생성하고 생성한 VPC에서 EC2 인스턴스를 시작했습니다.