Week 3

NAT-GW VPN SSL

7. NAT-GW

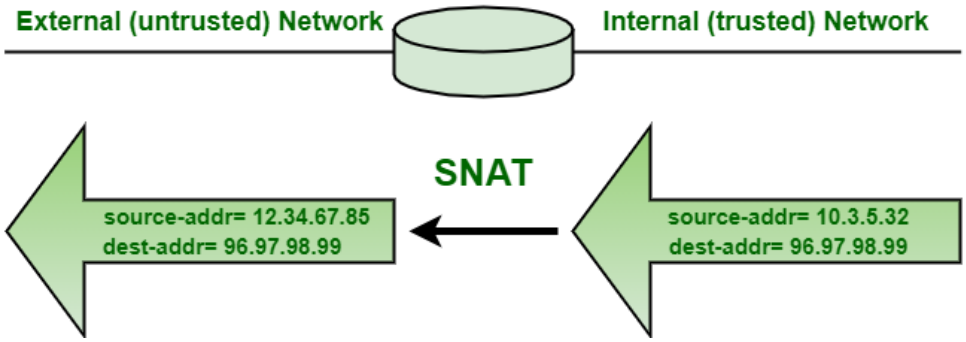
네트워크 주소 변환 서비스

▼ **Q1. SNAT/DNAT 기능은 언제 사용할까요?**

SNAT: 출발지 주소를 변경해주는 NAT

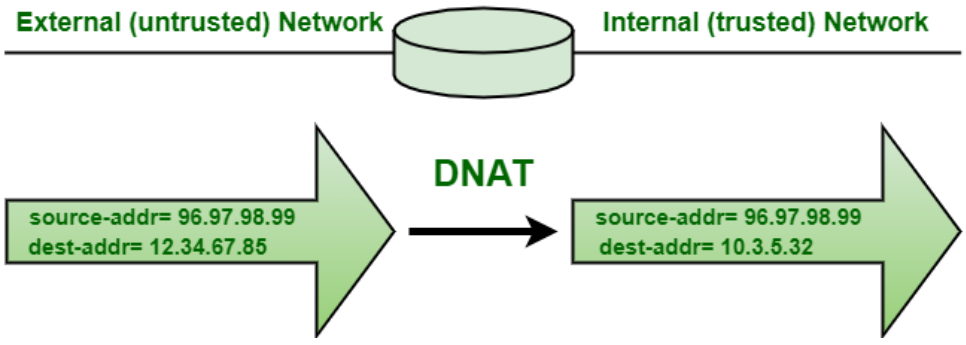
패킷의 Source 주소를 변경하는 것으로 Source NAT,혹은 IP 마스커레이드라고 한다.

• 인터넷으로 나가는 패킷의 Source IP를 G/W의 Public IP로 바꾼다.



DNAT: 도착지 주소를 변경해주는 NAT

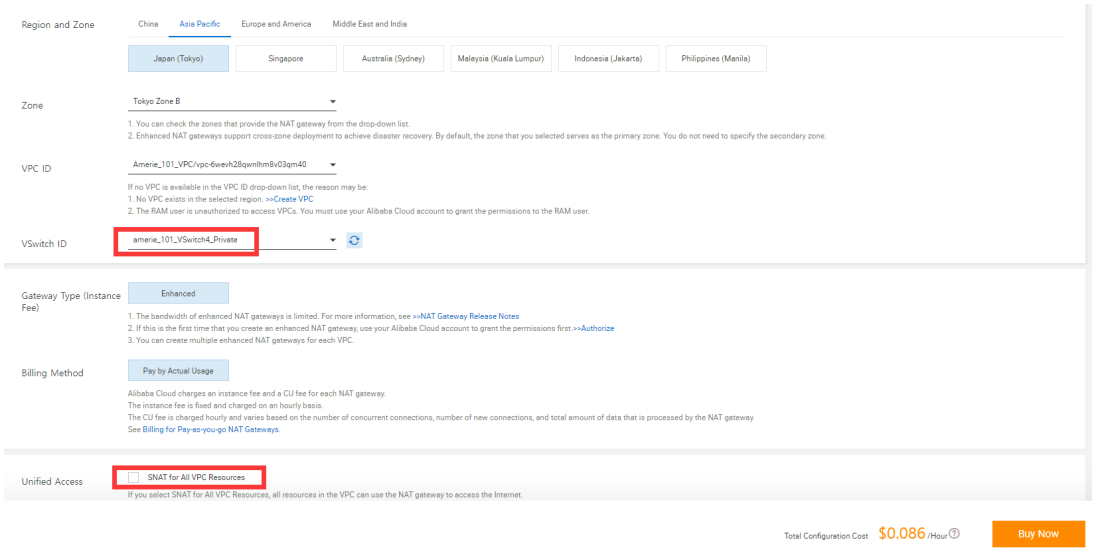
Destination IP 주소를 변경하여 내부에 접근할 수 있도록 패킷을 변경한다. 대표적인 것은 바로 Load Balancer이다.

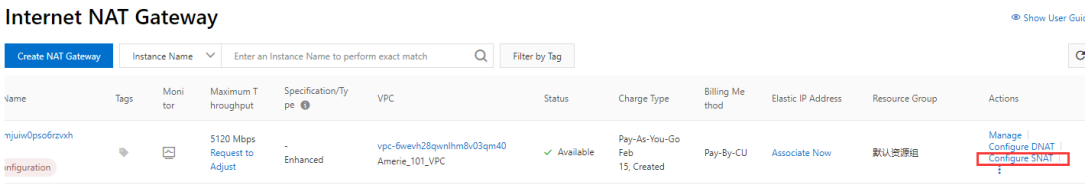


▼ Task Definitions

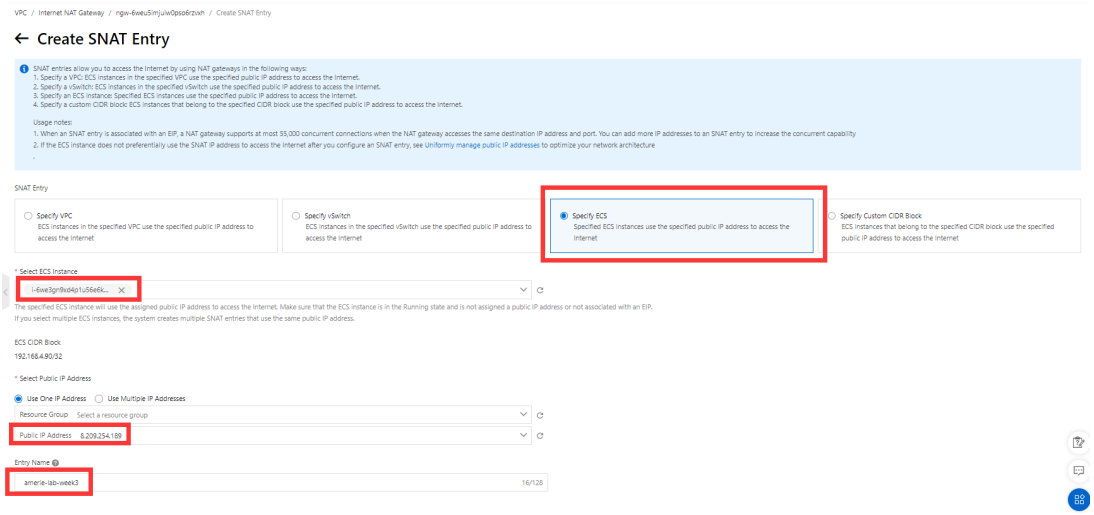
SNAT와 EIP를 동시에 사용 중인 ECS는 외부 통신을 요청하면 어느 서비스를 사용할까? 우선순위 라우팅을 컨트롤 할 수 있을까요?

- **Prerequisites**
  테스트할 ECS 존재 (WEB02 Instance)
  EIP 존재
- **Procedure**
  VPC 콘솔 접근 → NAT Gateway 생성 → EIP새로 생성 후 바인딩 → 외부 Ping 테스트 → traceroute test → EIP 언바인딩 후 traceroute test → SNAT entry 삭제 후 재설정 → Route Table에서 route entry 우선순위 컨트롤 가능 여부 체크
- **Step 1: SNAT 설정**
  1. VPC 콘솔 접근
  2. Internet NAT Gateway 선택 후 Create NAT Gateway 클릭





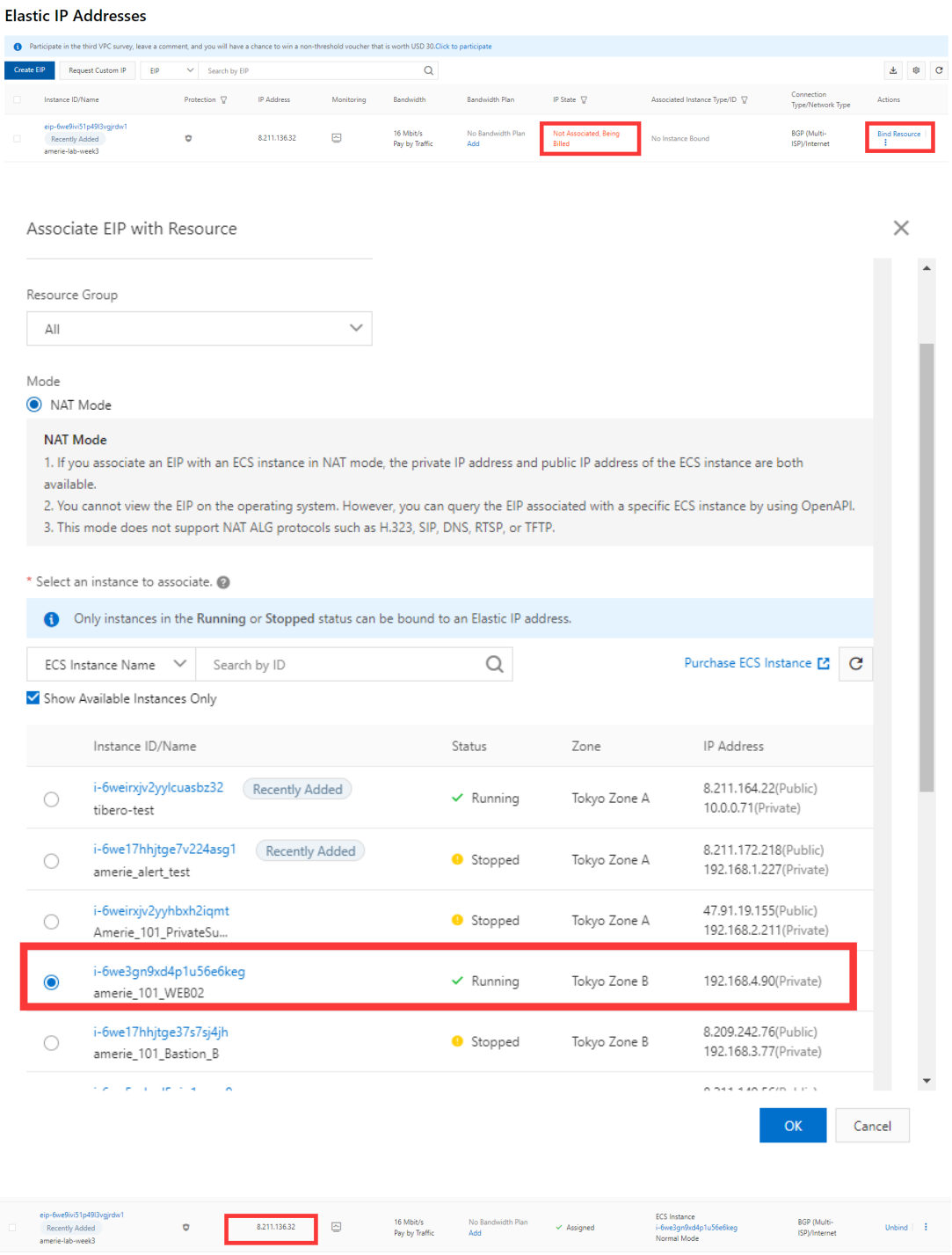
3. Configure SNAT 클릭 후 Create SNAT Entry
   ECS 테스트를 위해 특정 ECS로 설정하겠다. (WEB02 선택)
   Public IP쪽에서 EIP를 붙일 수 있다. (존재하지 않는 경우 새로 생성 가능)



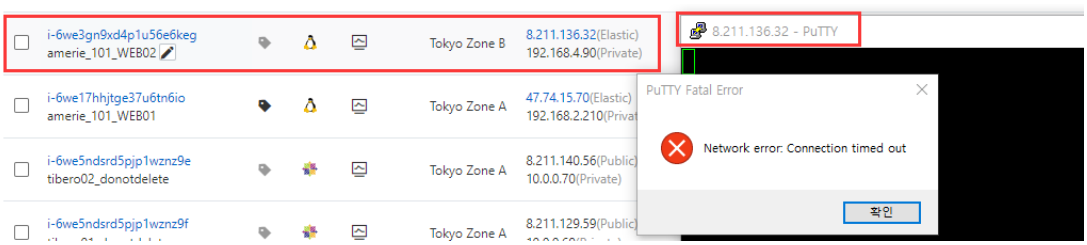
Bastion Host에서 ssh로 내부 WEB02 ECS에 접근해서 외부 통신 테스트 진행 - 성공

```
root@ameriebastion101:~# ssh 192.168.4.90
root@192.168.4.90's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-166-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Welcome to Alibaba Cloud Elastic Compute Service !

Last login: Tue Feb 15 14:39:20 2022 from 192.168.1.223
root@amerieweb02:~# ping 8.8.8.8 -c 3
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=5.53 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=5.73 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=5.40 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 5.402/5.554/5.730/0.134 ms
```

- **Step 2: EIP 새로 생성 후 ECS와 바인딩 (동일한 ECS에 바인딩)**
  1. VPC 콘솔 접근
  2. Elastic IP Address 클릭 후 Create EIP 클릭
  3. 생성 후 “Bind Resource” 클릭 후 동일한 ECS(WEB02) 선택



해당 EIP로 인스턴스에 접근 - 접근불가 (Bastion에서 접근가능, 외부 통신가능)
외부 통신 가능여부 체크 - 확인불가 (현재 SNAT와 EIP를 중복으로 바인딩 중)



- **Step 3: 경로 추적**

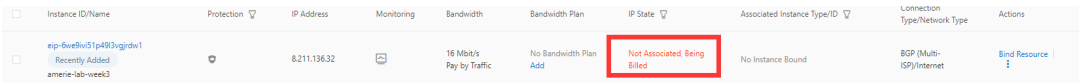
  1. Traceroute 설치 (ubuntu)

  설치 명령어: sudo apt-get install traceroute

  2. 해당 툴로 추적 (현재 SNAT와 EIP 중복 바인딩 상태)

```
root@amerieweb02:~# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  * * *
 2  10.106.201.25 (10.106.201.25)  3.282 ms *  3.367 ms
 3  10.106.203.6 (10.106.203.6)  2.896 ms 10.106.203.138 (10.106.203.138)  4.385 ms 10.106.207.6 (10.106.207.6)  2.745 ms
 4  47.246.117.18 (47.246.117.18)  2.925 ms 47.246.116.226 (47.246.116.226)  7.622 ms 47.246.116.230 (47.246.116.230)  7.318 ms
 5  218.100.6.173 (218.100.6.173)  2.221 ms 218.100.6.53 (218.100.6.53)  2.351 ms 218.100.6.173 (218.100.6.173)  2.567 ms
 6  108.170.242.161 (108.170.242.161)  2.699 ms  2.597 ms 108.170.242.193 (108.170.242.193)  3.553 ms
 7  142.251.226.141 (142.251.226.141)  2.208 ms 142.250.214.139 (142.250.214.139)  1.991 ms 108.170.237.93 (108.170.237.93)  3.285 ms
 8  dns.google (8.8.8.8)  2.909 ms  2.276 ms  2.281 ms
```

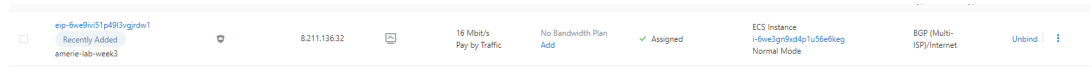
  3. EIP 언바인딩 후 다시 추적 - 경로가 달라짐




```
root@amerieweb02:~# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  * * *
 2  11.60.68.57 (11.60.68.57)  7.336 ms * *
 3  11.60.72.18 (11.60.72.18)  8.244 ms 11.60.68.198 (11.60.68.198)  7.945 ms 11.60.72.2 (11.60.72.2)  27.993 ms
 4  11.60.67.209 (11.60.67.209)  3.998 ms 11.60.67.233 (11.60.67.233)  4.257 ms 11.60.66.97 (11.60.66.97)  4.316 ms
 5  116.251.83.217 (116.251.83.217)  5.941 ms 116.251.83.78 (116.251.83.78)  5.119 ms 116.251.83.90 (116.251.83.90)  5.797 ms
 6  218.100.6.53 (218.100.6.53)  4.670 ms 218.100.6.173 (218.100.6.173)  4.492 ms 218.100.6.53 (218.100.6.53)  4.486 ms
 7  108.170.242.193 (108.170.242.193)  6.475 ms  6.381 ms  6.366 ms
 8  72.14.233.223 (72.14.233.223)  4.629 ms 142.250.61.143 (142.250.61.143)  5.141 ms 142.250.226.7 (142.250.226.7)  5.775 ms
 9  dns.google (8.8.8.8)  5.348 ms  5.063 ms  5.627 ms
```

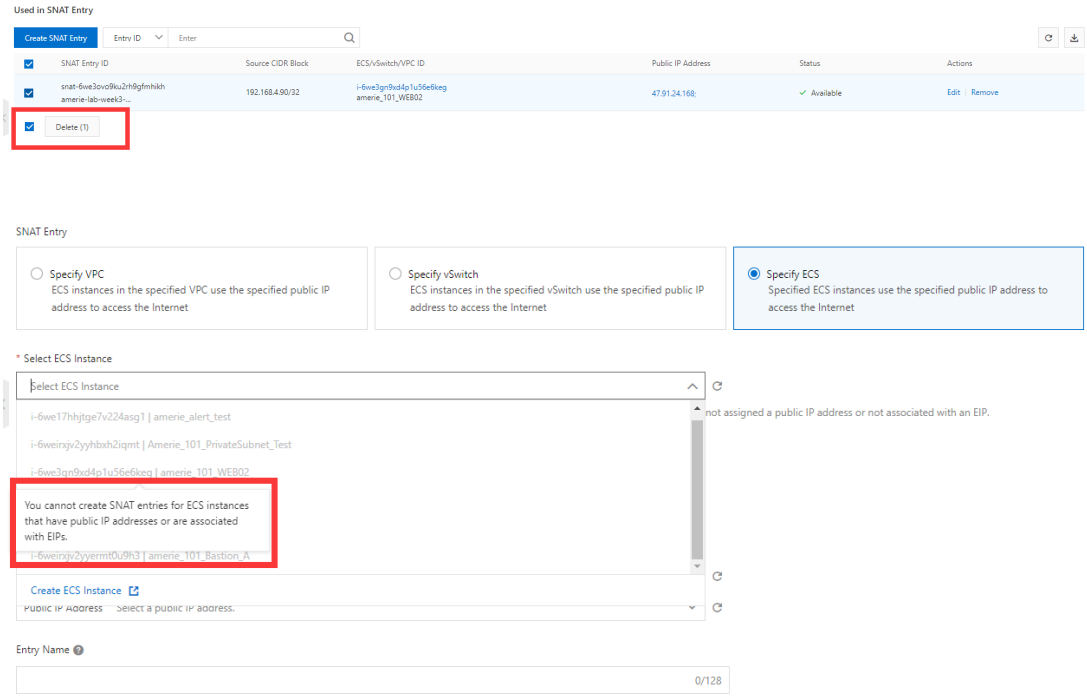
  4. 다시 EIP를 바인딩 후 추적 - 다시 10으로 시작한 IP - 다시 같은 경로가 나옴

  ※ 연속으로 추적을 할 경우 같은 IP대역 대의 서로 다른 IP로 나올 경우도 있다.




```
root@amerieweb02:~# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  * * *
 2  10.106.201.25 (10.106.201.25)  3.015 ms * *
 3  10.106.207.110 (10.106.207.110)  4.443 ms 10.106.203.2 (10.106.203.2)  4.395 ms 10.106.207.102 (10.106.207.102)  4.643 ms
 4  47.246.116.226 (47.246.116.226)  3.178 ms  3.439 ms  3.394 ms
 5  218.100.6.173 (218.100.6.173)  3.151 ms  3.181 ms 218.100.6.53 (218.100.6.53)  2.164 ms
 6  108.170.242.193 (108.170.242.193)  3.156 ms  3.098 ms 108.170.242.129 (108.170.242.129)  3.367 ms
 7  142.250.214.139 (142.250.214.139)  2.426 ms 142.250.226.61 (142.250.226.61)  3.472 ms 142.251.60.195 (142.251.60.195)  2.232 ms
 8  dns.google (8.8.8.8)  2.480 ms  1.937 ms  2.646 ms
```

  5. SNAT Entry 삭제 후 다시 설정 시도 - 현재 EIP가 바인딩 돼있어서 설정 안됨

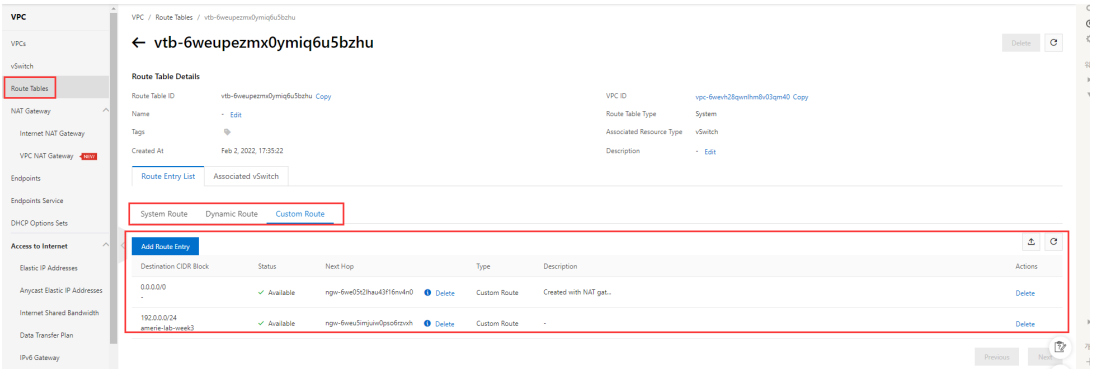


※ SNAT 와 EIP가 모두 동일한 ECS에 바인딩 돼있을 때 EIP로 인스턴스 접근 불가

※ EIP(Public IP)가 바인딩이 돼있으면 SNAT Entry 설정 불가

- **Step 4: Route Entry 우선순위 설정 가능 여부 - 불가능**
  라우팅 테이블에서 Route Entry 우선순위 컨트롤 가능 여부 - 불가능

  1. VPC 콘솔 접근
  2. Route Tables 선택 후 테스트 중인 Route Table(VPC)로 선택
  3. Route Entry List 탭 확인
  4. System Route, Dynamic Route에는 버튼이 없고 Custom Route에는 “Add Route Entry”만 있고 순위를 설정하는 기능 및 버튼이 없음



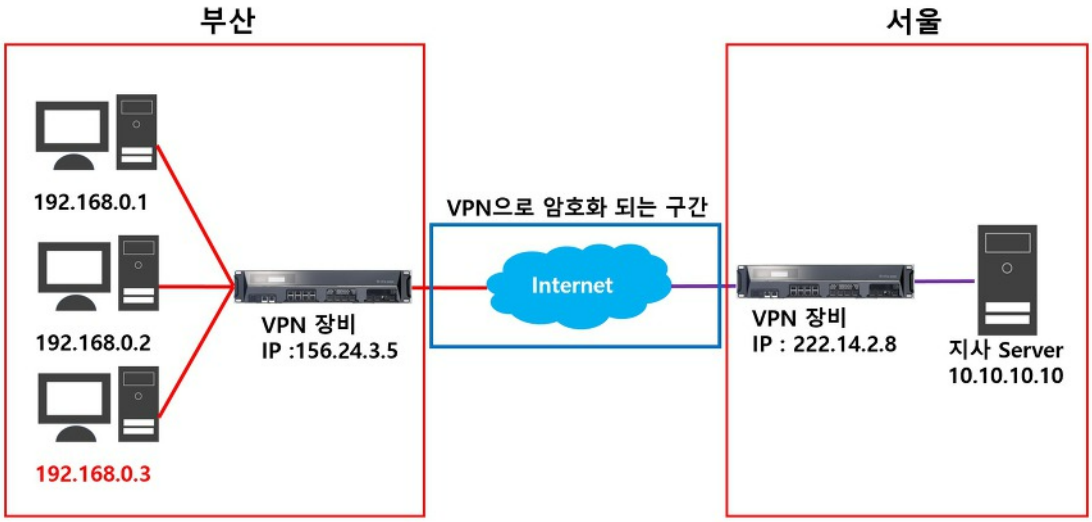
8. VPN

암호화 채널을 통해 안전하고 안정적인 연결을 구현하는 인터넷 기반 네트워크 연결 서비스

▼ **Q1. IPsec-VPN과 ssl-VPN의 차이?**

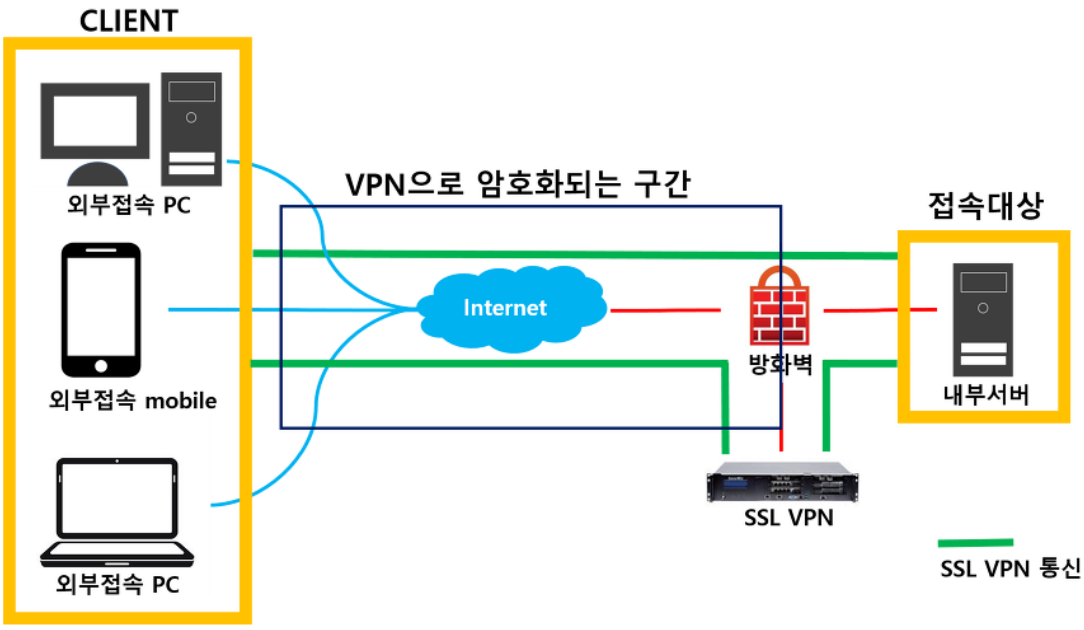
IPsec-VPN이란:

3계층 네트워크 단계에서 안전하게 정보를 전송하는 방법으로 간단하게 말하면, 장비가 2대가 필요하다. A와 B에 각각 VPN 장비를 설치해서 암호화 통신을 하는 방법이며 운영 방식에 따라 전송 모드와, 터널 모드가 있고, 암호화 여부에 따라 ESP, AH 프로토콜을 사용한다.



ssl-VPN이란:

sslVPN은 7계층 응용(Application) 계층에서 안전하게 정보를 전송하는 방법으로 간단하게 말하면, 장비 1대가 필요하다. 웹페이지 등을 통해 사용자의 인증이 완료되면 VPN을 사용할 수 있는 가상 IP가 할당되기 때문에, 장소나 단말의 종류와 관계없이 내부 네트워크와 접속할 수 있다.



차이점:

- IPsec-VPN은 장비 두 대가 필요하며 ssl-VPN은 한 대가 필요하다.
- IPsec-VPN은 3계층에서 전송하고 ssl-VPN은 7계층에서 전송한다.

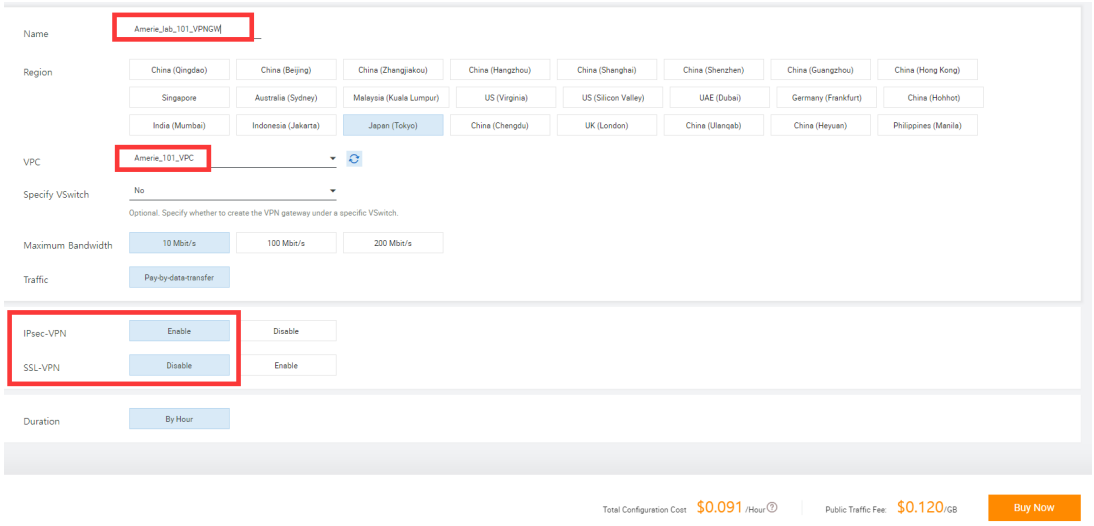
▼ Q2. IPsec-VPN에서 sa키란 무엇인가?

한곳에서 암호화된 데이터를 다른 곳에서 복호화하기 위해 서로 암호화 알고리즘을 정해서 사용해야하고, 암/복호화 키에 대해 알고 있어야한다. 이것을 SA라고 한다.

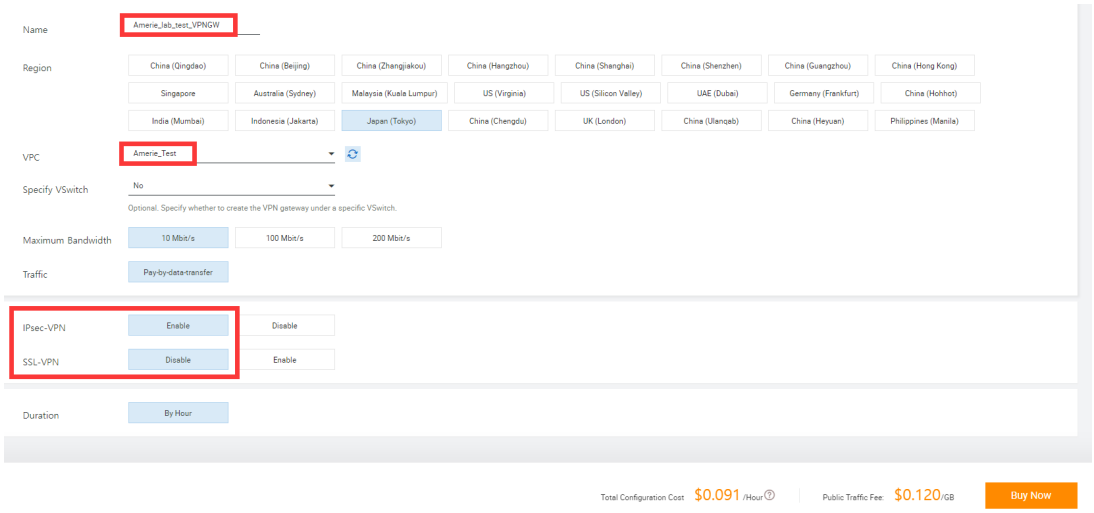
▼ Task Definitions

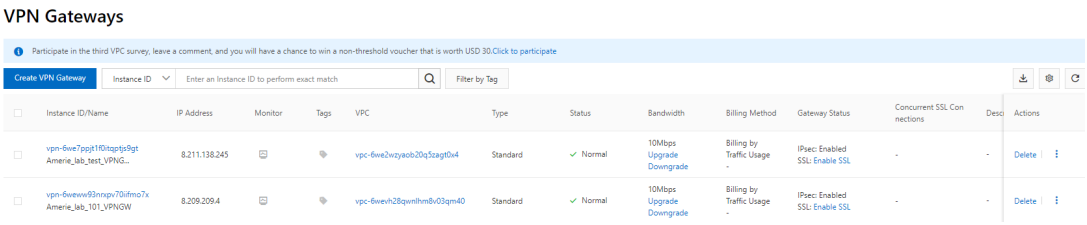
테스트 A(VPC)에서 VPN-GW를 구성하고 테스트 B(VPC)에서 VPN-GW를 구성하여 A<->B 에 ECS간에 VPN연결 확인하기, 즉 VPC간에 VPN으로 통신할 수 있게 설정

- **Prerequisites**
  VPC 2개 존재
  VPN-GW 2개 생성
  테스트할 각각의 VPC에 EC2 존재
- **Procedure**
  VPN-GW 구성 → Customer GW 구성 → IPsec Connections 구성 → VPC 간의 연결 테스트
- **Step 1: VPC 1 (name:101)에 VPN-GW 구성**
  1. VPN 콘솔에 접근
  2. Create VPN Gateway



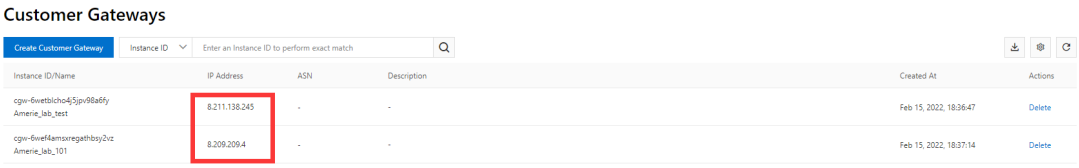
- **Step 2: VPC 2(name:test)에 VPN-GW 구성**
  1. VPN 콘솔에 접근
  2. Create VPN Gateway





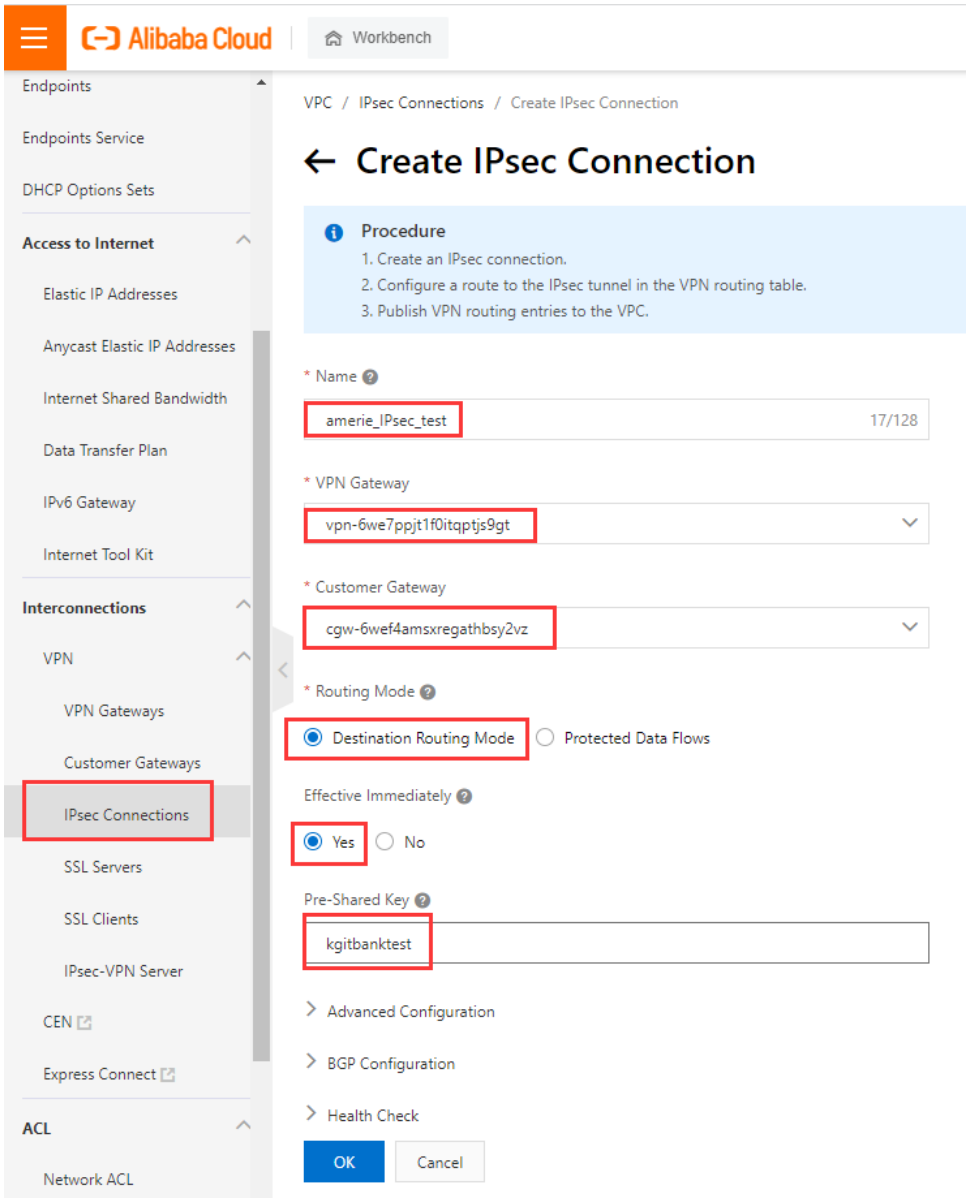
- **Step 3: Customer Gateway 2개 생성**
  1. VPN 콘솔 접근

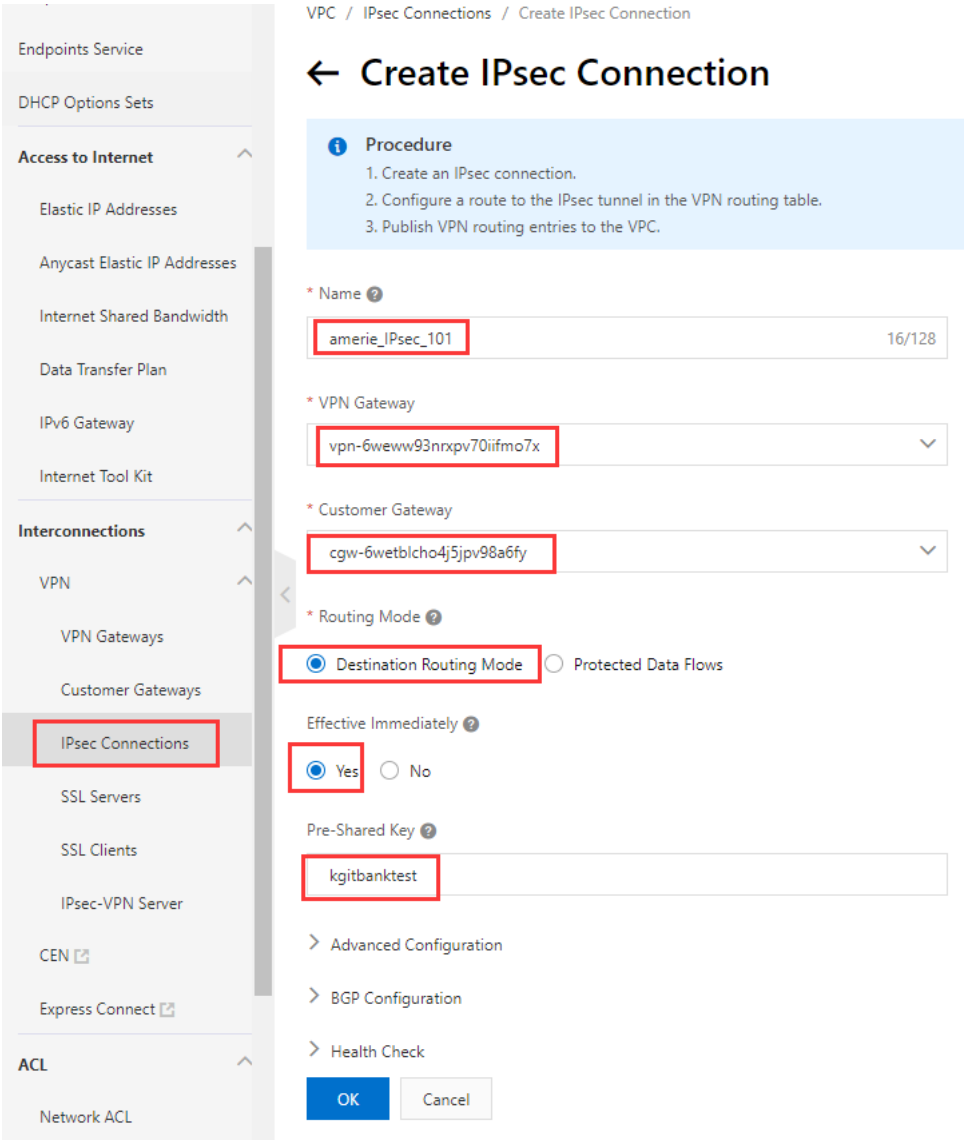
2. Create Customer Gateway 선택
3. 방금 생성한 2개의 VPN-GW의 IP로 설정 후 Customer Gateway 생성



- **Step 4: IPsec Connections 2개 생성**
  1. VPN 콘솔 접근
  2. IPsec Connections 선택 후 Create IPsec Connections 클릭
  3. 방금 생성한 Customer Gateway로 1개씩 설정
  - VPN Gateway는 VPC1, Customer Gateway는 VPC2로 설정
  ※ 연결하고자 하는 VPN Gateway하고 Customer Gateway는 정반대로 설정해야 한다.
  - Advanced Configuration, BGP Configuration, Health Check는 Default로 설정

  추가 설정: Destination Routing Mode 설정 시 “VPN Gateway”메뉴 “Policy Based-Routing”탭에서 “Add Route Entry”를 추가로 설정해야 VPN통신이 가능하다. 아래 4번 참조

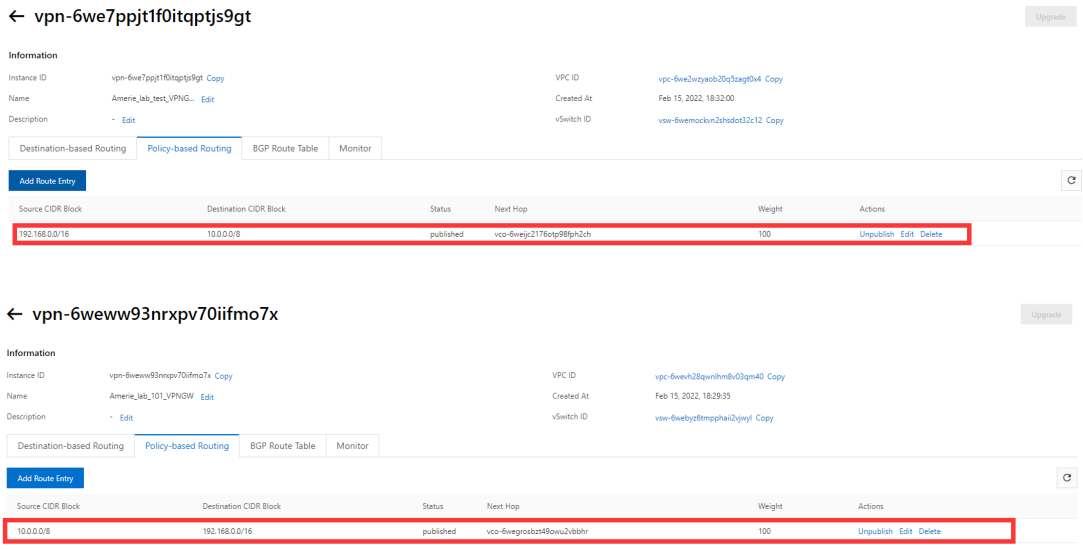

Alibaba Cloud
Workbench
Endpoints
Endpoints Service
DHCP Options Sets
Access to Internet
Elastic IP Addresses
Anycast Elastic IP Addresses
Internet Shared Bandwidth
Data Transfer Plan
IPv6 Gateway
Internet Tool Kit
Interconnections
VPN
VPN Gateways
Customer Gateways
IPsec Connections
SSL Servers
SSL Clients
IPsec-VPN Server
CEN
Express Connect
ACL
Network ACL
VPC / IPsec Connections / Create IPsec Connection
Create IPsec Connection
Procedure
1. Create an IPsec connection.
2. Configure a route to the IPsec tunnel in the VPN routing table.
3. Publish VPN routing entries to the VPC.
* Name
amerie_IPsec_test
17/128
* VPN Gateway
vpn-6we7ppjt1f0itqptjs9gt
* Customer Gateway
cgw-6wef4amsxregathbsy2vz
* Routing Mode
Destination Routing Mode
Protected Data Flows
Effective Immediately
Yes
No
Pre-Shared Key
kgitbanktest
Advanced Configuration
BGP Configuration
Health Check
OK
Cancel



4. VPN 콘솔 VPN Gateways에서 2개의 Gateway로 진입 후 “Policy-based Routing”탭 선택 후 Add Route Entry 클릭해서 아래와 같이 설정

- Destination CIDR Block: 접속할 VPC IP 대역대
- Source CIDR Block: 로컬 VPC IP 대역대
- Next Hop Type: IPsec Connection 선택
- Next Hop: Default로 1개가 나올 것이며 VPC1이면 VPC1로 선택
- Publish to VPC: 반드시 Yes로 선택
- Weight: Default 값 100으로 설정

이 작업은 2개의 Gatway에서 모두 해야 한다.



- **Step 5: VPC1, VPC2에 있는 ECS끼리 통신이 되는지 확인** - ????

1. ECS 콘솔 접근
2. 2개의 ECS로 원격접속 (Putty)
3. 현재 ECS IP 체크
4. 상대방 VPC에 있는 ECS로 Ping 테스트

```
root@ameriebastion101:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.223  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::216:3eff:fe00:4e12  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:00:4e:12  txqueuelen 1000  (Ethernet)
        RX packets 9880  bytes 8744325 (8.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5794  bytes 2290596 (2.2 MB)
        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 858  bytes 75267 (75.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 858  bytes 75267 (75.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@ameriebastion101:~# ping 10.0.1.171 -c 3
PING 10.0.1.171 (10.0.1.171) 56(84) bytes of data.
From 192.168.1.228 icmp_seq=1 Time to live exceeded
From 192.168.1.228 icmp_seq=2 Time to live exceeded
From 192.168.1.228 icmp_seq=3 Time to live exceeded

--- 10.0.1.171 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2044ms
```

문의중!!!

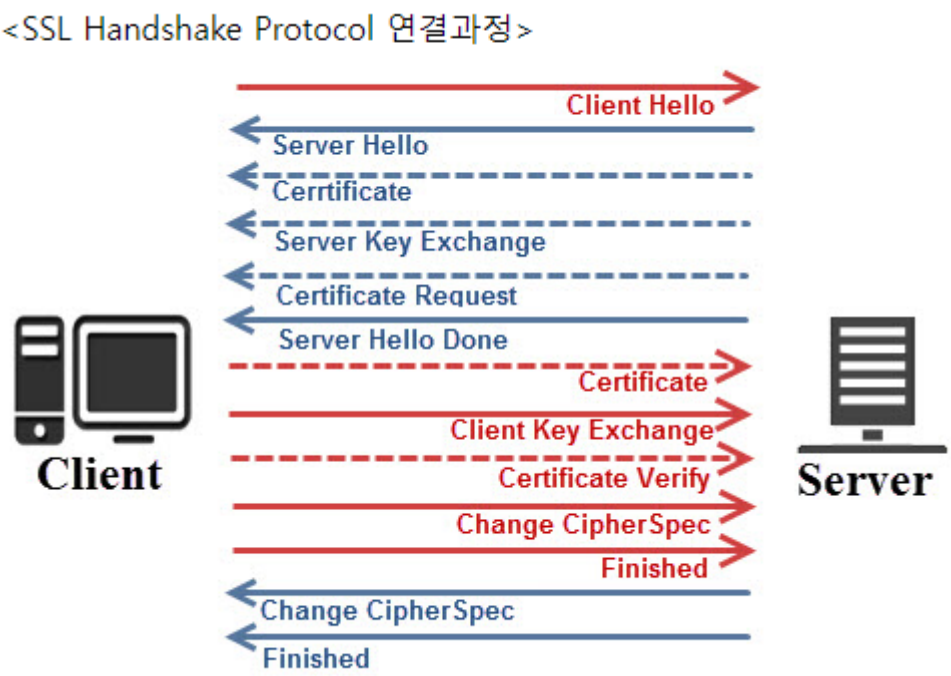
9. SSL

HTTP에서 HTTPS로 변환할 수 있도록 도와주며, 웹사이트 또는 모바일 애플리케이션의 인증 및 암호화된 데이터 전송서비스

▼ **Q1. 인증서 발급 과정 알아보기**

SSL Handshake 과정

1. 클라이언트가 먼저 서버에 접속해서 말을 건다 (Client Hello)
2. 서버 또한 응답하면서 다음 정보를 클라이언트에게 제공한다 (Server Hello)
3. 브라우저는 서버의 SSL인증서가 믿을만한지 확인한다
4. 브라우저는 자신이 생성한 난수와 서버의 난수를 사용하여 Premaster secret을 만든다
5. 서버는 사이트의 비밀키로 브라우저가 보낸 Premaster secret 값을 복호화 한다.
6. 서버 및 클라이언트는 SSL Handshake를 종료하고 HTTPS로 통신을 시작한다.

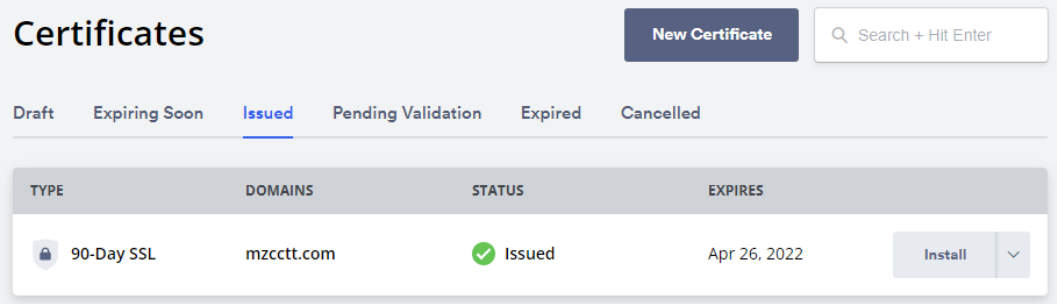


▼ **Task Definitions**

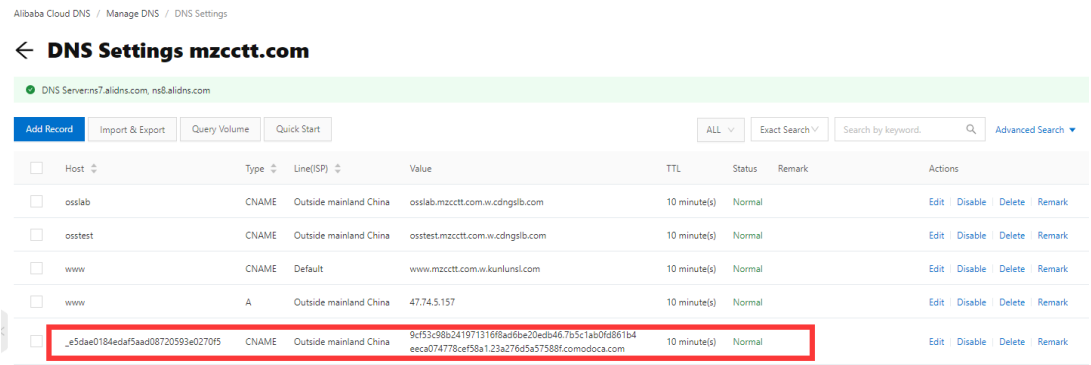
개인 무료 인증서를 생성하여 Alibaba SSL 서비스에 업로드해보기

- **Prerequisites**
  무료 SSL인증서 사이트 가입
  테스트할 ECS 및 SLB 있어야 함
  도메인이 있어야 함

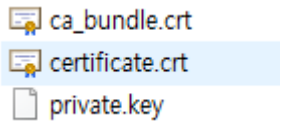
- **Procedure**
  무료SSL인증서 발급 사이트 회원 가입 → 무료 인증서 발급 → 인증 절차 → Alibaba Cloud에 SSL등록 → SLB에 Listener 추가 → HTTPS로 접근 테스트
- **Step 1:**
  1. 무료 SSL 인증서 사이트 접근
  2. 도메인 입력 후 90일 무료 인증서 발급 받기
  3. CSR 및 Private key 자동 받기

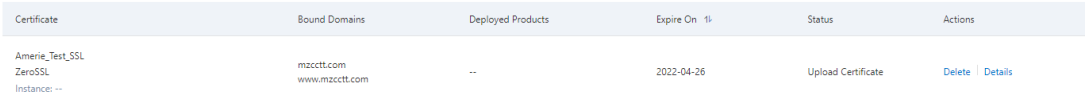


- **Step 2: 인증 절차 - Alibaba Cloud DNS에서 CNAME으로 인증**
  1. DNS 콘솔 접근
  2. CNAME으로 사이트에서 받은 키값 입력
  3. 해당 사이트에서 인증 완료될 때까지 대기

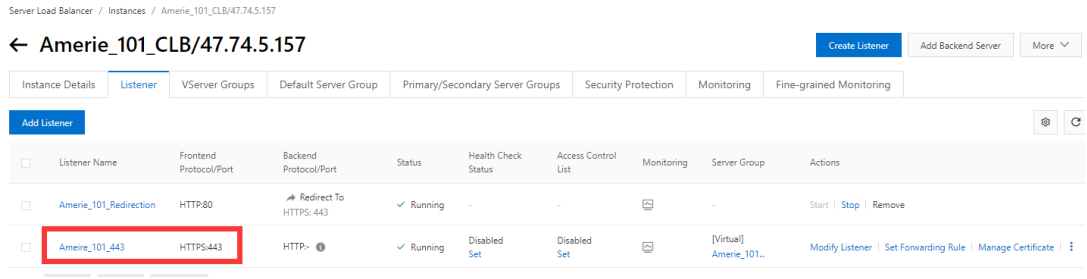


- **Step 3: Alibaba 콘솔에 인증서 등록**
  1. SSL 콘솔 접근
  2. Upload Certificate 클릭
  3. 무료 인증서 발급 시 받은 Certificate.crt 및 private.key에 있는 값으로 등록





- **Step 4: SLB에 Listener(https) 추가**
  1. SLB 콘솔 접근
  2. 해당 SLB의 백엔드 ECS는 모두 Running 상태이어야 함
  3. Add Listener 추가 (443 포트)



- **Step 5: HTTPS로 접근 테스트 - 성공**
  1. 해당 SLB와 연결된 도메인 주소로 접근 (HTTPS)