AWS 운영 기초

유정현

목차

1. VPC, Subnet

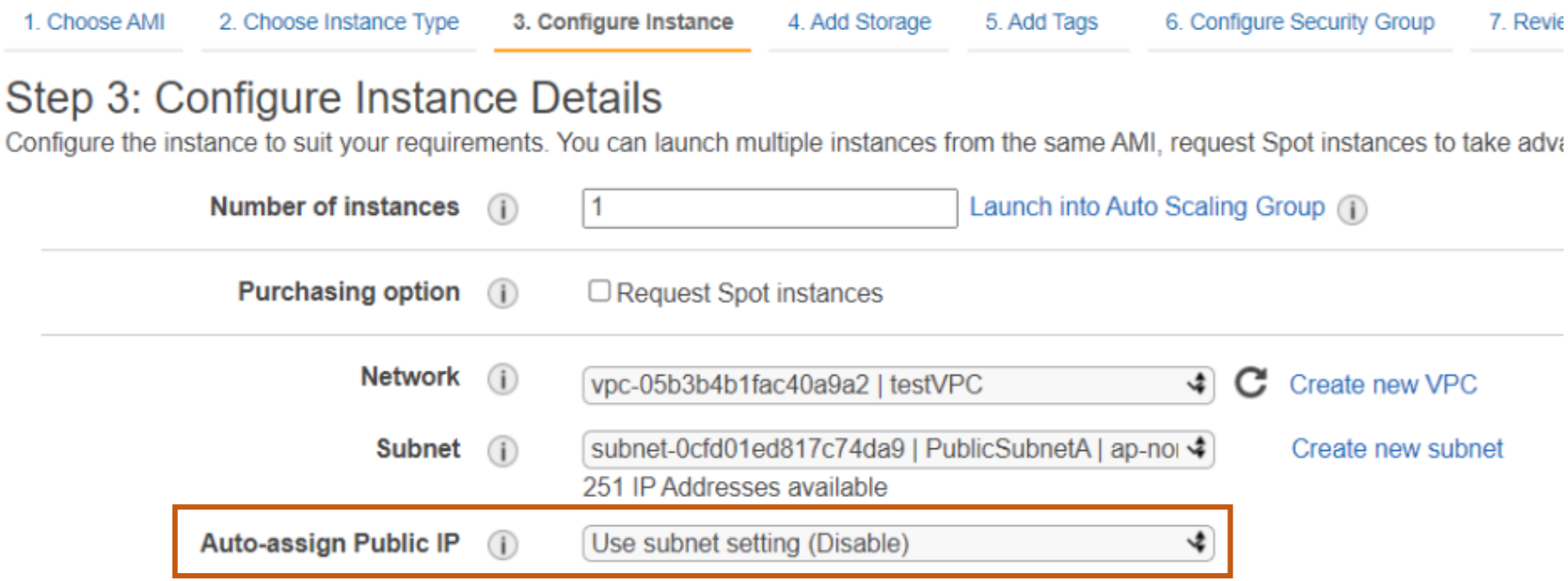
10.0.0.0/16 IPv4 CIDR 블록을 가지는 VPC를 생성
가용영역 A와 B에 각각 VPC의 IPv4 CIDR 블록에 포함되는 Private, Public Subnet을 생성

Name	VPC ID	State	IPv4 CIDR
testVPC	vpc-05b3b4b1fac40a9a2	Available	10.0.0.0/16

Name	Subnet ID	State	VPC	IPv4 CIDR
PrivateSubnetA	subnet-098037c1b09d22408	Available	vpc-05b3b4b1fac40a9a2 | test...	10.0.16.0/20
PublicSubnetA	subnet-0cfd01ed817c74da9	Available	vpc-05b3b4b1fac40a9a2 | test...	10.0.0.0/24
PrivateSubnetB	subnet-069e7afe931689ccc	Available	vpc-05b3b4b1fac40a9a2 | test...	10.0.32.0/20
PublicSubnetB	subnet-0a8d53401b07bd4db	Available	vpc-05b3b4b1fac40a9a2 | test...	10.0.1.0/24

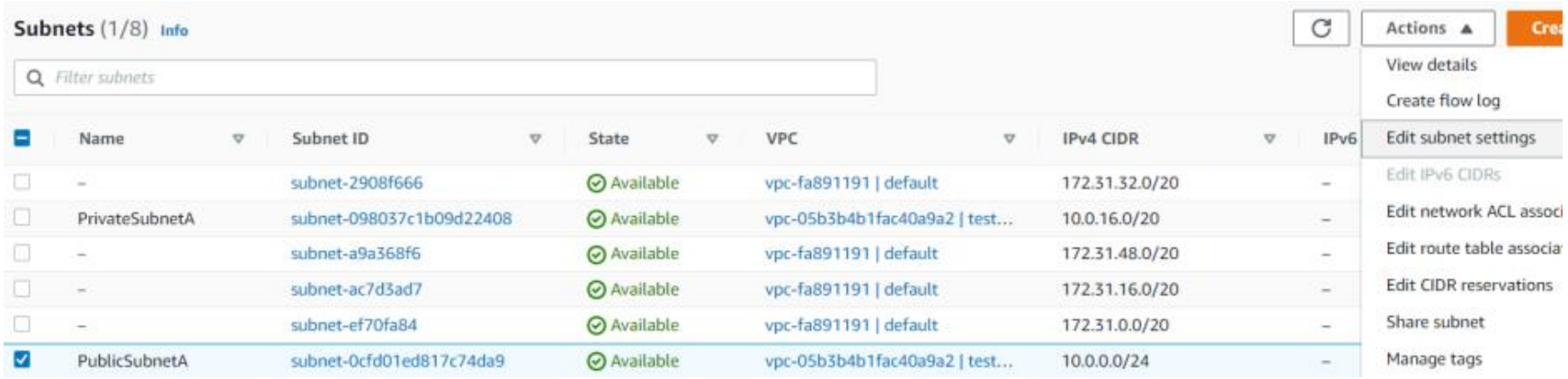
2. Public IP 자동할당

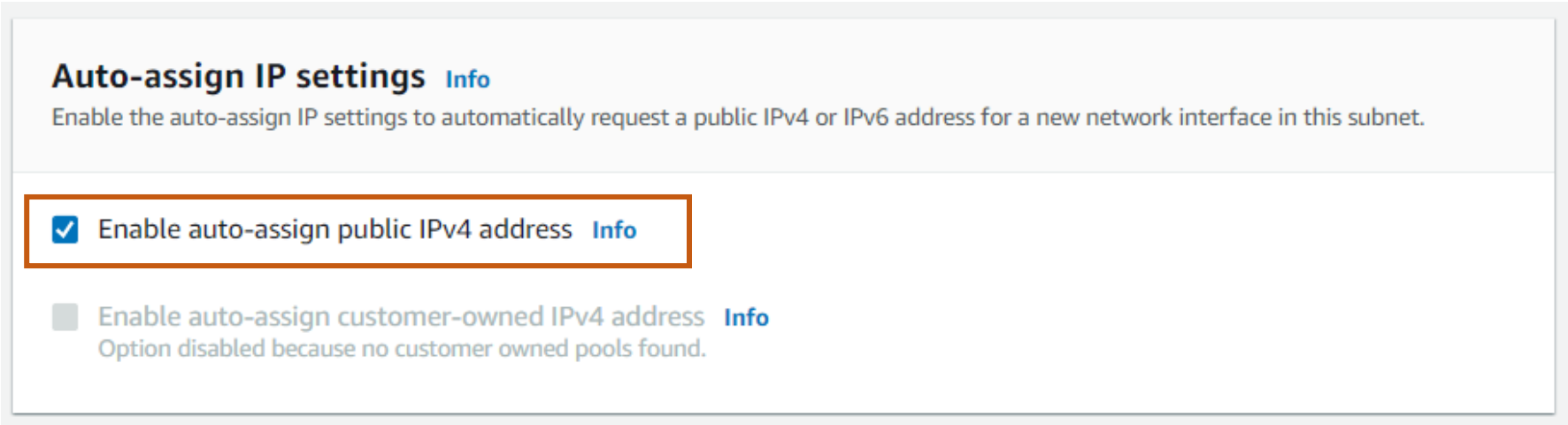
현재는 instance 생성 시 Public IP를 할당하지 않는다



2. Public IP 자동할당

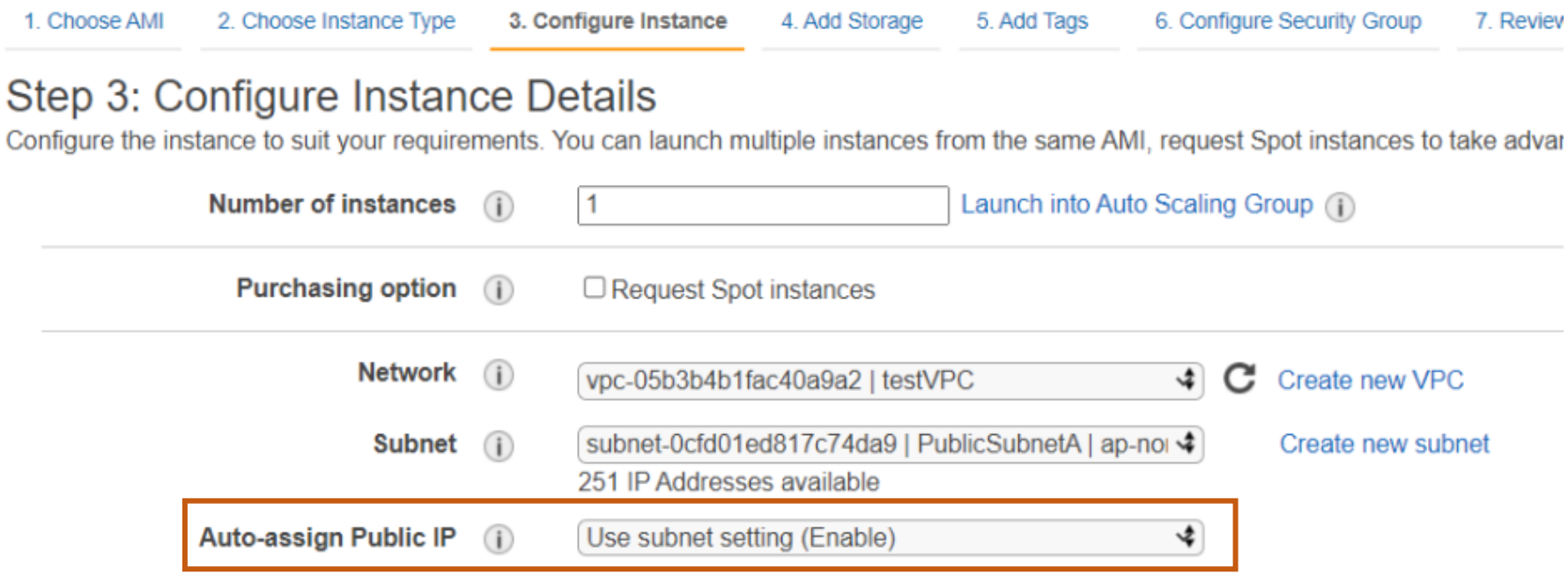
외부 연결이 필요한 Public Subnet의 설정을 수정해 IPv4 자동할당을 활성화





2. Public IP 자동할당

instance 생성 시 Public IP를 할당하는 것을 확인 가능



3. Internet Gateway

Internet Gateway를 생성 후 VPC에 연결

Name	Internet gateway ID	State
testIGW	igw-0eefad139f037d885	Detached

VPC > Internet gateways > igw-0eefad139f037d885

igw-0eefad139f037d885 / testIGW

Actions ▲

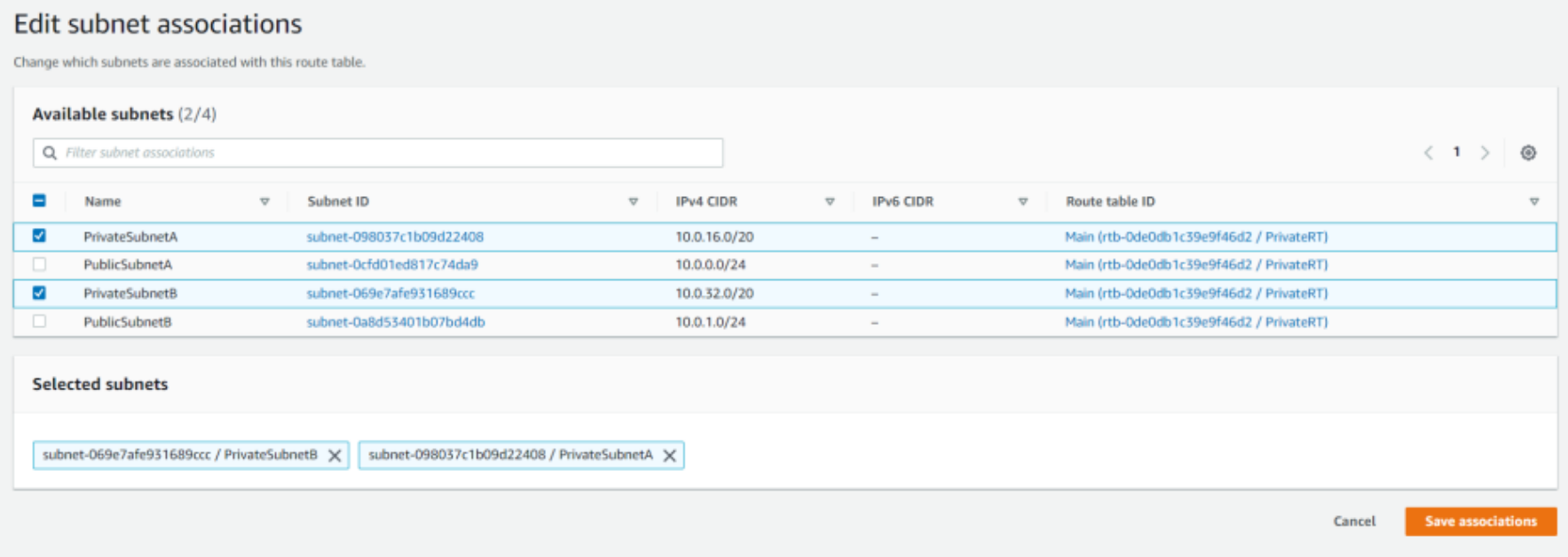
Attach to VPC

Name	Internet gateway ID	State	VPC ID
testIGW	igw-0eefad139f037d885	Attached	vpc-00a58e0c6b61b107b | testVPC

4. Route Table

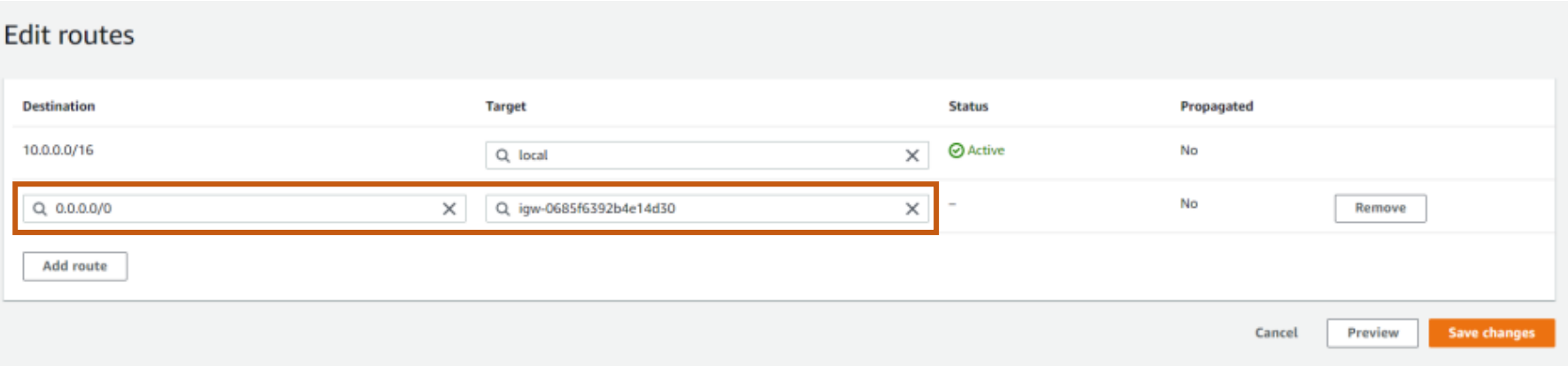
VPC에 이미 존재하는 Route Table은 Private으로 변경, Public Route Table은 생성
Private에는 Private Subnet, Public에는 Public Subnet을 명시적으로 연결

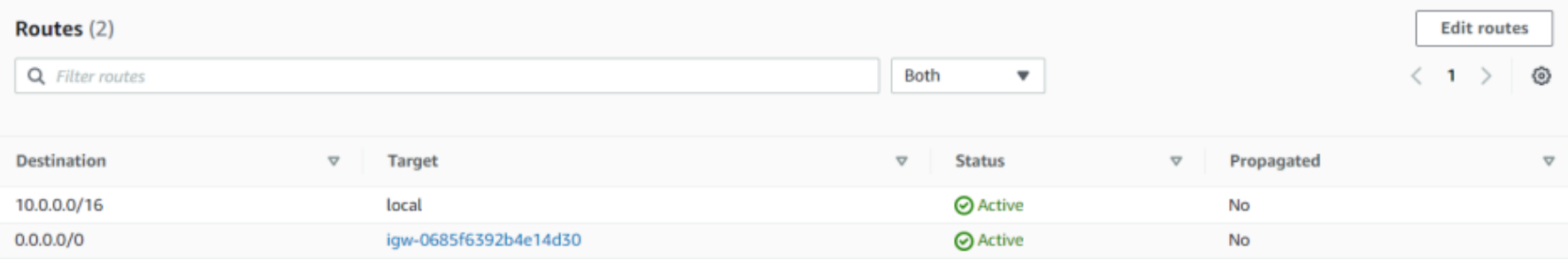
Name	Route table ID
PublicRT	rtb-0a34491e57835b985
PrivateRT	rtb-0de0db1c39e9f46d2



4. Route Table

외부 연결이 필요한 Public Route Table에 Internet Gateway를 연결





5. Public Instance

외부 연결이 가능하도록 Public Subnet A에 Bastion Instance를 생성
AMI : Linux / Instance Type : t2.micro / Security Group : SSH, HTTP 허용

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Bastion	i-0935a9c82b3bf3ac7	Running	t2.micro	2/2 checks passed	No alarms	ap-northeast-2a

외부 연결이 가능한 것 확인

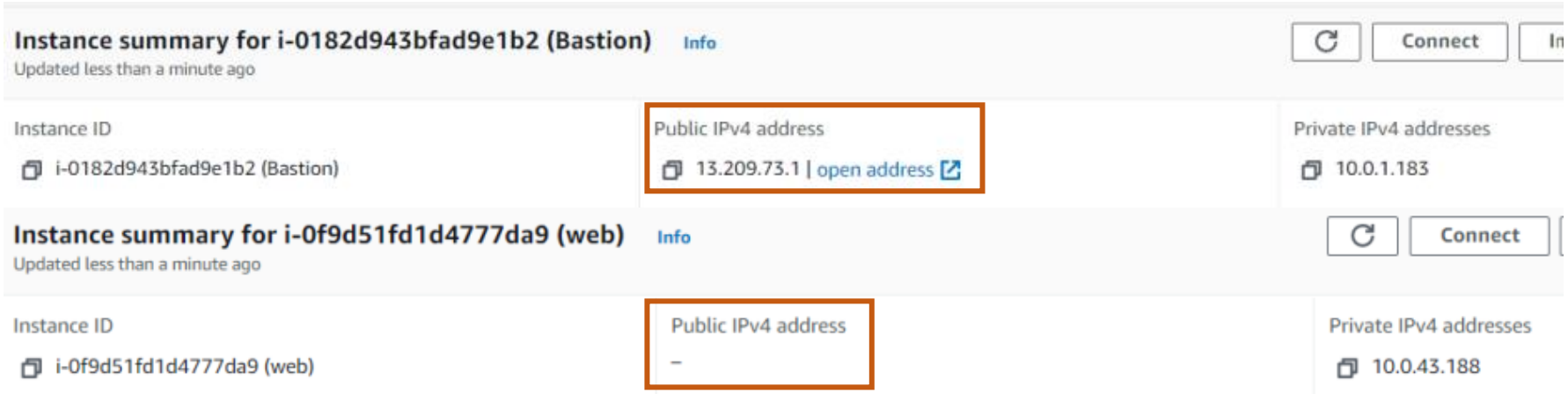
```
       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-68 ~]$ ping google.com
PING google.com (172.217.175.46) 56(84) bytes of data.
64 bytes from nrt20s19-in-f14.1e100.net (172.217.175.46): icmp_seq=1 ttl=105 time=31.5 ms
64 bytes from nrt20s19-in-f14.1e100.net (172.217.175.46): icmp_seq=2 ttl=105 time=31.6 ms
64 bytes from nrt20s19-in-f14.1e100.net (172.217.175.46): icmp_seq=3 ttl=105 time=31.6 ms
```

6. Private Instance

외부 연결이 불가능하도록 Private Subnet A에 Web Instance를 생성
AMI : Linux / Instance Type : t2.micro / Security Group : SSH, HTTP 허용

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
web	i-0d64d4fd331449cb5	Running	t2.micro	2/2 checks passed	No alarms	ap-northeast-2a

Bastion에는 IPv4 할당, Web에는 IPv4 할당되지 않은 것 확인 가능



6. Private Instance

Bastion Instance를 통해서 내부 IP로 접속이 가능

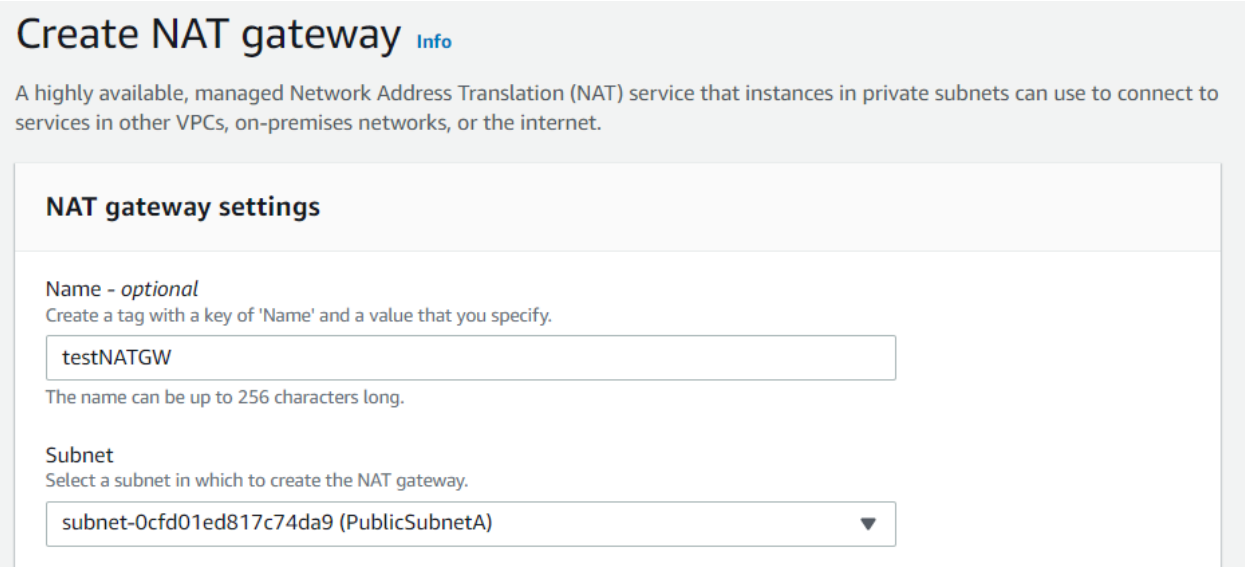
```
[ec2-user@ip-10-0-1-183 ~]$ sudo ssh -i aws.pem ec2-user@10.0.43.188

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-43-188 ~]$
```

그러나 외부 인터넷과는 연결이 불가능

```
[ec2-user@ip-10-0-43-188 ~]$ ping google.com
PING google.com (142.251.42.142) 56(84) bytes of data.
^C
--- google.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1015ms
```

7. NAT Gateway

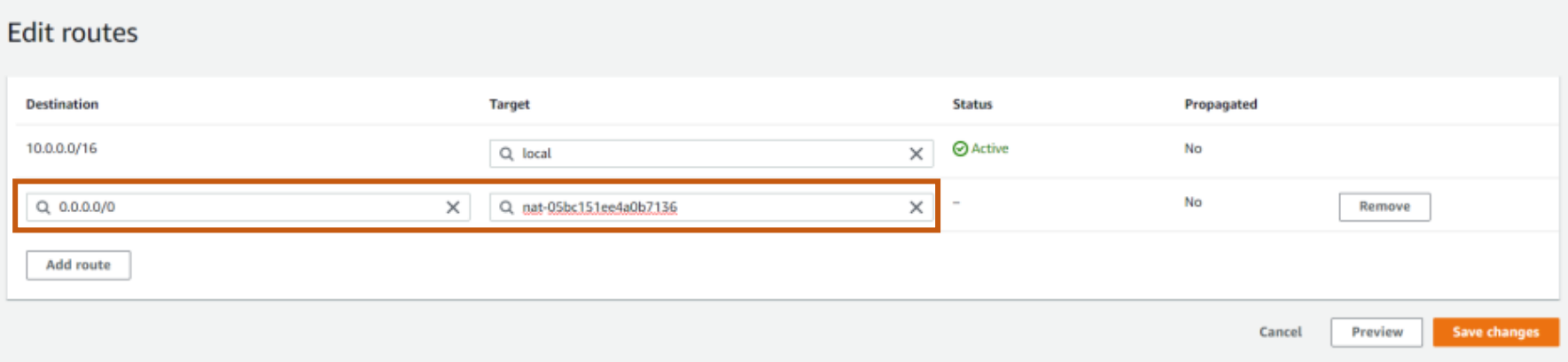
Web Instance에서도 외부 인터넷 연결이 가능하도록 Public Subnet에 NAT Gateway를 생성



할당 받은 Elastic IP를 연결

7. NAT Gateway

Private Route Table에 추가해줘야 Private Subnet에서도 외부 인터넷 연결이 가능



이제 Web Instance에서도 외부 인터넷 접속 가능

```
[ec2-user@ip-10-0-43-188 ~]$ ping google.com
PING google.com (142.251.42.142) 56(84) bytes of data.
64 bytes from nrt12s45-in-f14.1e100.net (142.251.42.142): icmp_seq=1 ttl=100 time=34.8 ms
64 bytes from nrt12s45-in-f14.1e100.net (142.251.42.142): icmp_seq=2 ttl=100 time=34.5 ms
64 bytes from nrt12s45-in-f14.1e100.net (142.251.42.142): icmp_seq=3 ttl=100 time=34.4 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 34.471/34.607/34.838/0.270 ms
```