

대학생을 위한 AWS 강의(20)

보안그룹

서진호

제 20 강 목표

- 보안과 방화벽
- 아마존 보안 그룹
- 아마존 보안 그룹의 주요 특징
- 아마존 보안 그룹 사용 예
- Stateful vs. Stateless
- 실습 – 보안 그룹을 활용하여 보안 강화하기



1. 보안과 방화벽

보안



AWS Identity and Access Management (IAM)



Amazon GuardDuty



AWS Shield



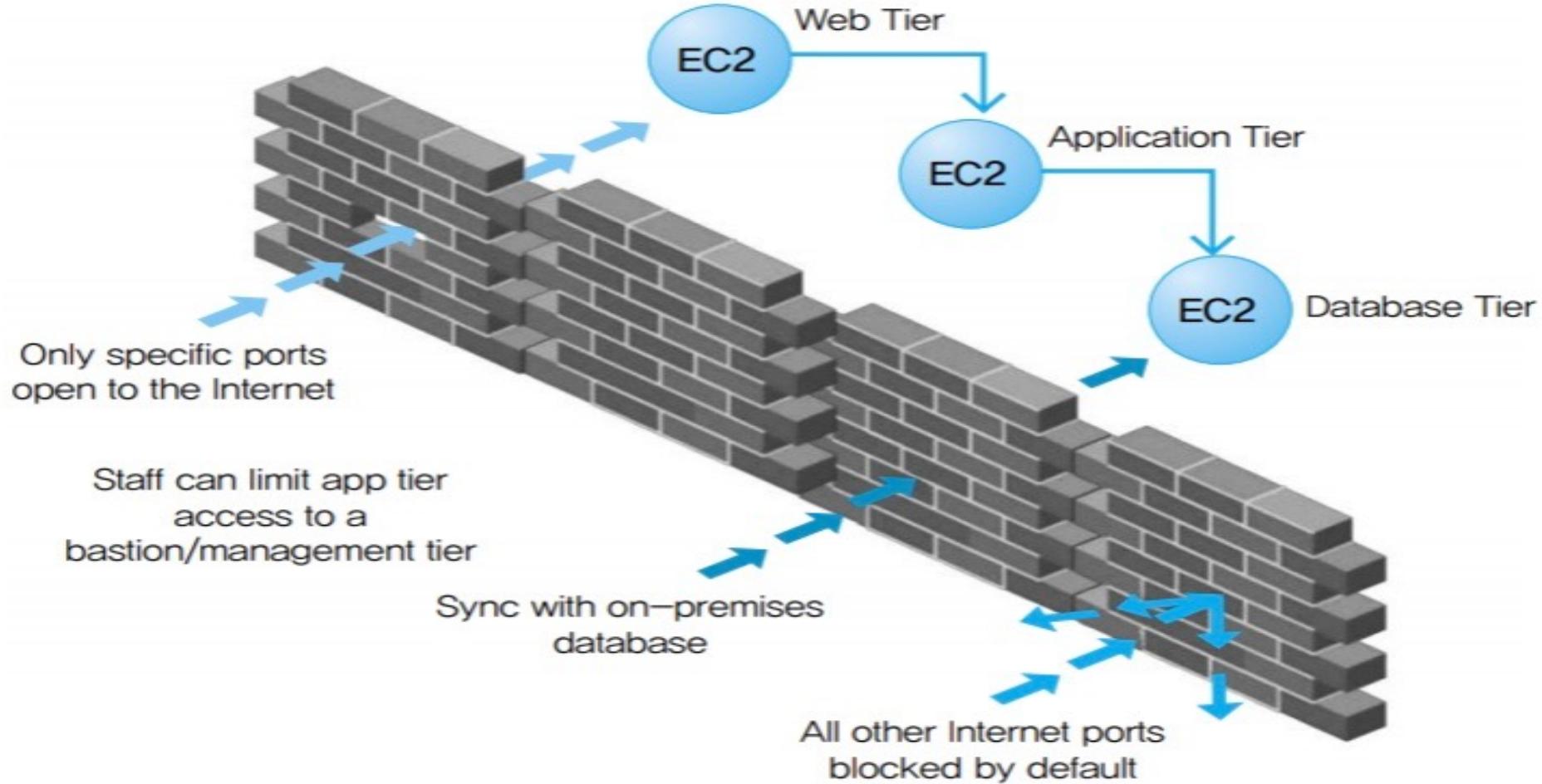
AWS WAF

방화벽



Network ACL

2. 아마존 보안 그룹



3. 아마존 보안 그룹의 주요 특징

EC2 > 보안 그룹 > sg-0c5bc4eb6dd10b7f2 - launch-wizard-3

sg-0c5bc4eb6dd10b7f2 - launch-wizard-3

작업 ▾

세부 정보			
보안 그룹 이름 launch-wizard-3	보안 그룹 ID sg-0c5bc4eb6dd10b7f2	설명 launch-wizard created 2022-06-08T07:03:25.664Z	VPC ID vpc-34dd415f
소유자 534520364753	인바운드 규칙 수 1 권한 항목	아웃바운드 규칙 수 1 권한 항목	

인바운드 규칙 아웃바운드 규칙 태그

ⓘ 이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다.

Reachability Analyzer 실행 X

인바운드 규칙 (1/1)		C	태그 관리	인바운드 규칙 편집	
<input type="text"/> 보안 그룹 규칙 필터		<	1	>	
<input checked="" type="checkbox"/>	Name	보안 그룹 규칙 ID	IP 버전	유형	프로토콜
<input checked="" type="checkbox"/>	-	sgr-0750444969d42c...	IPv4	SSH	TCP

4. 보안 그룹의 주요 기능 (1)

Security group

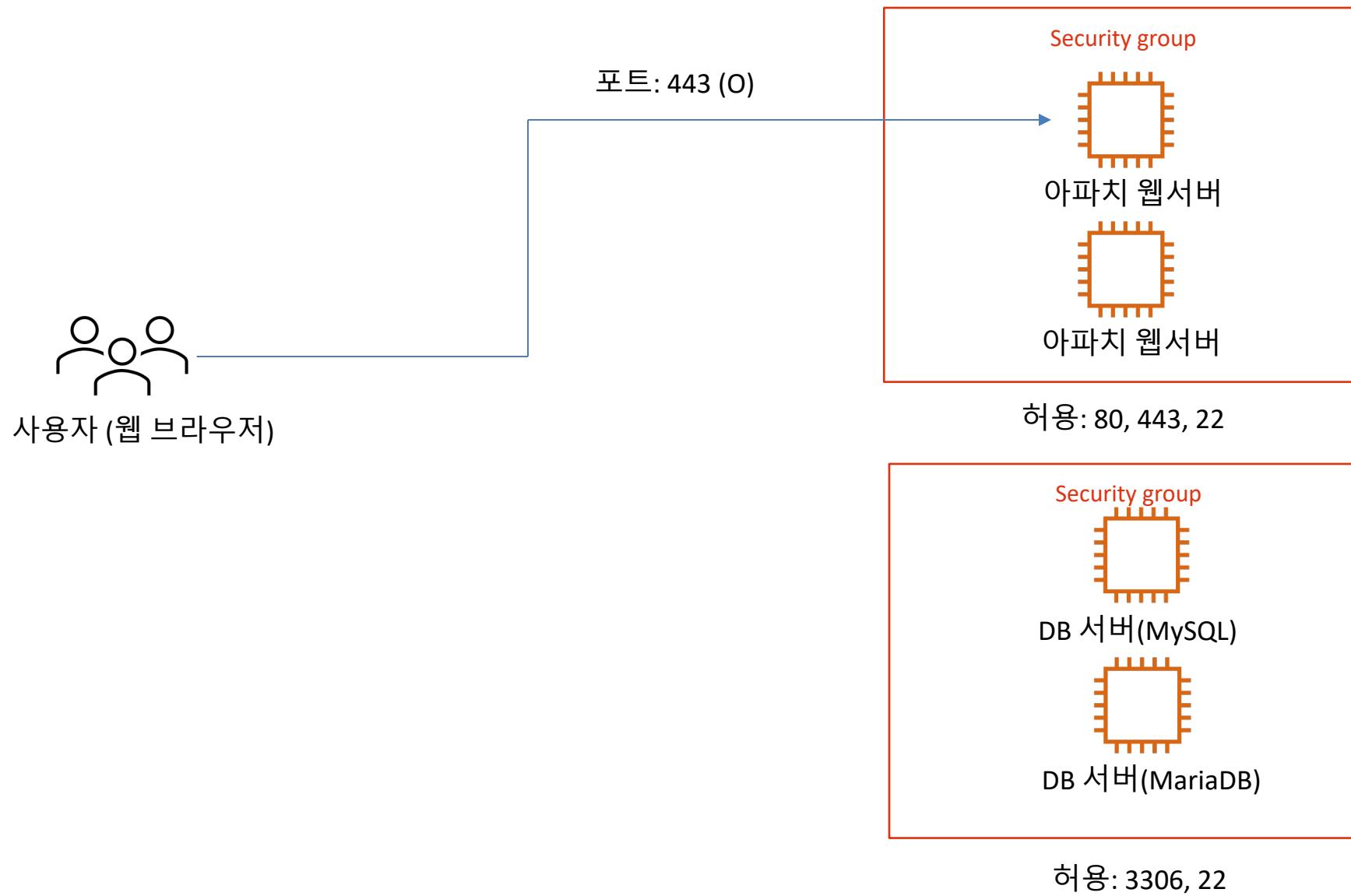
- 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽 역할
 - 인바운드: 밖에서 서버로 들어오는 통신
 - 아웃바운드: 서버에서 밖으로 나가는 통신
- VPC에서 인스턴스를 시작할 때 최대 5개의 보안 그룹에 인스턴스 할당
- 서브넷 수준이 아니라 인스턴스 수준에서 동작함
- VPC에 있는 서브넷의 각 인스턴스를 서로 다른 보안 그룹 집합에 할당
- EC2 인스턴스 시작할 때 특정 그룹을 지정하지 않으면 인스턴스가 자동으로 VPC의 기본 보안 그룹에 할당함.

5. 보안 그룹의 주요 기능 (2)

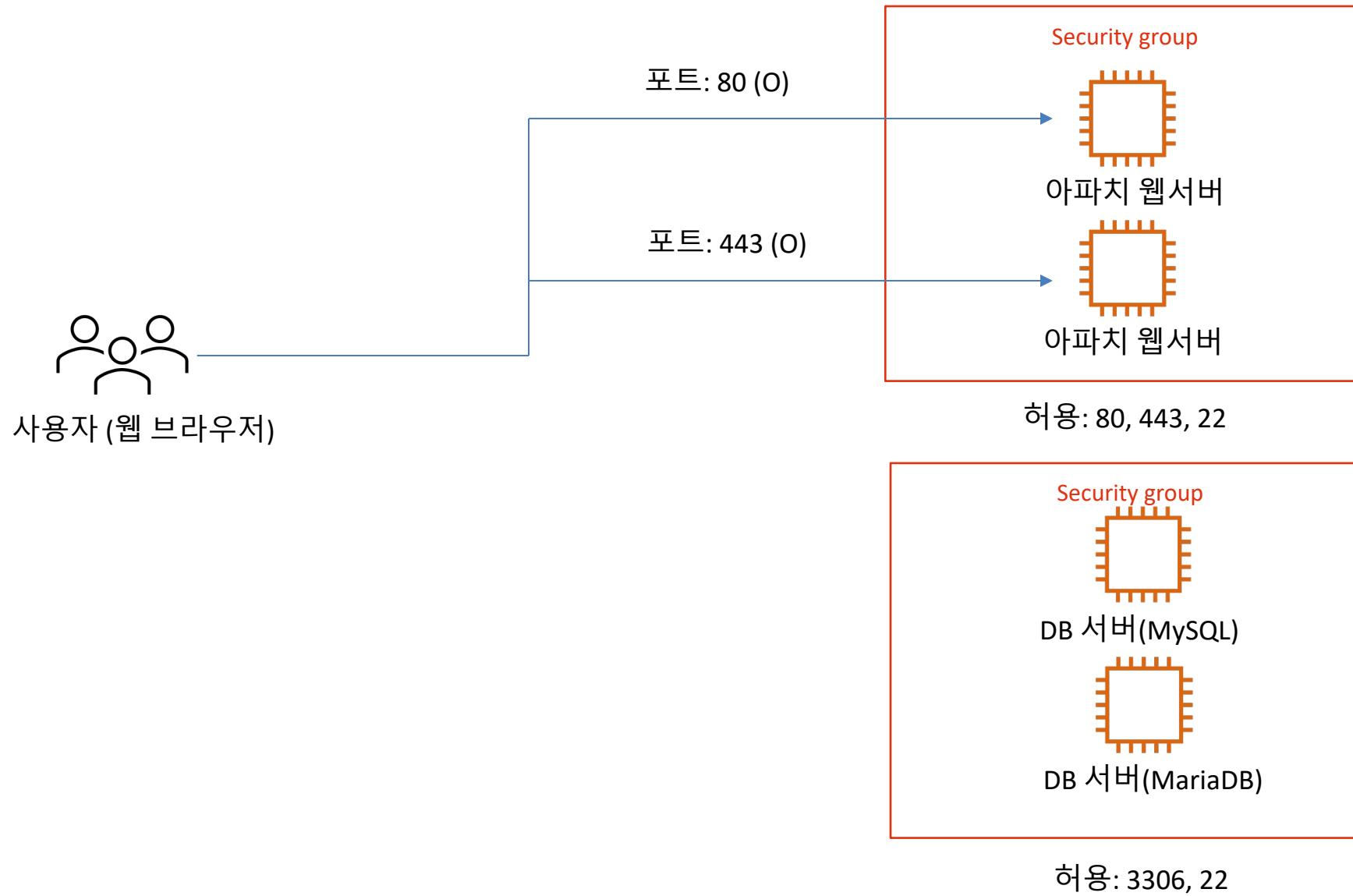
Security group

- 보안 장치
 - NACL (네트워크 액세스 컨트롤 리스트)와 함께 방화벽의 역할함. NACL과 차이점은 허용만 가능함. (차단 안됨)
 - 포트 허용
 - 트래픽이 지나갈 수 있는 원본IP와 포트를 설정 가능
 - 차단(Deny) 안됨
 - 인스턴스 단위
 - 하나의 인스턴스에 하나 이상의 보안 그룹 설정 가능
 - NACL 의 경우 서브넷 단위
 - 설정된 인스턴스는 설정한 모든 보안 그룹 규칙 적용 받음

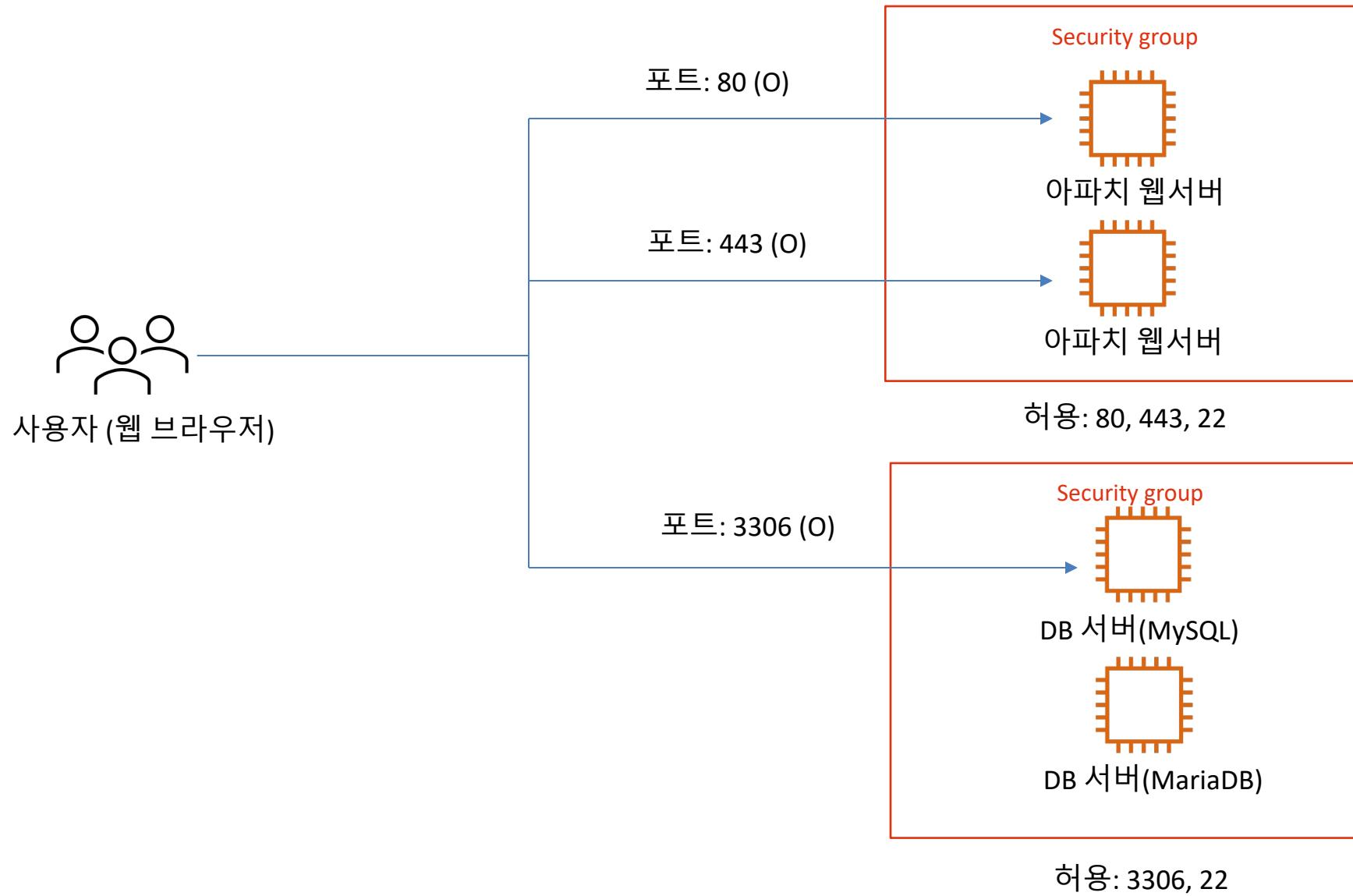
6. 보안 그룹 사용 예 (1)



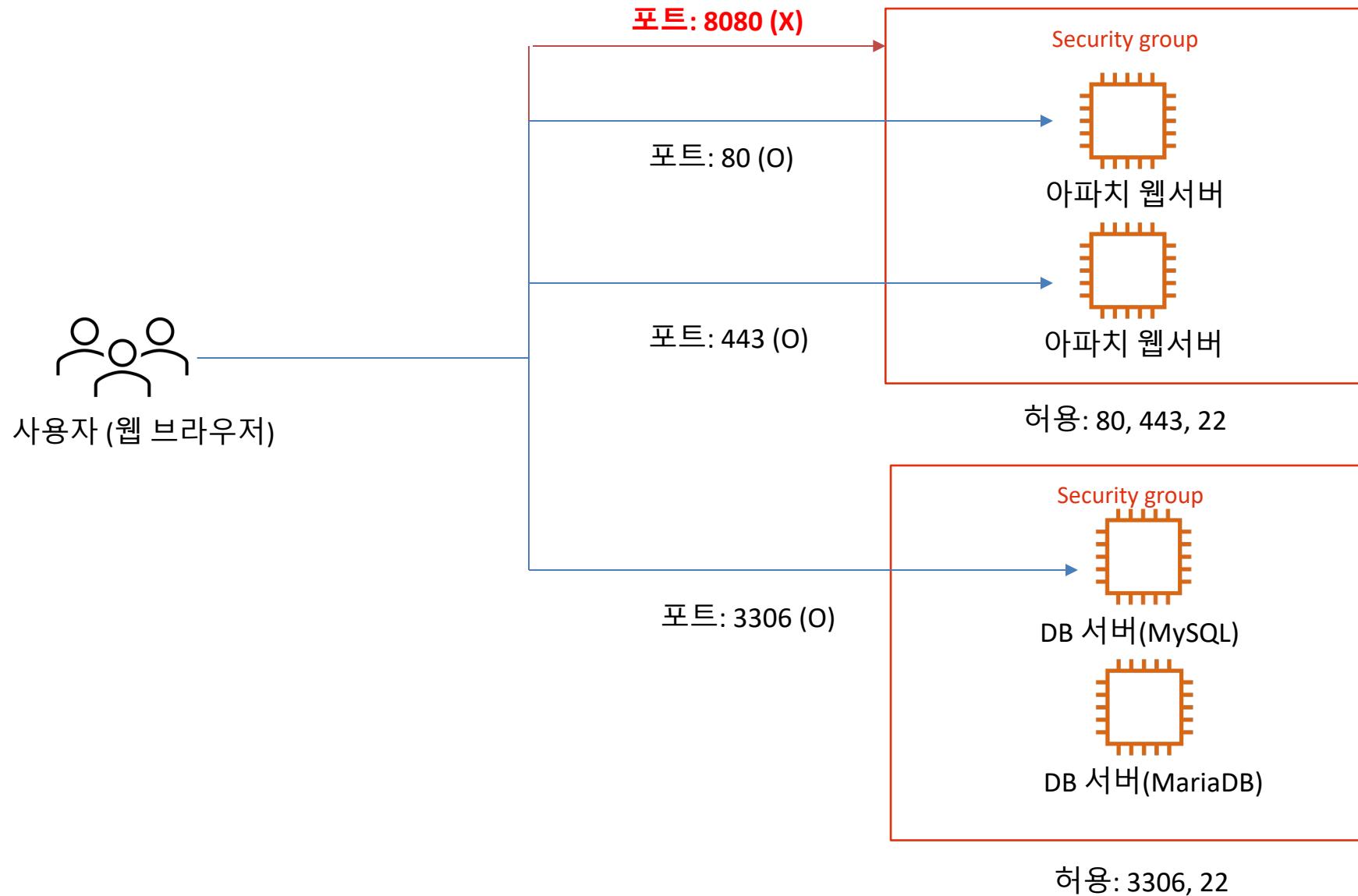
6. 보안 그룹 사용 예 (2)



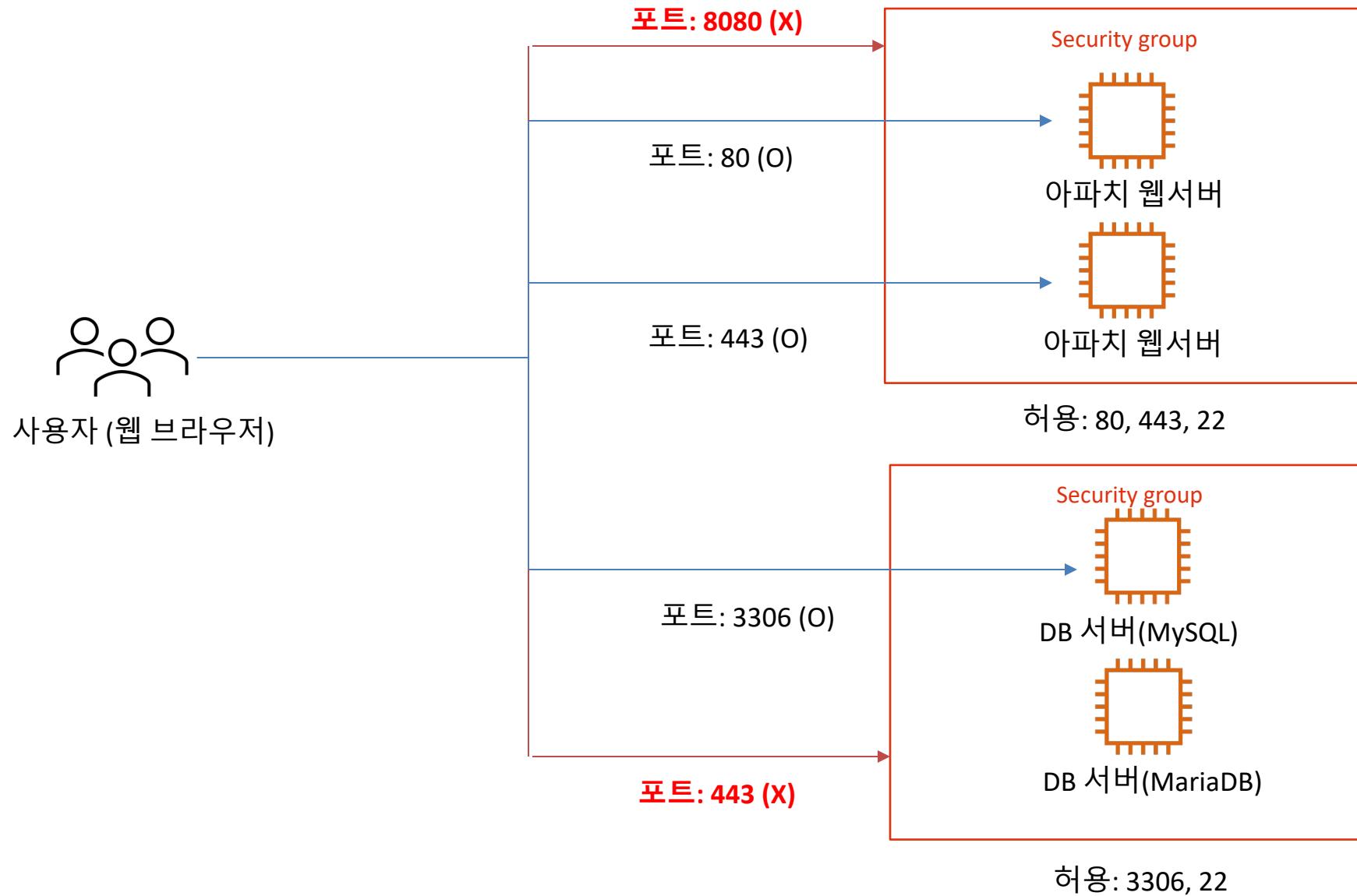
6. 보안 그룹 사용 예 (3)



6. 보안 그룹 사용 예 (4)



6. 보안 그룹 사용 예 (5)

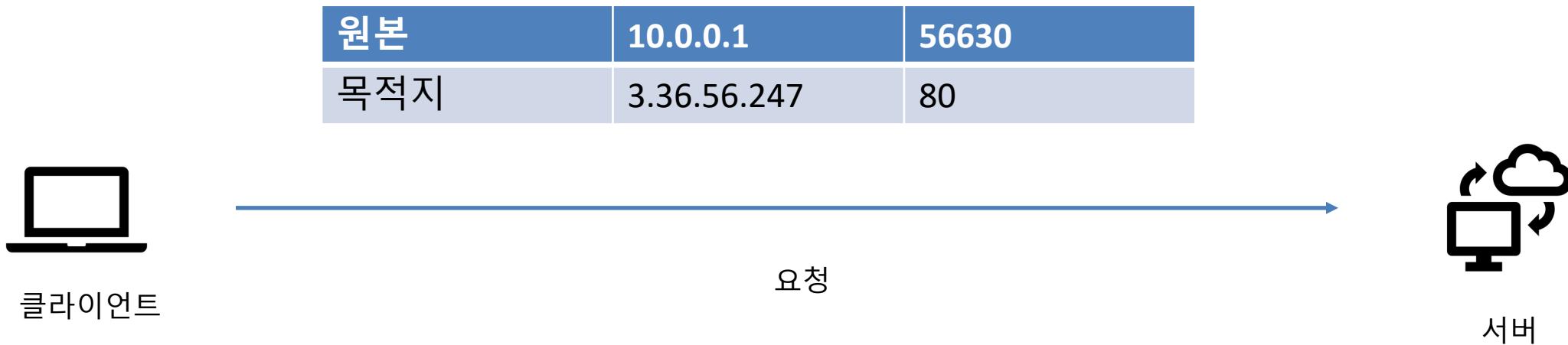


7. 보안 그룹과 NACL 관계

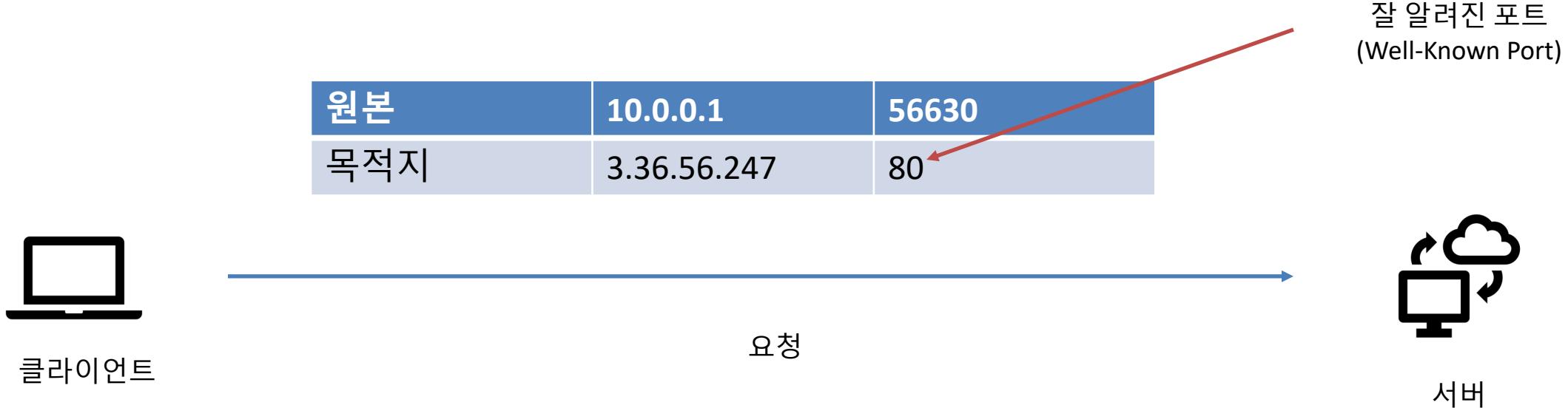
Security group

- 보안그룹:
 - 규칙 설정된 순서에 상관없이 규칙을 사용해서 필터링함
 - Stateful : 세션에 상태 값을 저장하고 있기 때문에 인바운드로 들어온 트래픽이 별다른 아웃바운드로 설정 없이 나갈 수 있음
- NACL
 - 규칙 설정된 순서에 따라 필터링함.
 - Stateless : 세션 상태로 저장하지 않기 때문에 허용과 차단 규칙에 의해 규칙을 적용함.

8. Stateful vs. Stateless (1)

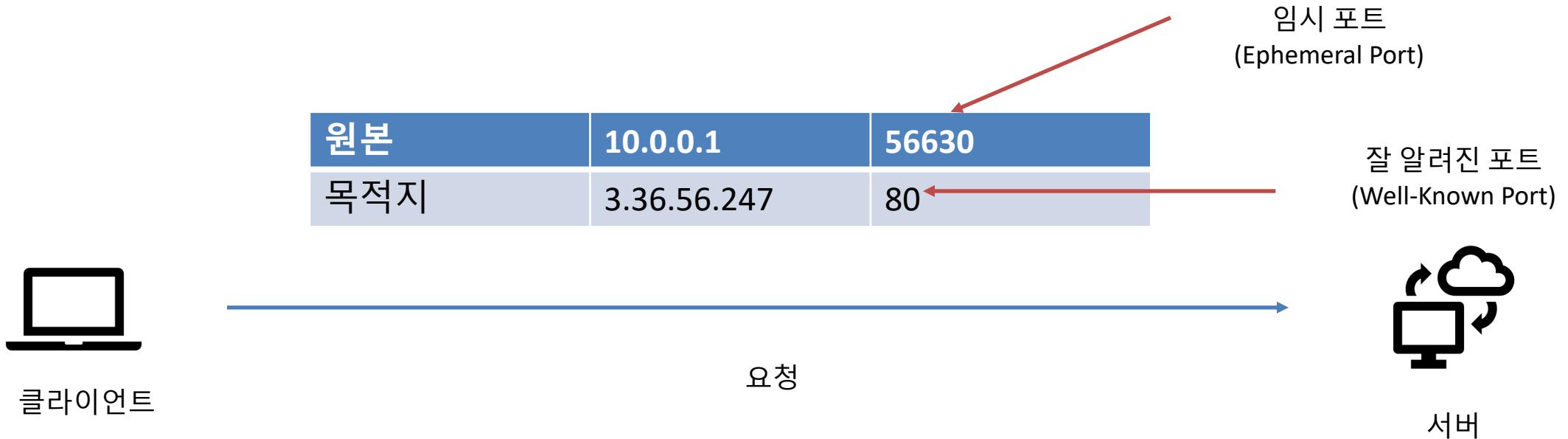


8. Stateful vs. Stateless (2)



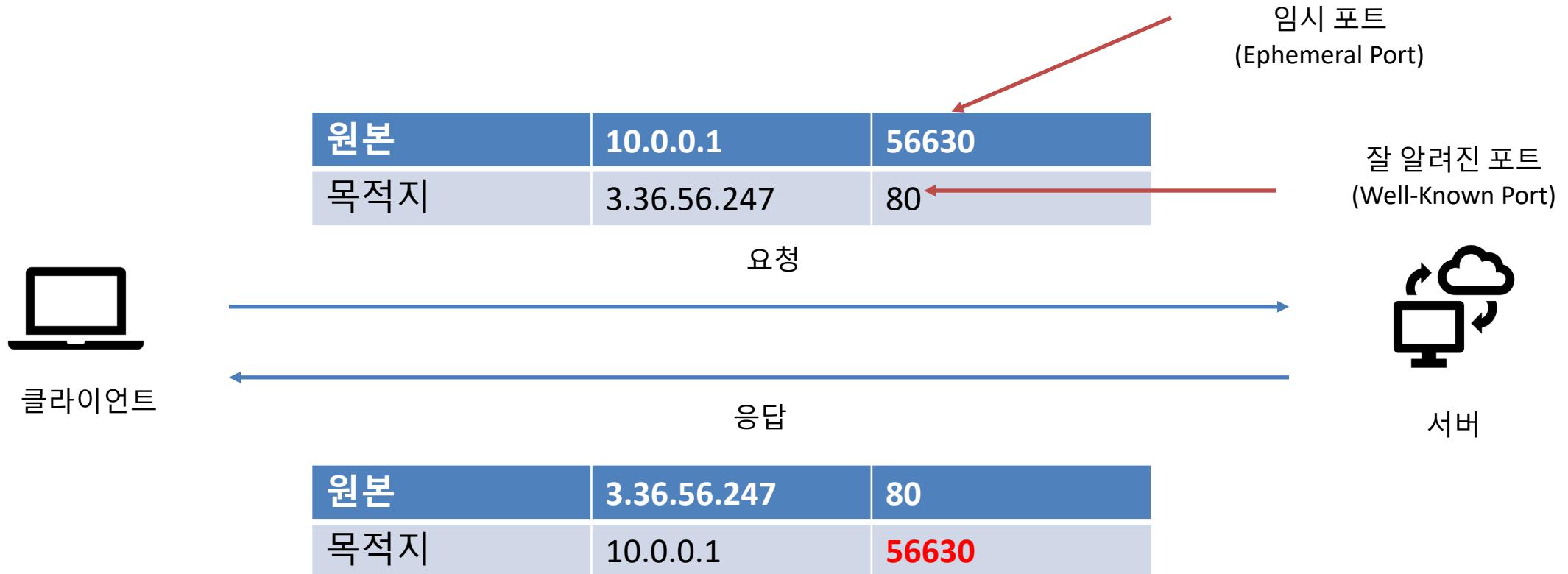
- 클라이언트 포트는 무작위로 열어 줌
 - 윈도우XP:
 - 리눅스:

8. Stateful vs. Stateless (3)

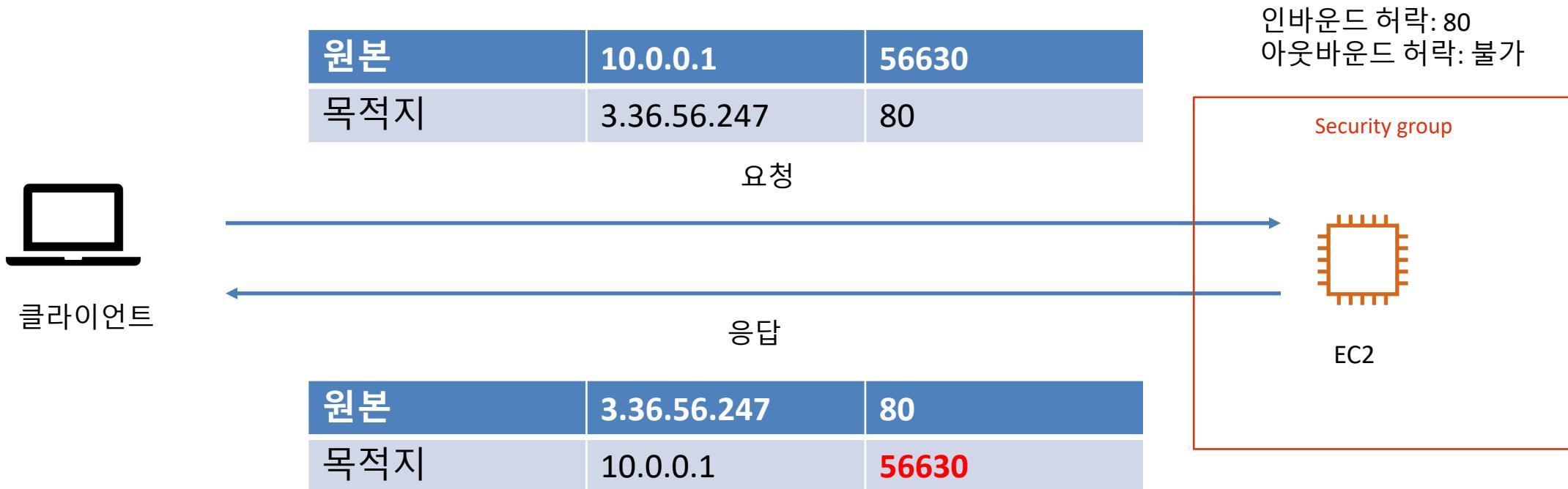


- 클라이언트 포트는 임시포트로 지정
- 윈도우XP: 1024 – 4999 (old BSD)
- 윈도우XP 이후: 49152-65535
- 리눅스 2.4 커널: 32768 - 61000

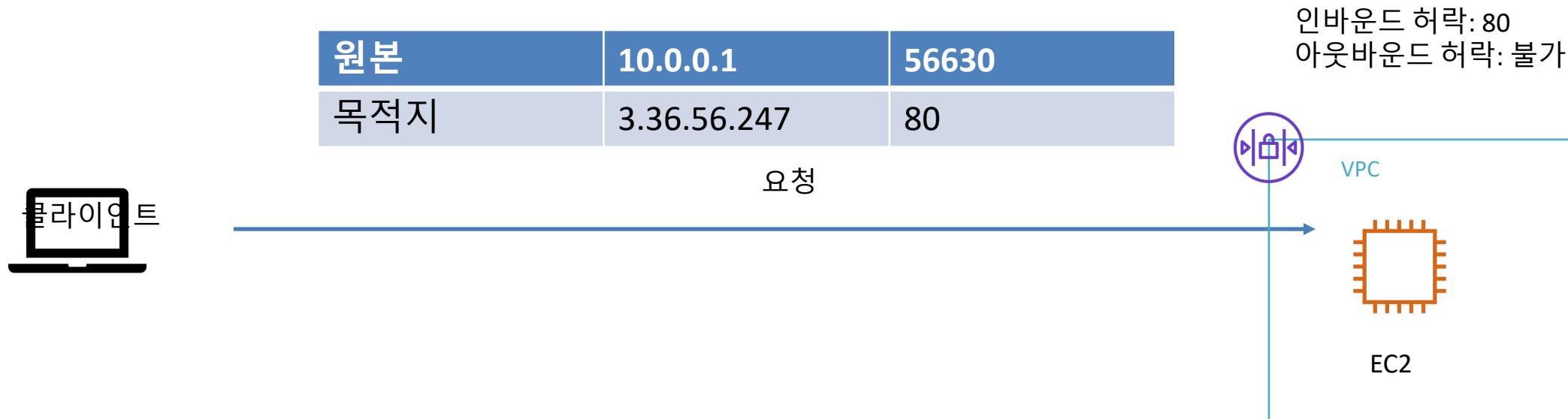
8. Stateful vs. Stateless (4)



9. Stateful



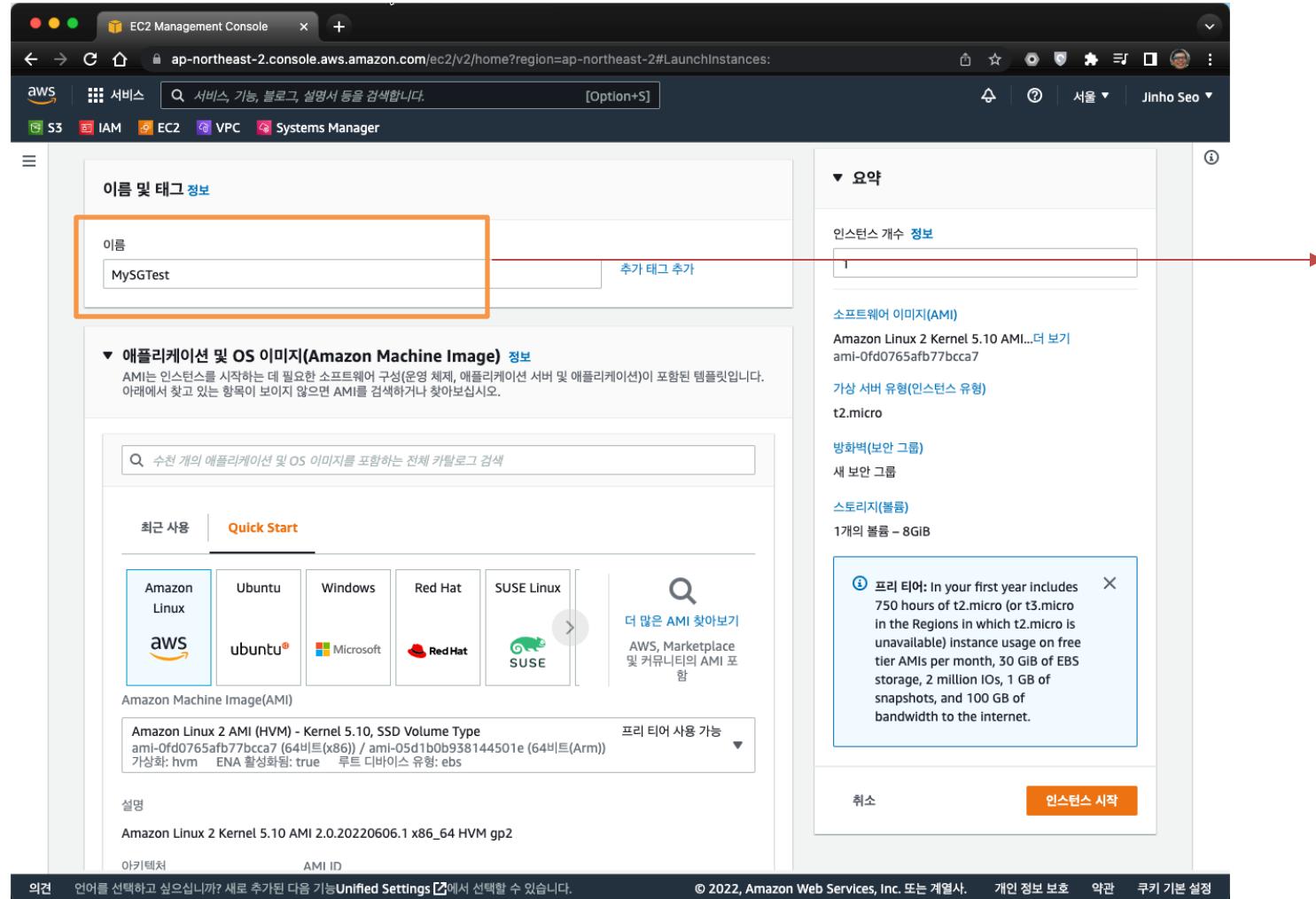
10. Stateless



실습 - 보안 그룹을 활용하여
보안 강화하기

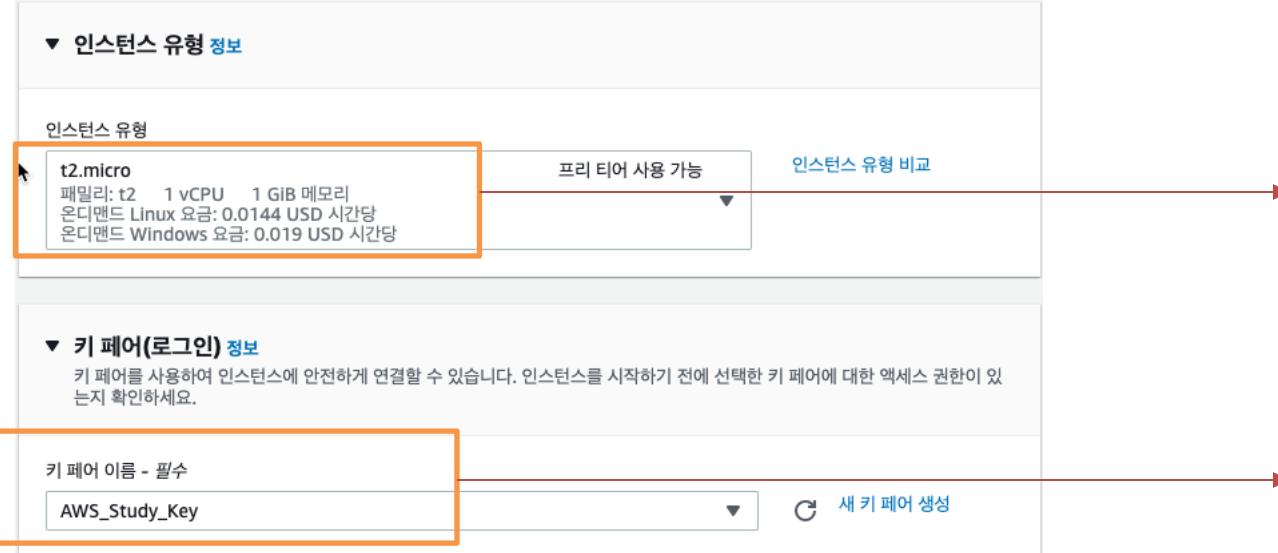


4-1. 실습 - 아파치 서버 실행을 위한 인스턴스 생성



이름: MySGTest
애플리케이션 및 OS 이미지:
아마존 리눅스 2

4-2. 실습 - 키 페어(로그인) 필요



T2.micro 그대로

SSH 연결 위해 키페어
이름 필요

4-3. 실습 - 네트워크 설정

EC2 Management Console

ap-northeast-2.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-2#LaunchInstances:

서비스, 기능, 블로그, 설명서 등을 검색합니다. [Option+S]

S3 IAM EC2 VPC Systems Manager

키 페어 이름 - 필수
AWS_Study_Key 새 키 페어 생성

네트워크 설정

VPC - 필수 정보
vpc-34dd415f 172.31.0.0/16 172.32.0.0/16 (기본값)

서브넷 정보
subnet-00aa246b VPC: vpc-34dd415f 소유자: 534520364753 사용 영역: ap-northeast-2a IP 주소 사용 가능: 4091 새 서브넷 생성

퍼블릭 IP 자동 할당 정보
활성화

방화벽(보안 그룹) 정보
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
 보안 그룹 생성 기존 보안 그룹 선택

보안 그룹 이름 - 필수
MySG-01

설명 - 필수 정보
MySG-01

인스턴스 개수 정보
1

소프트웨어 이미지(AMI)
Amazon Linux 2 Kernel 5.10 AMI... 더 보기 ami-0fd0765afb77bcc7

가상 서버 유형(인스턴스 유형)
t2.micro

방화벽(보안 그룹)
새 보안 그룹

스토리지(볼륨)
1개의 볼륨 – 8GiB

프리 티어: In your first year includes 750 hours of t2.micro (or t3.micro) in the Regions in which t2.micro is unavailable instance usage on free tier AMIs per month, 30 GB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

취소 인스턴스 시작

의견 언어를 선택하고 싶으십니까? 새로 추가된 다음 기능Unified Settings에서 선택할 수 있습니다.

© 2022, Amazon Web Services, Inc. 또는 계열사. 개인 정보 보호 약관 쿠키 기본 설정

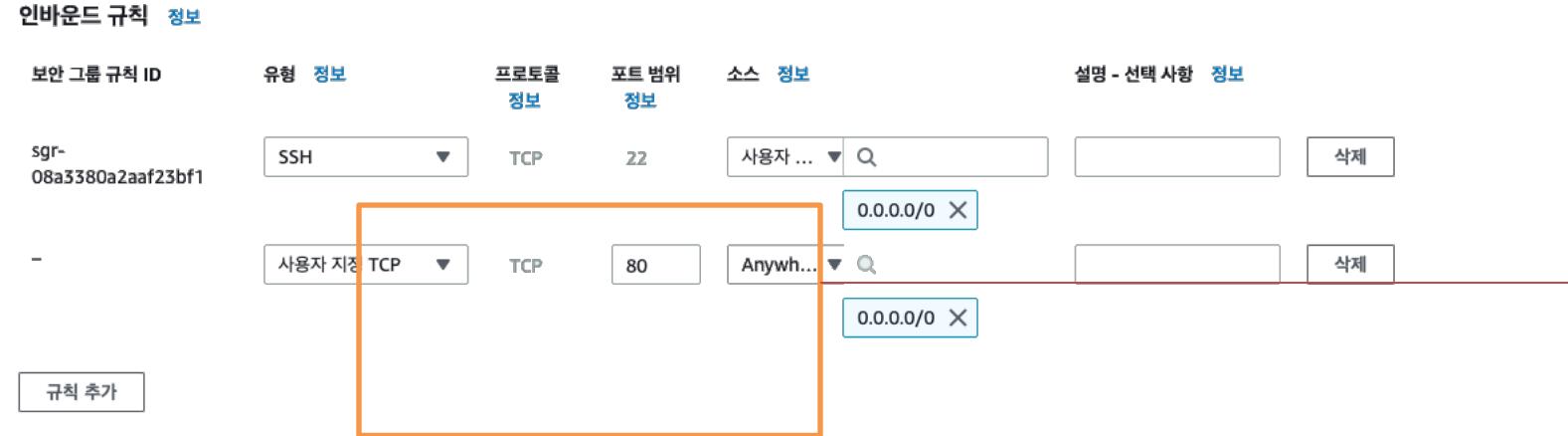
네트워크 설정 편집 클릭
서브넷 사용 영역: ap-northeast-2a
보안 그룹 이름: MySG-01

4-4. 실습 - 인바운드 규칙 편집

인바운드 규칙 정보

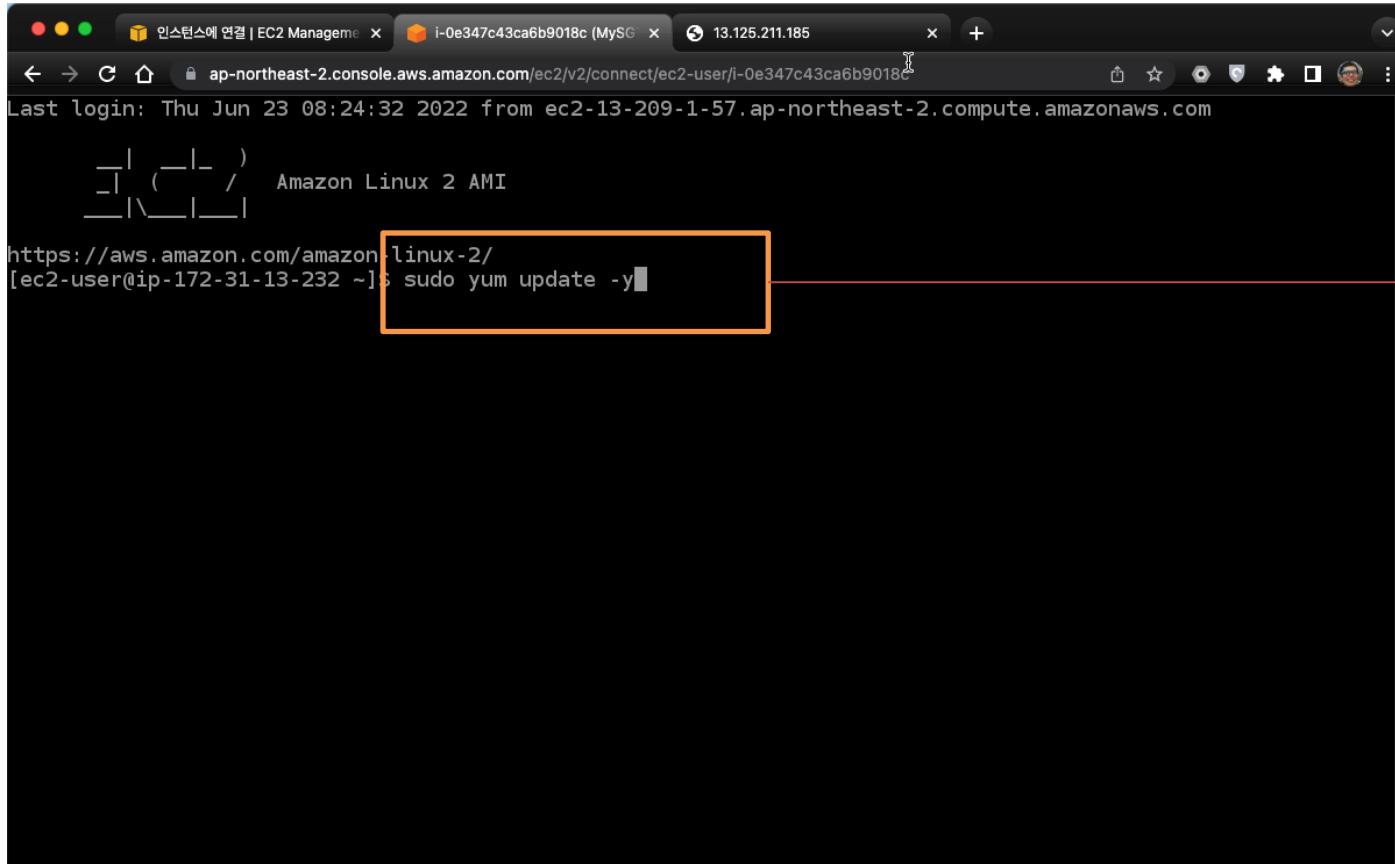
보안 그룹 규칙 ID	유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	설명 - 선택 사항 정보	삭제
sgr-08a3380a2aaaf23bf1	SSH	TCP	22	사용자 ... ▾	0.0.0.0/0 ×	삭제
-	사용자 지정 TCP	TCP	80	Anywhere ▾	0.0.0.0/0 ×	삭제

규칙 추가



- SSH 외에 웹서버 동작하는 것을 확인 하기 위해 Add security group role 선택
- HTTP 80, Anywhere IPv4, 0.0.0.0/0 CIDR 설정
- 그외 나머지는 그대로 두고 인스턴스 생성

4-5. 실습 - 인스턴스 생성 후 SSH 연결



```
Last login: Thu Jun 23 08:24:32 2022 from ec2-13-209-1-57.ap-northeast-2.compute.amazonaws.com
[ec2-user@ip-172-31-13-232 ~]$ sudo yum update -y
```

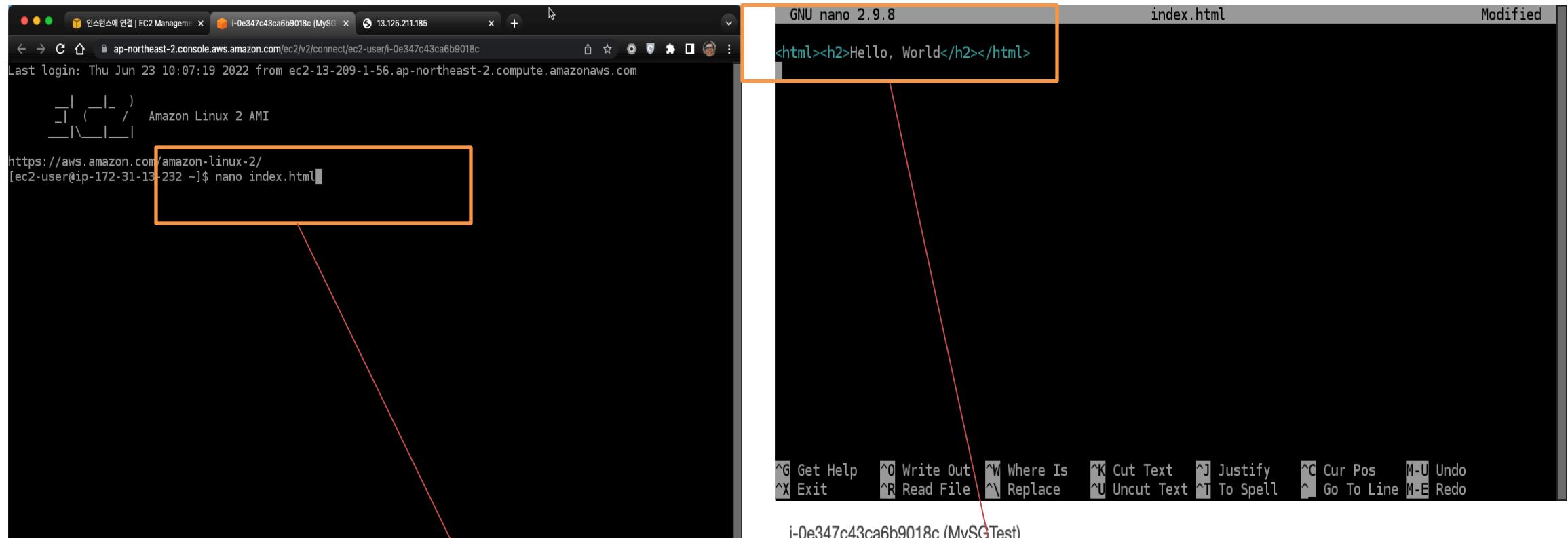
- EC2 인스턴스 연결
- 리눅스 아파치 서버 설치 및 업데이트

sudo yum install -y
sudo yum update -y

i-0e347c43ca6b9018c (MySGTest)

퍼블릭 IP: 13.125.211.185 프라이빗 IP: 172.31.13.232

4-6. 실습 - nano 에디터로 index.html 편집



i-0e347c43ca6b9018c (MySGTest)

퍼블릭 IP: 13.125.211.185 프라이빗 IP: 172.31.13.232

sudo nano index.html

<html><h2>Hello, World</h2></html>
CTRL+X 를 누르면 Y (Save)됨

4-7. 실습 - 리눅스 아파치 서버 실행

The screenshot shows a terminal window titled 'ap-northeast-2.console.aws.amazon.com/ec2/v2/connect/ec2-user/i-0e347c43ca6b9018c' with the IP '13.125.211.185'. The terminal session is as follows:

```
[ec2-user@ip-172-31-13-232 ~]$ sudo -s
[root@ip-172-31-13-232 ec2-user]# yum install httpd -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
Package httpd-2.4.53-1.amzn2.x86_64 already installed and latest version
Nothing to do
[root@ip-172-31-13-232 ec2-user]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-13-232 ec2-user]# chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
[root@ip-172-31-13-232 ec2-user]# dir
index.html
[root@ip-172-31-13-232 ec2-user]# cp index.html /var/www/html/index.html
cp: overwrite '/var/www/html/index.html'? y
[root@ip-172-31-13-232 ec2-user]#
```

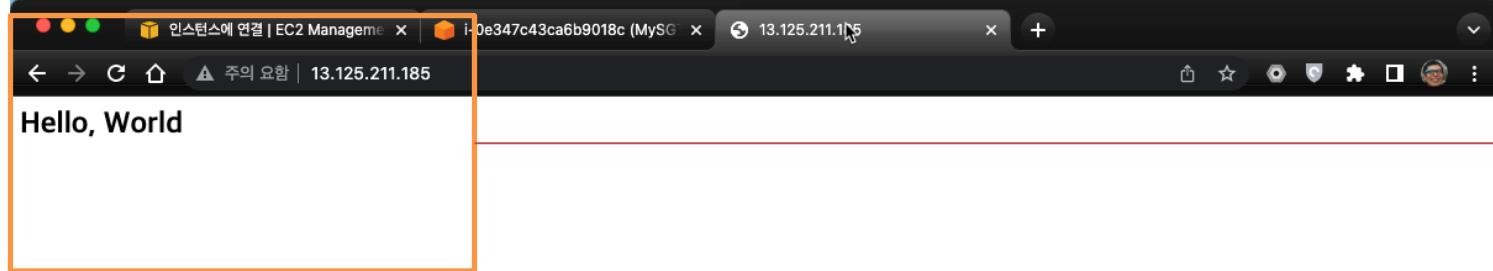
A red arrow points from the terminal output to the command 'sudo -s'.

sudo -s
service httpd start
chkconfig httpd on
dir
cp index.html
/var/www/html/index.html

i-0e347c43ca6b9018c (MySGTest)

퍼블릭 IP: 13.125.211.185 프라이빗 IP: 172.31.13.232

4-8. 실습 - IP주소로 웹서버 실행 확인



퍼블릭 IP 주소 복사:
<http://13.125.211.185/>

(각자마다 생성 IP 주소 다름)

4-9. 실습 - 보안그룹 변경 (아웃바운드 삭제)

The screenshot shows the AWS EC2 Management Console with the URL ap-northeast-2.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-2#SecurityGroup:securityGroupId=sg-0933be77469146f10. The left sidebar includes links for New EC2 Experience, EC2 대시보드, EC2 글로벌 보기, 이벤트, 태그, 제한, 인스턴스 (New), 인스턴스 유형, 시작 템플릿, 스팟 요청, Savings Plans, 예약 인스턴스 (New), 전용 호스트, 용량 예약, 이미지 (AMI New), AMI 카탈로그, and Elastic Block Store. The main content area displays the security group details for 'MySG-01' (sg-0933be77469146f10) with a VPC ID of 'vpc-34dd415f'. Below this, the 'Outbound Rules' tab is selected, showing one rule: '아웃바운드 규칙 (1/1)' with 'Name' as '-' and 'IP 버전' as 'IPv4', '유형' as '모든 트래픽', and '프로토' as '전체'. A tooltip message says '이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다.' and a 'Reachability Analyzer 실행' button is shown. A red callout arrow points from the 'Delete' button in the table header to the explanatory text on the right.

세부 정보

보안 그룹 이름 MySG-01	보안 그룹 ID sg-0933be77469146f10	설명 MySG-01	VPC ID vpc-34dd415f
소유자 534520364753	인바운드 규칙 수 2 권한 항목	아웃바운드 규칙 수 1 권한 항목	

인바운드 규칙 | 아웃바운드 규칙 | 태그

아웃바운드 규칙 (1/1)

Name	IP 버전	유형	프로토
-	IPv4	모든 트래픽	전체

Reachability Analyzer 실행

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다.

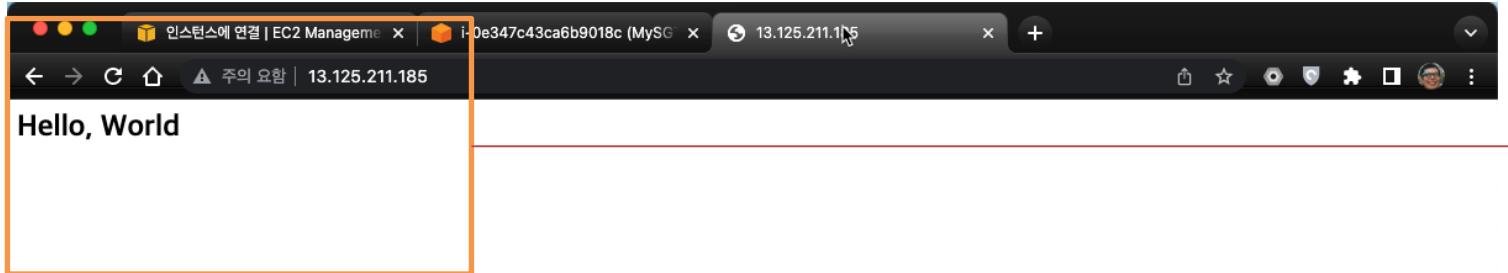
보안 그룹 규칙 필터

태그 관리 | 아웃바운드 규칙 편집

의견 언어를 선택하고 싶으십니까? 새로 추가된 다음 기능Unified Settings에서 선택할 수 있습니다. © 2022, Amazon Web Services, Inc. 또는 계열사. 개인 정보 보호 약관 쿠키 기본 설정

아웃바운드 규칙 편집 ->
아웃바운드 규칙 삭제 ->
규칙 저장

4-10. 실습 - IP주소로 웹서버 다시 확인



웹브라우저 새로고침해도 잘 나옴

이유: 아웃바운드
삭제했음에도 불구하고 세션
상태가 Stateful 하기 때문

즉, 나가는 트래픽과 들어오는
트래픽이 동일한 트래픽으로
적용하기 때문에
보안그룹에서는 stateful 로
지정됨.

4-11. 실습 - 보안그룹 변경 (인바운드 삭제)

EC2 Management Console

3.36.56.247

ap-northeast-2.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-2#ModifyInboundSecurityGroupRule... : 서울 Jinho Seo

S3 IAM EC2 VPC Systems Manager

EC2 > 보안 그룹 > sg-0933be77469146f10 - MySG-01 > 인바운드 규칙 편집

인바운드 규칙 편집 정보

인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙 정보					
보안 그룹 규칙 ID	유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	설명 - 선택 사항 정보
sgr-0491c0bbcc2404f02	HTTP	TCP	80	사용자 ...	0.0.0.0/0
sgr-08a3380a2aaf23bf1	SSH	TCP	22	사용자 ...	0.0.0.0/0

규칙 추가

취소

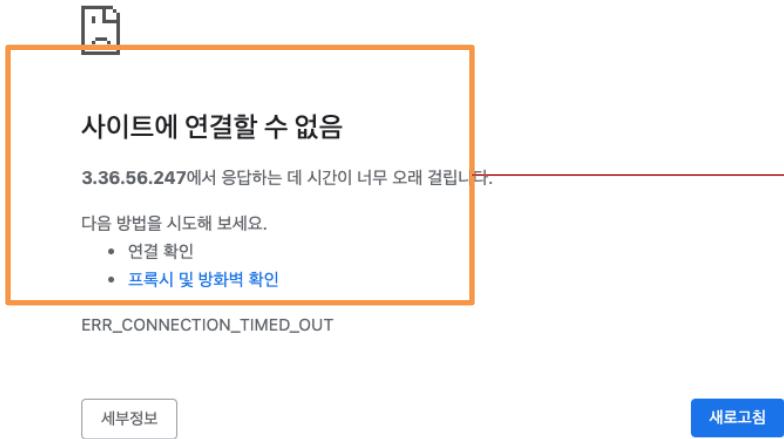
변경 사항 미리 보기

규칙 저장

의견 언어를 선택하고 싶으십니까? 새로 추가된 다음 기능Unified Settings에서 선택할 수 있습니다. © 2022, Amazon Web Services, Inc. 또는 계열사. 개인 정보 보호 약관 쿠키 기본 설정

인바운드 규칙 편집 -> HTTP
80만 인바운드 규칙 삭제 ->
규칙 저장

4-12. 실습 - IP주소로 웹서버 다시 확인



인바운드 규칙에서 HTTP 80 포트를 삭제했으니 허락하지 않는다는 의미이고 웹브라우저 새로고침하면 오랫동안 웹브라우저가 접속(빙글빙글 돌다가)해서 Hello, world 가 나오지 않고 접근 에러 발생

4-13. 실습 - 보안그룹 변경 (인바운드 추가)

EC2 Management Console

3.36.56.247

ap-northeast-2.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-2#ModifyInboundSecurityGroupRule... 서울 Jinho Seo

S3 IAM EC2 VPC Systems Manager

EC2 > 보안 그룹 > sg-0933be77469146f10 - MySG-01 > 인바운드 규칙 편집

인바운드 규칙 편집 정보

인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙 정보									
보안 그룹 규칙 ID	유형	정보	프로토콜	포트 범위	소스	정보	설명	선택 사항	정보
sgr-08a3380a2aaaf23bf1	SSH		TCP	22	사용자 ...				
-	HTTP		TCP	80	Anywhere				

0.0.0.0/0 X
0.0.0.0/0 X

규칙 추가

취소

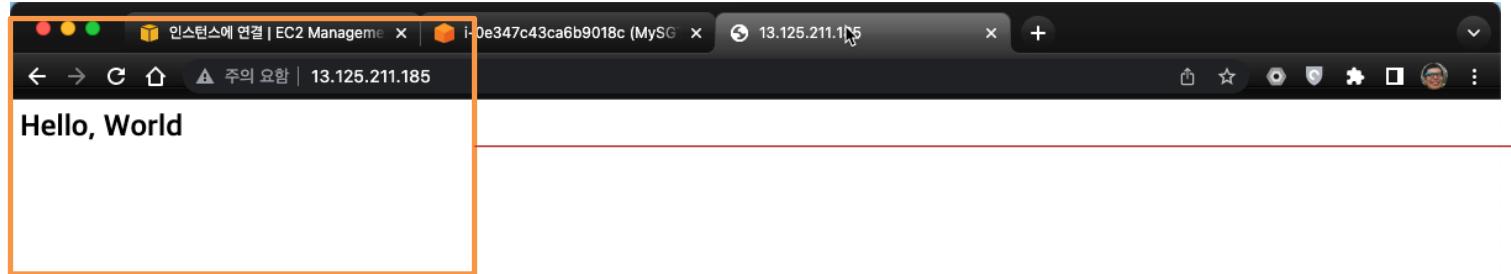
변경 사항 미리 보기

규칙 저장

의견 언어를 선택하고 싶으십니까? 새로 추가된 다음 기능Unified Settings에서 선택할 수 있습니다. © 2022, Amazon Web Services, Inc. 또는 계열사. 개인 정보 보호 약관 쿠키 기본 설정

인바운드 규칙 편집 -> HTTP
80만 인바운드 규칙 추가 ->
규칙 저장

4-14. 실습 - IP주소로 웹서버 다시 확인



웹브라우저 새로 고침하면
원래대로 Hello, World 가
나옴