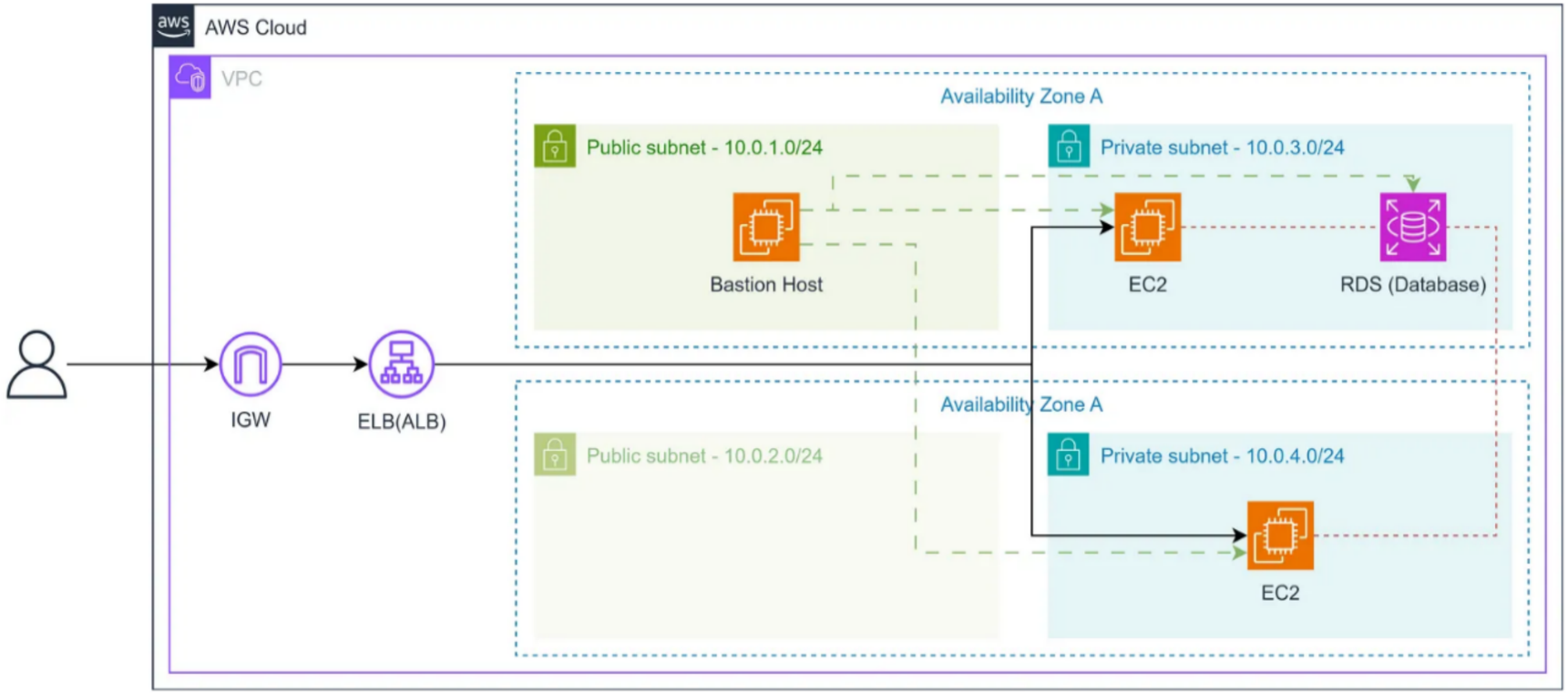
— EC2 Bastion Host



Null4U, 20201 경대영

목차

1.BastionHost란?

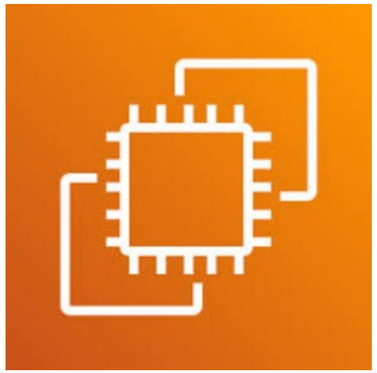
Bastion Host는 Public IP를 가지며 Public 서브넷에 위치한 SSH 접속 전용 서버로,

외부에서 Private 서브넷의 서버에 안전하게 접근하기 위한 중간 관문임.

2.아키텍처 설명

아키텍처에서 사용한 기능

ELB



EC2

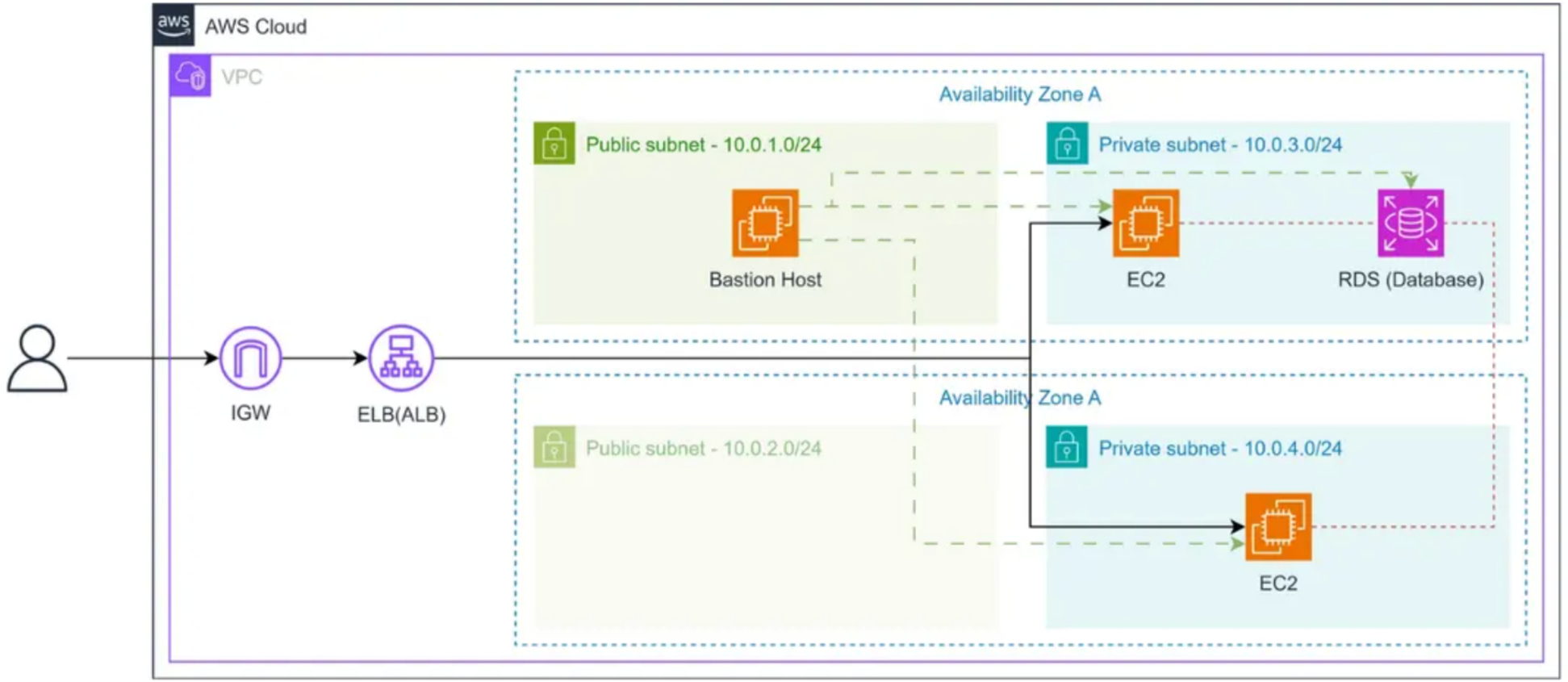
RDS

(등등..)

2.아키텍처 설명 (요약)

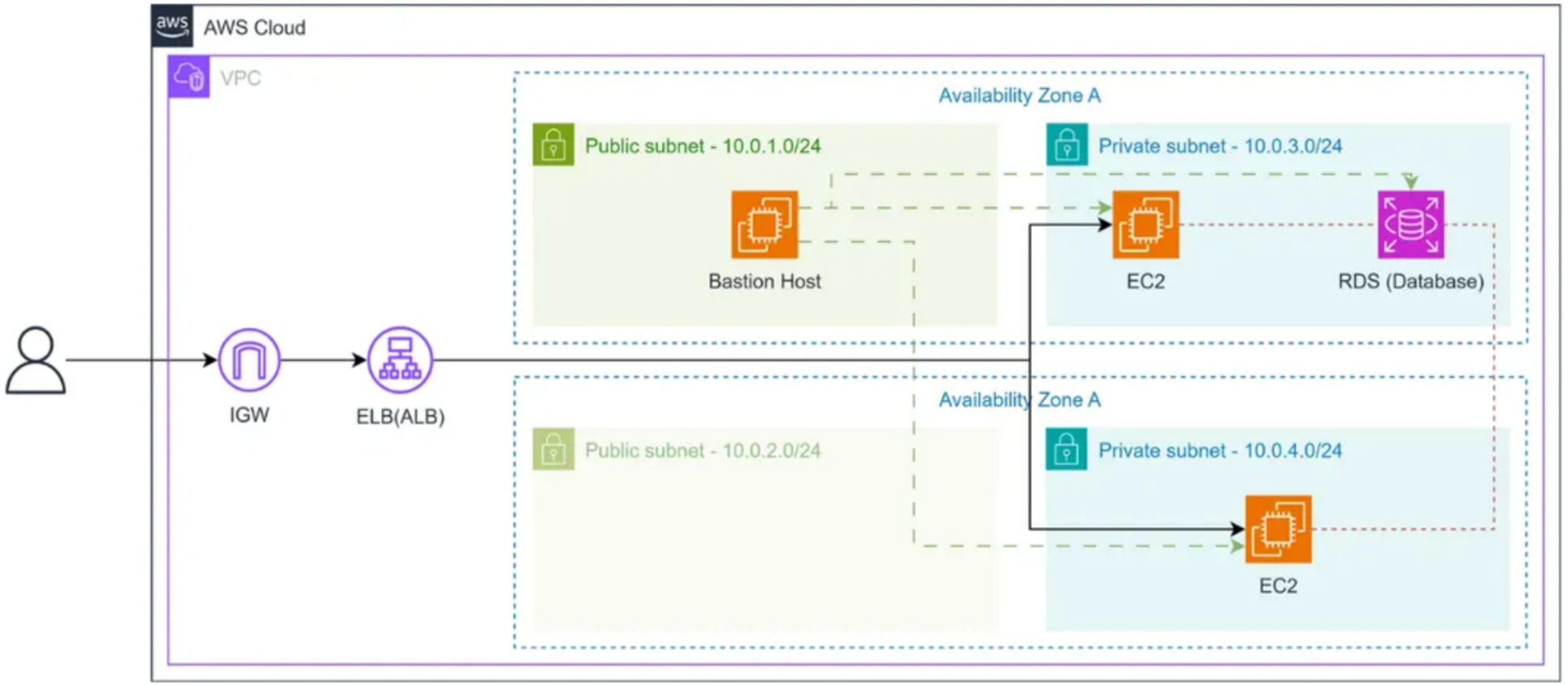
사용자의 트래픽은 ELB(ALB)로 받아 Private EC2 및 Private RDS로 처리됨.

이때 Bastion Host를 통해 Private EC2 및 Private RDS에 접근할 수 있는 구조 (인프라 관리용)



2.아키텍처 설명

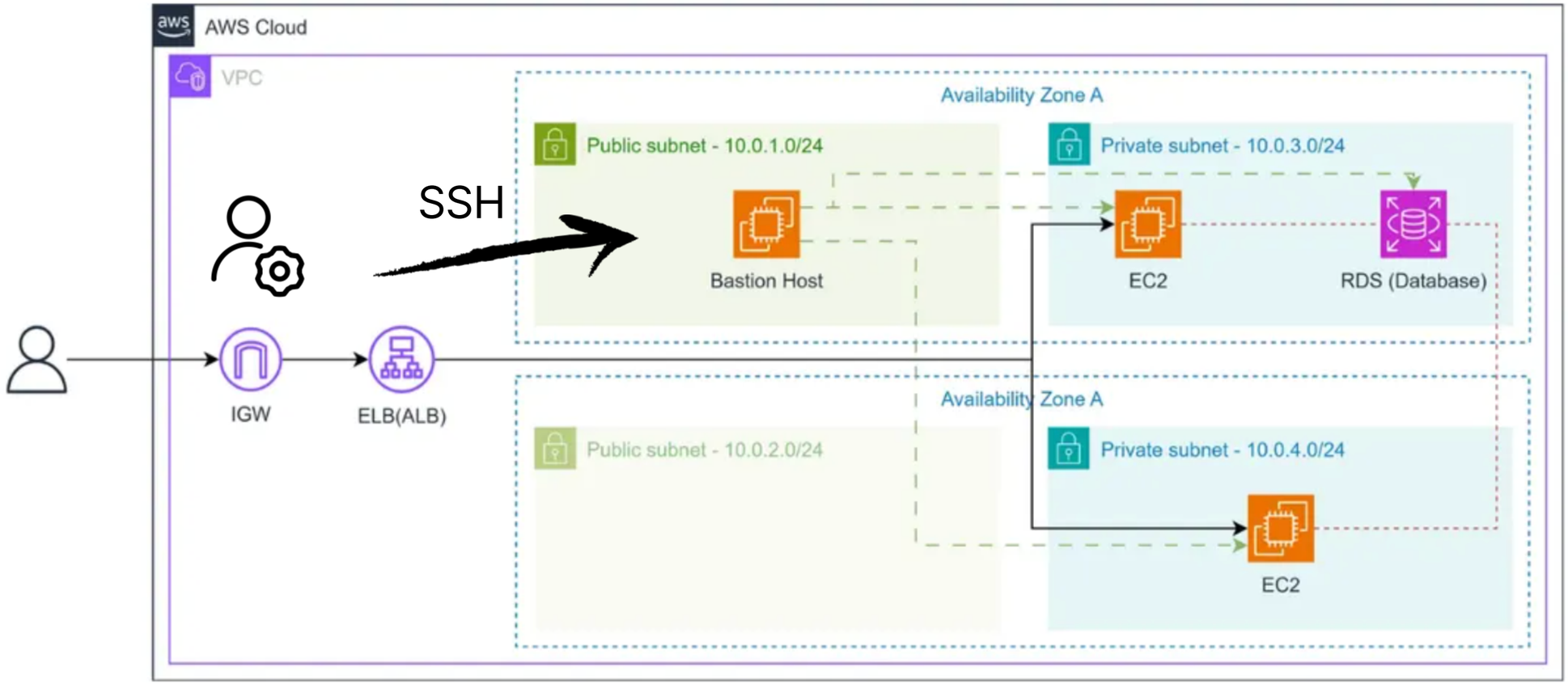
관리자 접근 방법



2.아키텍처 설명

관리자 접근 방법

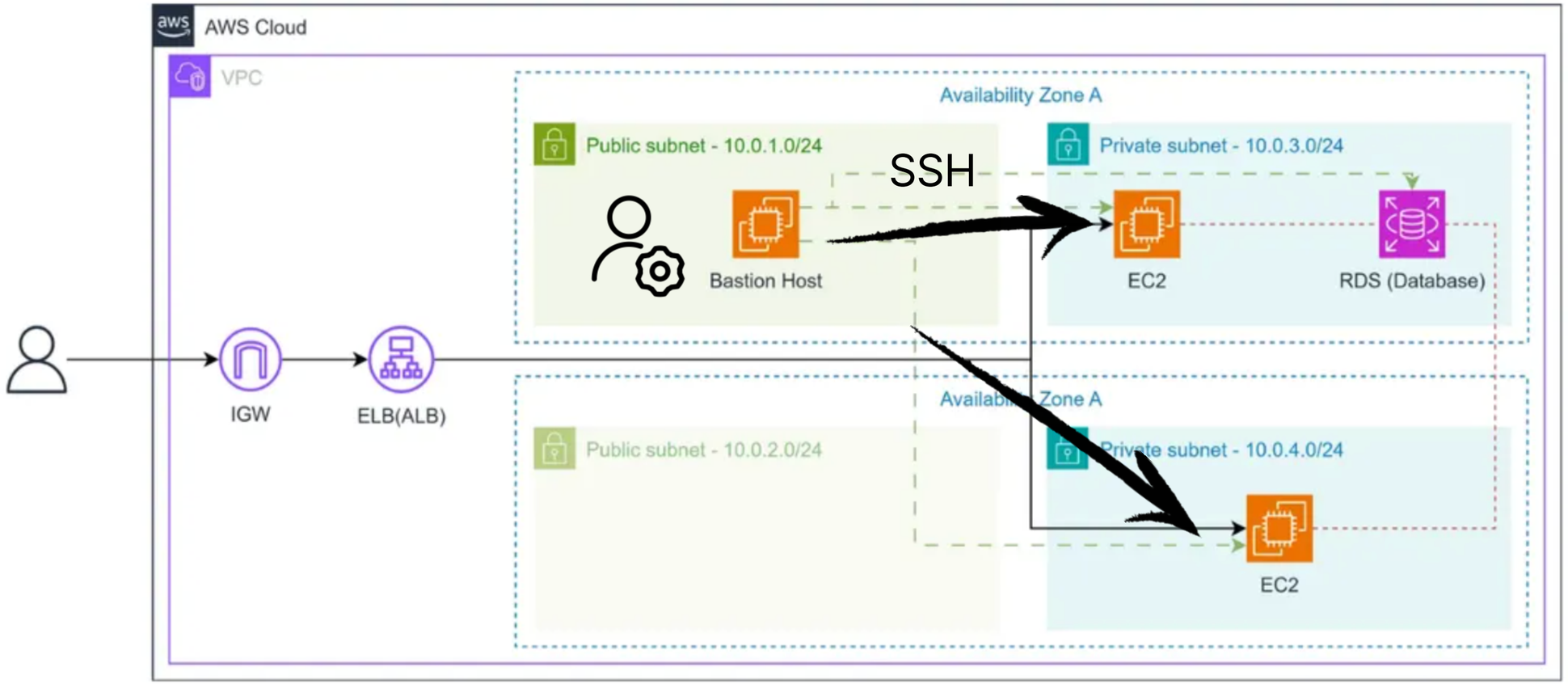
관리자는 Internet Gateway를 통해 퍼블릭 서브넷에 있는 Bastion Host에 SSH로 접속하고



2.아키텍처 설명

관리자 접근 방법

프라이빗 서브넷의 EC2 사설(Private) IP 로 접근



2.아키텍처 설명

요약하자면:

인터넷 외부 > Bastion Host(Public IP로 SSH 접속) > Private Servers(Private IP로 SSH 접속)

키페어 키페어

2.아키텍처 설명

Bastion Host로 얻을수 있는 장점

1. 내부 서버(Private EC2)를 인터넷에 직접 노출하지 않고 외부와 연결(보안 강화)
   = Private EC2에 Public IP 없이도 관리 접근이 가능

2. 모든 관리 접속을 하나의 서버로 통제할 수 있음

2.아키텍처 설명

Bastion Host 단점

1. Bastion Host로 인한 민감한 보안 문제가 발생할 수 있음(내부에 접속할 수 있기 때문)

(마지막에 다시 설명)

2. Bastion Host를 위한 별도의 EC2 인스턴스를 프로비저닝 할 필요가 있음

그래서 AWS에선 SSM EC2 Session 기능을 제공하는데,
Private EC2 + SSH 인바운드 허용 없이도 원격으로 접속 가능한 서비스가 있음.

(참고만)

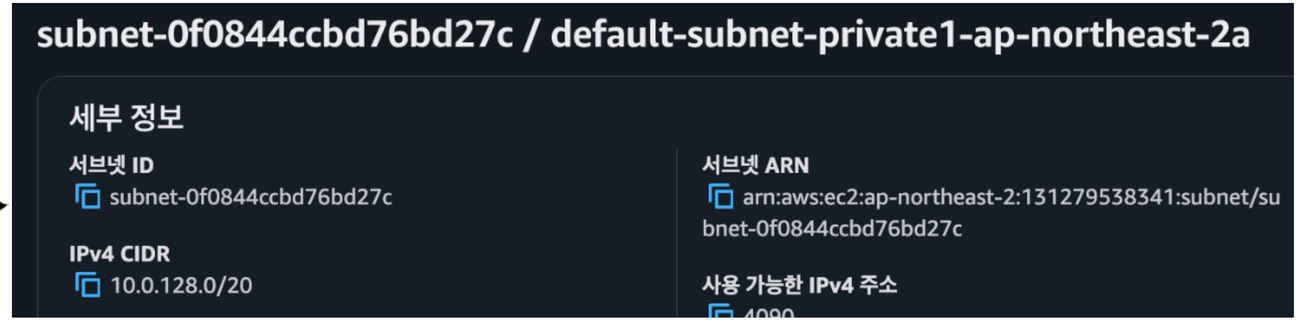
(대충 AWS 리소스 관리하는 서비스)

3.구현 과정 VPC


리소스 맵 정보
모든 세부 정보 표시
VPC
AWS 가상 네트워크
default-vpc
10.0.0.0/16
IPv6 없음
서브넷 (4)
이 VPC 내의 서브넷
ap-northeast-2a
default-subnet-public1-ap-northeast-2a
10.0.0.0/20
IPv6 없음
default-subnet-private1-ap-northeast-2a
10.0.128.0/20
IPv6 없음
ap-northeast-2b
default-subnet-public2-ap-northeast-2b
10.0.16.0/20
IPv6 없음
default-subnet-private2-ap-northeast-2b
10.0.144.0/20
IPv6 없음
라우팅 테이블 (4)
네트워크 트래픽을 리소스로 라우팅
rtb-0d78f99896ef59039
서브넷 연결 없음
로컬 포함 라우팅 1개
default-rtb-private1-ap-northeast-2a
서브넷 1개 연결
로컬 포함 라우팅 2개
default-rtb-private2-ap-northeast-2b
서브넷 1개 연결
로컬 포함 라우팅 2개
default-rtb-public
서브넷 2개 연결
로컬 포함 라우팅 2개
네트워크 연결 (2)
다른 네트워크에 연결
default-igw
2개의 퍼블릭 서브넷으로 인터넷 라우팅
인터넷으로 0개의 프라이빗 서브넷 라우팅
default-vpce-s3
S3에 대한 게이트웨이 엔드포인트

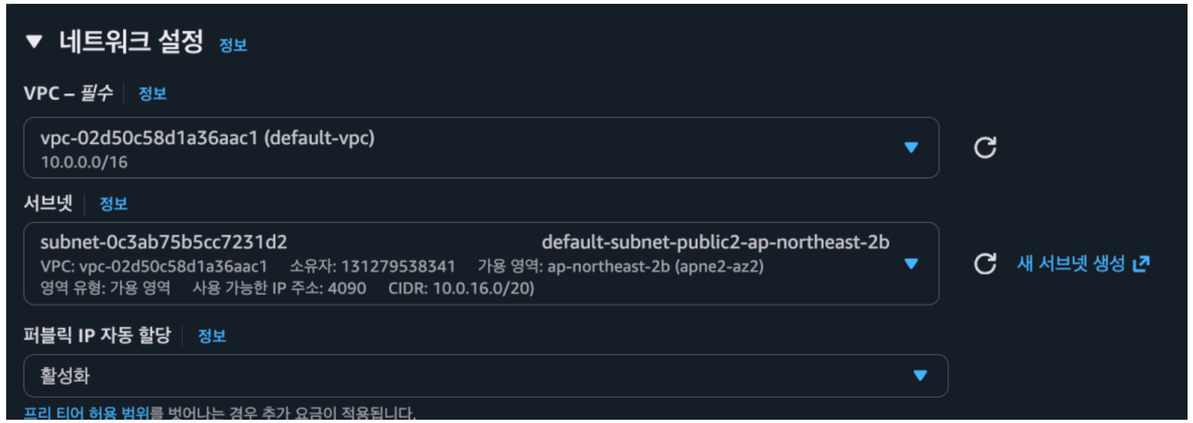
3.구현 과정 Private EC2

서브넷을 프라이빗 서브넷으로 선택하고 IP 자동 활성화를 비활성 시킴

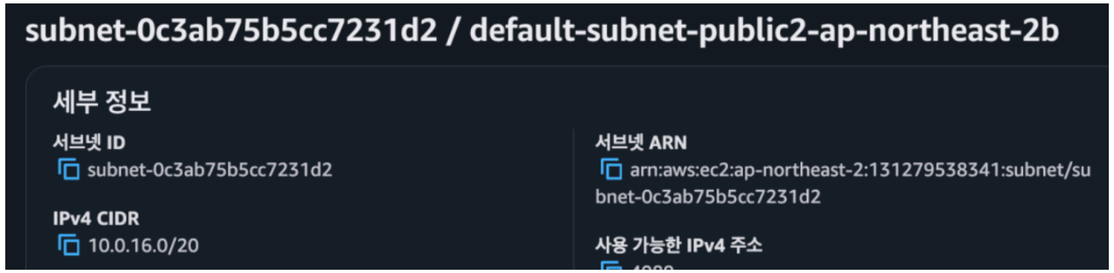


Private 2a 서브넷의 CIDR 범위 내에서 Private IP 할당됨

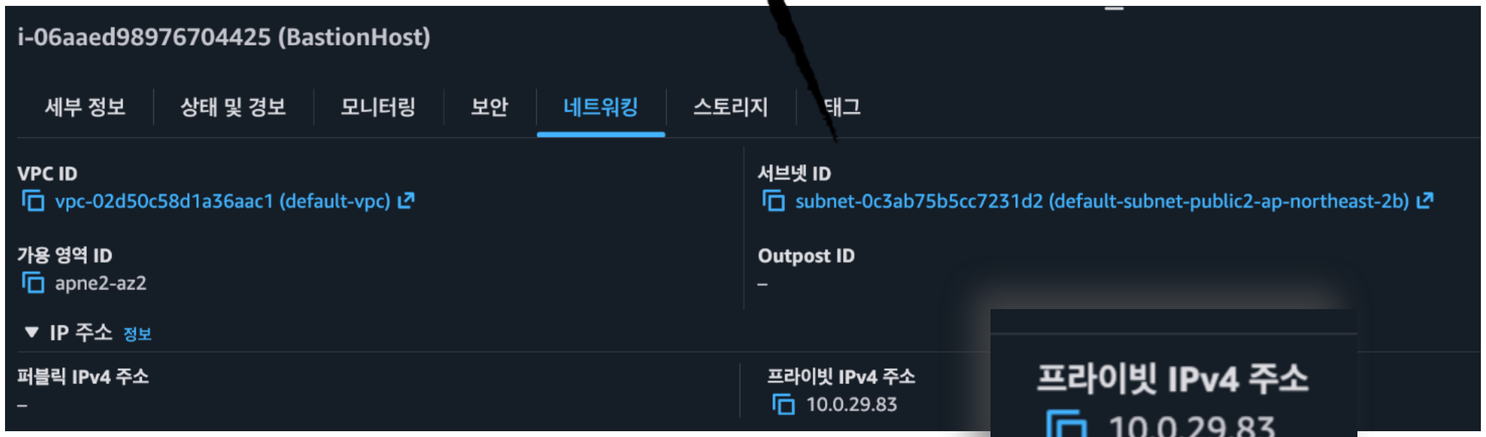
3.구현 과정 Bastion Host



2) 마찬가지로 지정한 서브넷(Public 2b)의 CIDR(IP 범위)을 따라서 IP 할당됨



1) 서브넷은 Public으로 설정하고 IP 자동 할당을 활성화 시킴

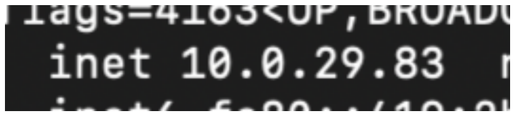


(인스턴스를 꺼둔 상태라 Public IP가 안보이는 것 뿐임)

3.구현 과정 Public EC2 = Bastion Host 접속

```
[gyeongdaeyeong@gyeongdaeyeong-ui-MacBookAir ~ % ssh -i "/Users/gyeongdaeyeong/Desktop/key/temporary-study-key.pem" ubun]
tu@43.201.44.133
The authenticity of host '43.201.44.133 (43.201.44.133)' can't be established.
ED25519 key fingerprint is SHA256:EUp8+eHI0KpA3IQWiHobm8EYeD5cd3Kqtf6LLKCwxzA.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:54: ec2-43-201-44-133.ap-northeast-2.compute.amazonaws.com
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '43.201.44.133' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Jan  6 14:31:39 UTC 2026

  System load:  0.01              Temperature:           -273.1 C
  Usage of /:   25.8% of 6.71GB   Processes:             116
  Memory usage: 24%               Users logged in:       0
  Swap usage:   0%                IPv4 address for ens5: 10.0.29.83

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-29-83:~$
```

```
ubuntu@ip-10-0-29-83:~$ ifconfig
ens5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.0.29.83  netmask 255.255.240.0  broadcast 10.0.31.255
        inet6 fe80::419:2bff:fef6:cc2f  prefixlen 64  scopeid 0x20<link>
        ether 06:19:2b:f6:cc:2f  txqueuelen 1000  (Ethernet)
        RX packets 7101  bytes 732181 (732.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3734  bytes 418578 (418.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 86  bytes 9058 (9.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86  bytes 9058 (9.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



(Bastion Host Private IP)

이제 이 Bastion Host에서
Private EC2 접속 가능

3.구현 과정 Private EC2 접속

Private 서브넷의 Private EC2에 접속하기 위해 scp 명령어를 통해 Bastion Host에 키페어를 보냄

```
gyeongdaeyeong@gyeongdaeyeong-ui-MacBookAir ~ % scp -i /Users/gyeongdaeyeong/Desktop/key/temporary-study-key.pem \
/Users/gyeongdaeyeong/Desktop/key/temporary-study-key.pem \
ubuntu@43.201.44.133:~

temporary-study-key.pem                                       100% 1674   165.5KB/s   00:00
```

```
ubuntu@ip-10-0-29-83:~$ ll
total 36
drwxr-x--- 4 ubuntu ubuntu 4096 Jan  6 15:13 ./
drwxr-xr-x 3 root   root   4096 Jan  6 14:27 ../
-rw------- 1 ubuntu ubuntu  590 Jan  6 14:35 .bash_history
-rw-r--r-- 1 ubuntu ubuntu  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Mar 31  2024 .bashrc
drwx------ 2 ubuntu ubuntu 4096 Jan  6 14:31 .cache/
-rw-r--r-- 1 ubuntu ubuntu  807 Mar 31  2024 .profile
drwx------ 2 ubuntu ubuntu 4096 Jan  6 14:59 .ssh/
-rw-r--r-- 1 ubuntu ubuntu    0 Jan  6 14:57 .sudo_as_admin_successful
-r-------- 1 ubuntu ubuntu 1674 Jan  6 15:13 temporary-study-key.pem
```

※ scp = 원격 서버 간 파일 전송 시 사용되는 명령어

3.구현 과정 Private EC2 접속 + 결론

Private EC에 접속된 것을 확인 할 수 있음

```
ubuntu@ip-10-0-29-83:~$ ssh -i temporary-study-key.pem ubuntu@10.0.130.57
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

 * Documentation:  ht
 * Management:     ht
 * Support:        https://ubuntu.com/pro

 System information as of Tue Jan  6 15:15:43 UTC 2026

  System load:  0.0               Temperature:           -273.1 C
  Usage of /:   25.8% of 6.71GB   Processes:             110
  Memory usage: 23%               Users logged in:       0
  Swap usage:   0%                IPv4 address for ens5: 10.0.130.57

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-130-57:~$
```

```
ubuntu@ip-10-0-29-83:~$ ssh -i temporary-study-key.pem ubuntu@10.0.130.57
```

Private EC2의 Private IP를 바탕으로 SSH에 접속할 수 있음

(만약 Bastion Host가 없었다면 Private IP로는 외부에서 절대 접속 불가능)

VPC 외부에서(예: 인터넷) 접속을 위해서라면 무조건 Public IP가 필요했음

(VPC 피어링, Transit Gateway 등등 제외)

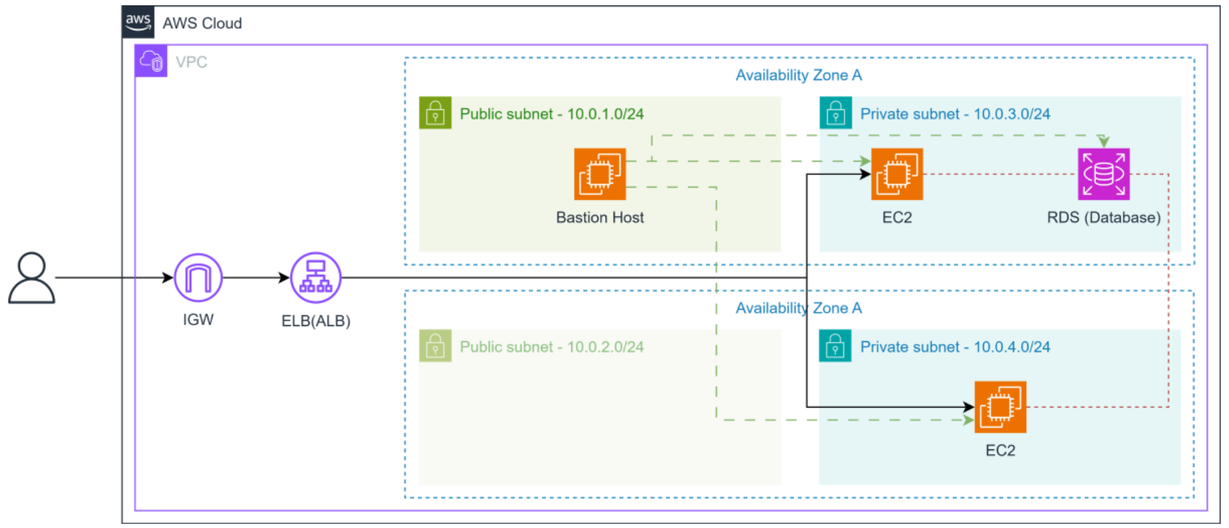
하지만 Bastion Host(Public IP)를 거쳐 Private IP로 Private EC2에 접속했다는 것이 핵심

4.느낌점

Bastion Host는 보안을 위해 Private 서브넷으로 구성된 아키텍처에서 운영 시 필요에 따라 접근하기 위한 수단임을 알게 되었고

작은 설정 하나가 내부 서버 안전성과 운영 편의성에 큰 영향을 준다는 점,

그리고 아키텍처 내부(Private 서브넷)에 접근할 수 있기 때문에 사용 시 보안적인 부분을 고려해야 한다는 점도 알게 되었음.



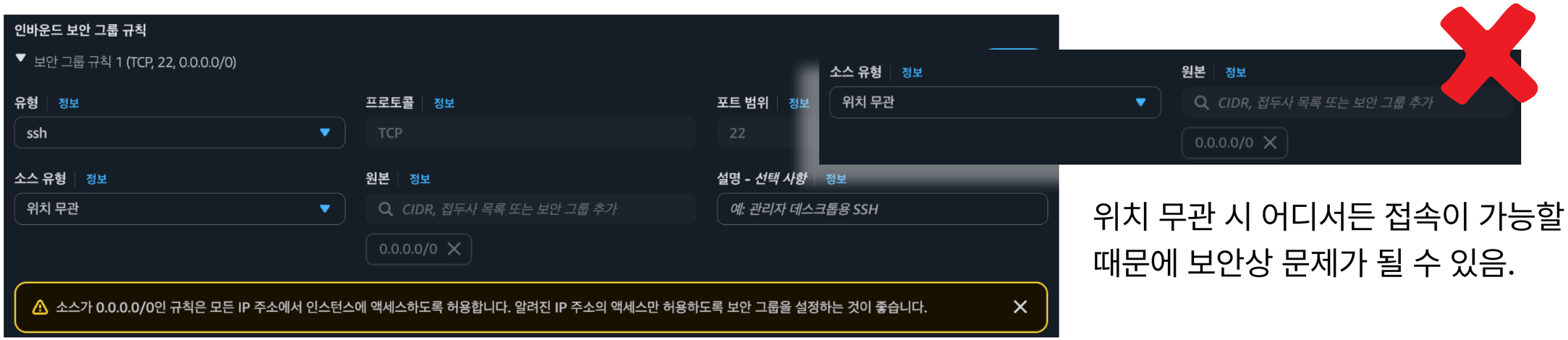
4.느낌점

실제 환경에서 Bastion Host를 효율적으로 운영하고 장애 상황에도 대비할 수있는 구조를 설계해보고 싶고

IAM 등의 접근 권한 관리와 모니터링을 자동화하여 보안과 운영 효율성을 동시에 높이는 것도 시도 해보고 싶음.

5. (추가적으로 조사한 부분) 보안 강화 방법

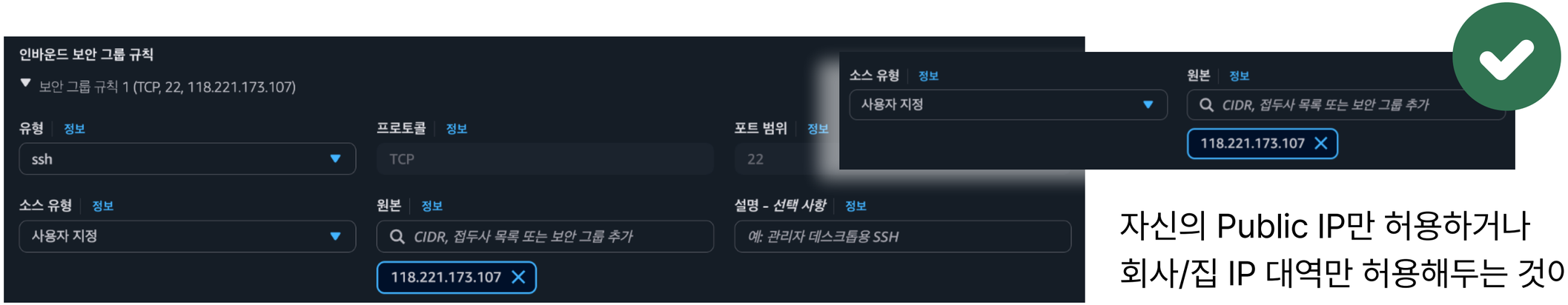
보안 그룹에서 SSH 인바운드 규칙 설정 시, 모든 IP 대역을 허용하지 않고 담당자나 회사 컴퓨터, 서버의 IP 대역(CIDR)만 허용하거나 특정 IP만 허용하도록 하는 것이 좋음.



위치 무관 시 어디서든 접속이 가능할 수 있기 때문에 보안상 문제가 될 수 있음.

5. (추가적으로 조사한 부분) 보안 강화 방법

보안 그룹에서 SSH 인바운드 규칙 설정 시, 모든 IP 대역을 허용하지 않고 담당자나 회사 컴퓨터, 서버의 IP 대역(CIDR)만 허용하거나 특정 IP만 허용하도록 하는 것이 좋음.



자신의 Public IP만 허용하거나
회사/집 IP 대역만 허용해두는 것이 좋음

(특히 SSH)

감사합니다.