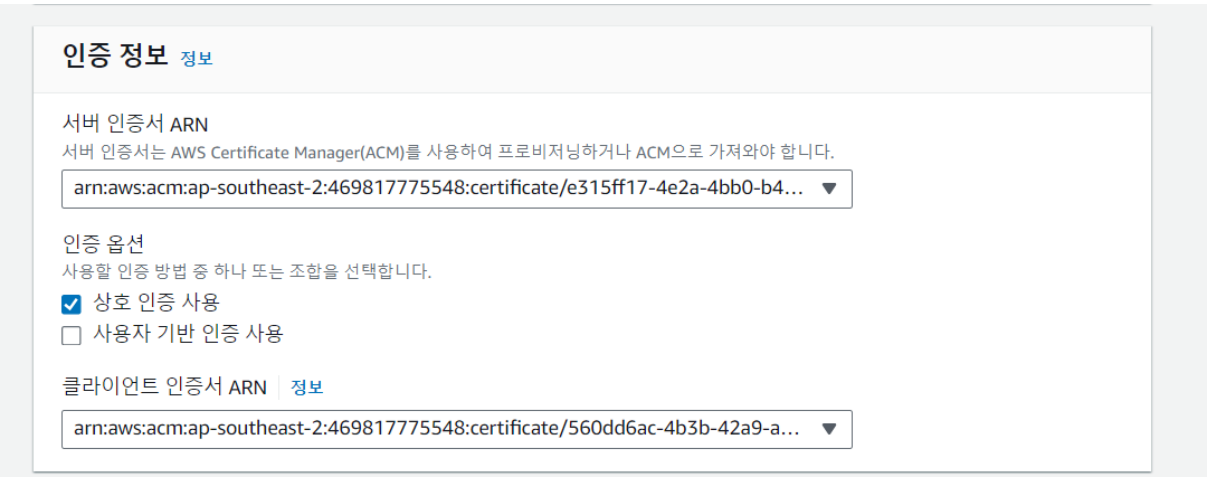
6/28


인증 정보 정보
서버 인증서 ARN
서버 인증서는 AWS Certificate Manager(ACM)를 사용하여 프로비저닝하거나 ACM으로 가져와야 합니다.
arn:aws:acm:ap-southeast-2:469817775548:certificate/e315ff17-4e2a-4bb0-b4…
인증 옵션
사용할 인증 방법 중 하나 또는 조합을 선택합니다.
상호 인증 사용
사용자 기반 인증 사용
클라이언트 인증서 ARN 정보
arn:aws:acm:ap-southeast-2:469817775548:certificate/560dd6ac-4b3b-42a9-a…

기타 파라미터 - *선택 사항*

DNS 서버 1 IP 주소
사용할 DNS 서버의 IP 주소입니다. 기본 DNS 서버는 없습니다.

10.0.0.0

DNS 서버 2 IP 주소
사용할 DNS 서버의 IP 주소입니다. 기본 DNS 서버는 없습니다.

10.0.0.1

전송 프로토콜 | 정보
TLS 세션에서 사용하는 전송 프로토콜입니다.

- (●) UDP
- ( ) TCP

분할 터널 활성화 정보

VPC ID

vpc-053d9694eb2b3665c (cloudwave)

보안 그룹 ID
엔드포인트에 적용할 보안 그룹입니다.

보안 그룹 선택

sg-0091b6128c16f8917 (ljk-pri-svr-sg) ×
launch-wizard-1 created 2024-06-28T00:03:33.161Z

VPN 포트
AWS Client VPN은 TCP 및 UDP 모두에 대해 포트 443과 1194를 지원합니다.

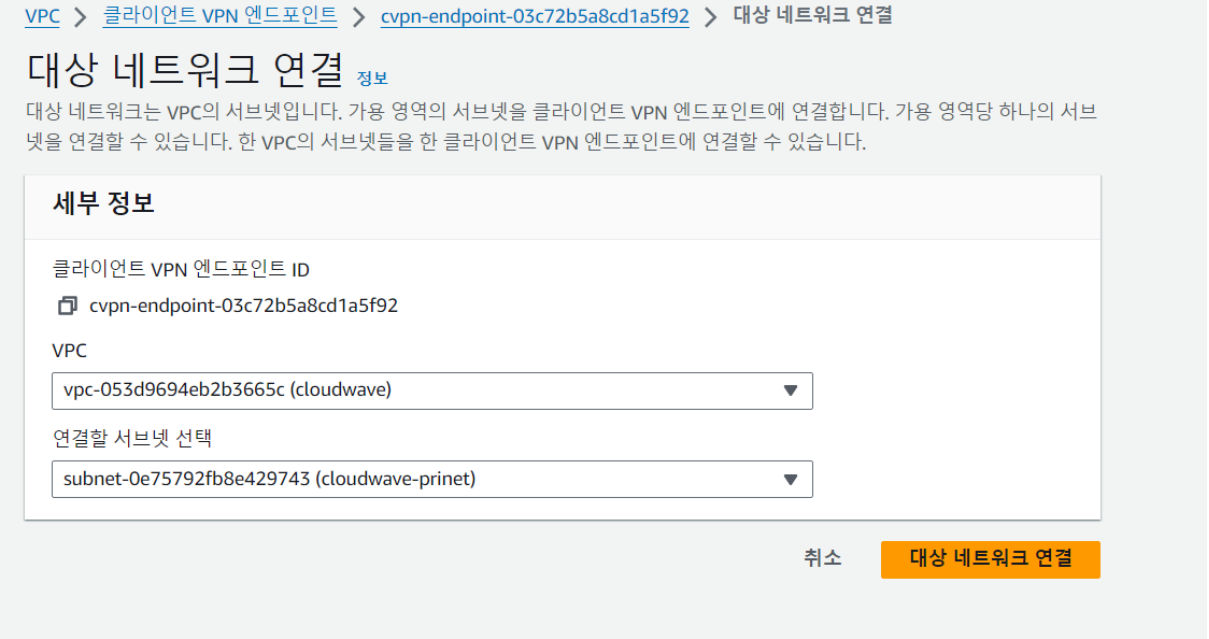
1194

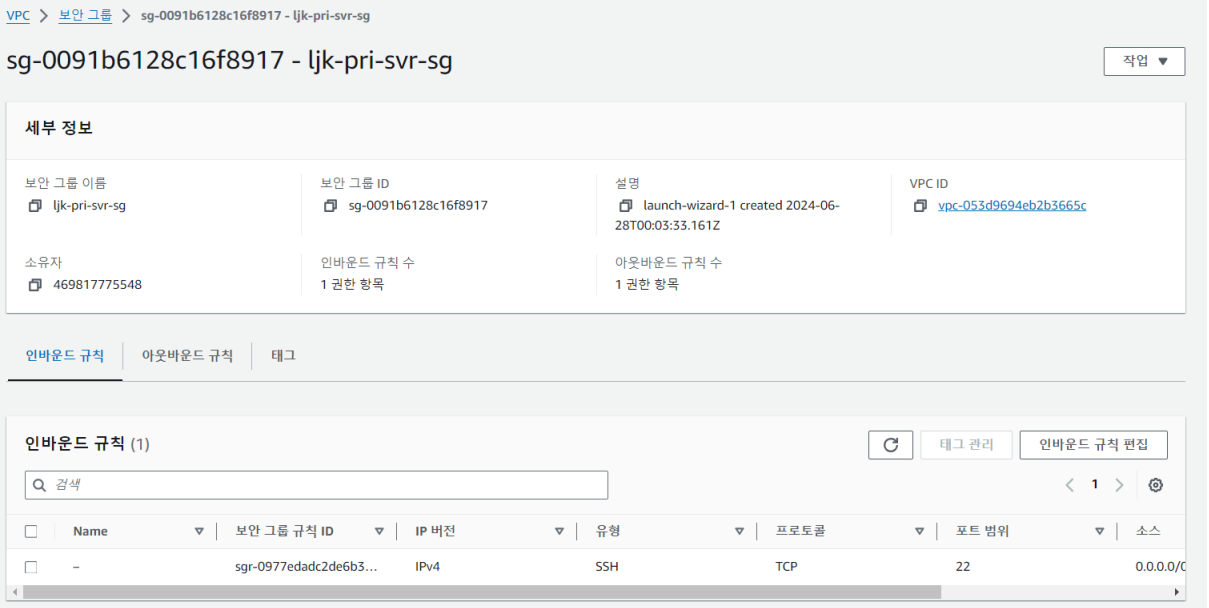
셀프 서비스 포털 활성화 정보

세션 제한 시간 | 정보

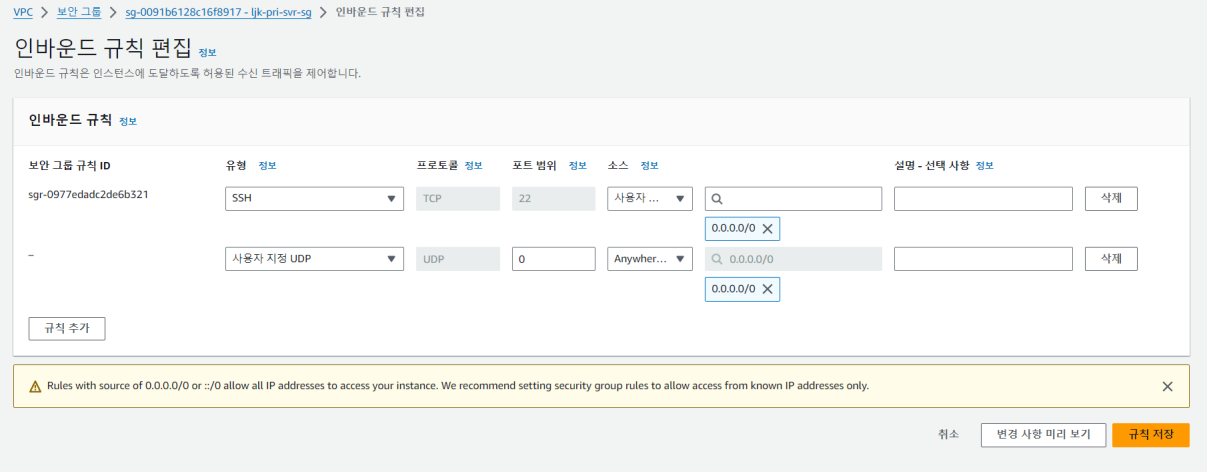
24

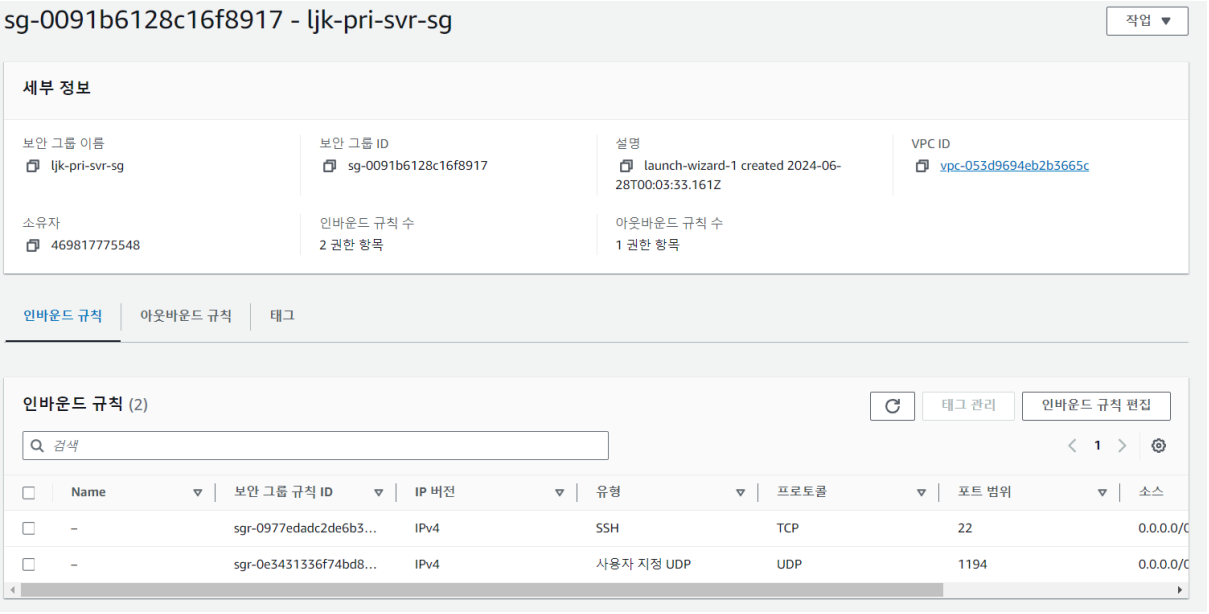
클라이언트 로그인 배너 사용 설정 정보

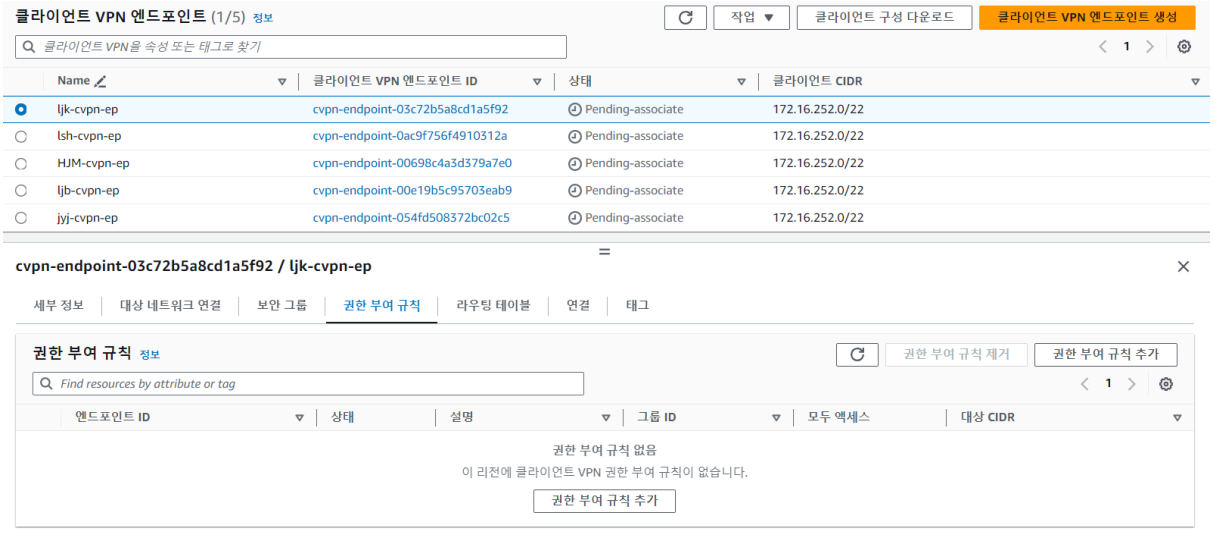


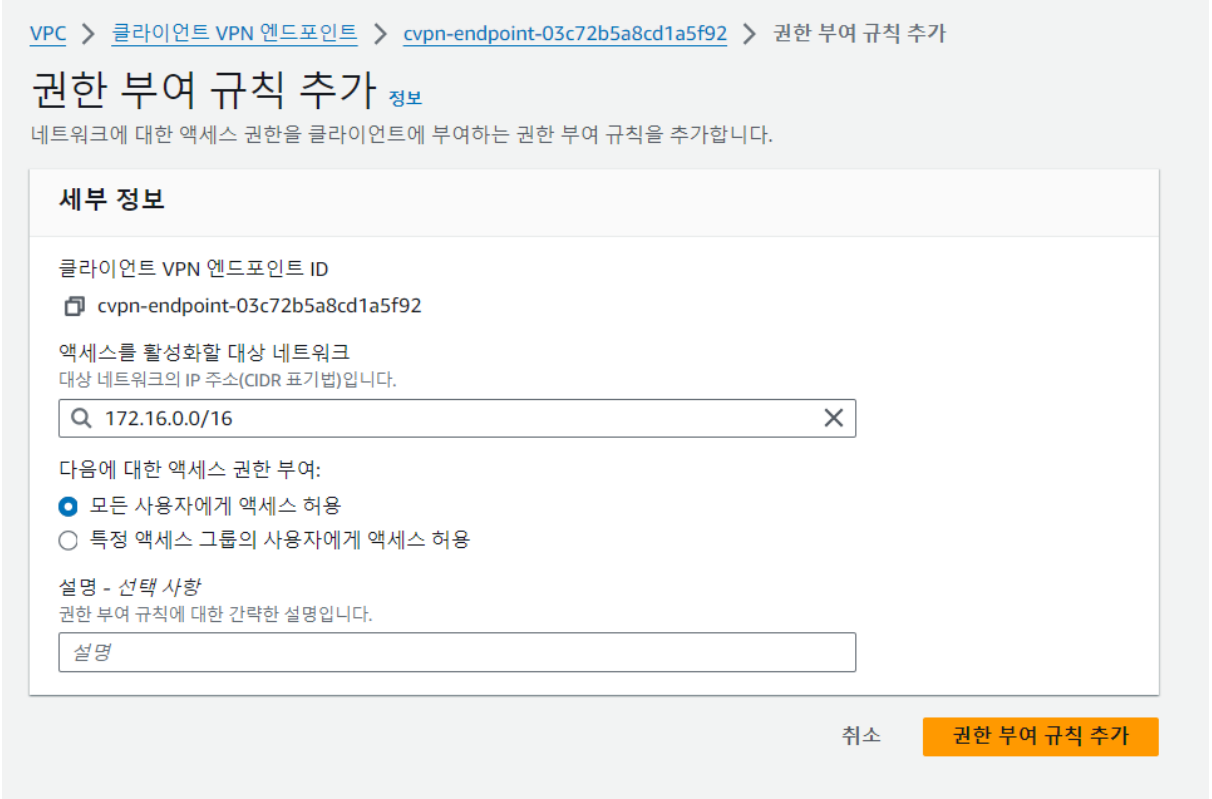


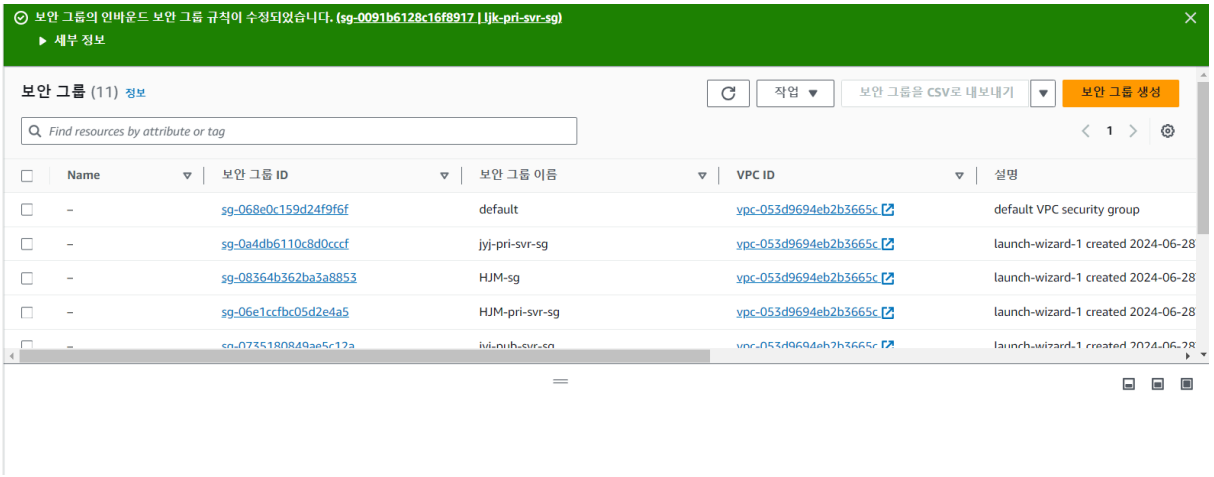
udp로 만들었기에 udp 규칙 만들어야 사용 가

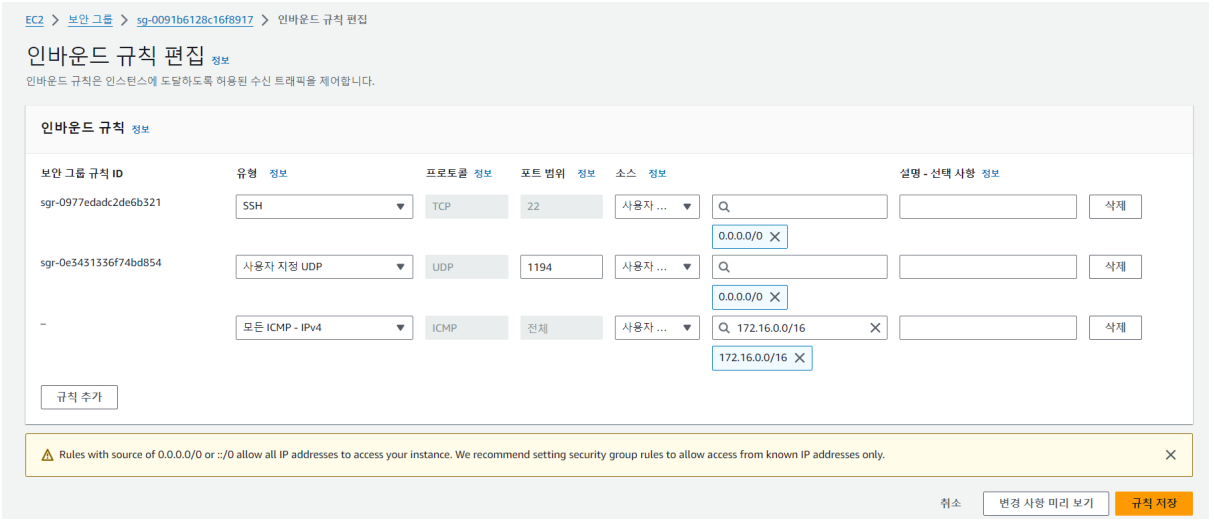

VPC > 보안 그룹 > sg-0091b6128c16f8917 - ljk-pri-svr-sg > 인바운드 규칙 편집
인바운드 규칙 편집 정보
인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.
인바운드 규칙 정보
보안 그룹 규칙 ID
유형 정보
프로토콜 정보
포트 범위 정보
소스 정보
설명 - 선택 사항 정보
sgr-0977edadc2de6b321
SSH
TCP
22
사용자 ...
0.0.0.0/0
삭제
-
사용자 지정 UDP
UDP
0
Anywher...
0.0.0.0/0
0.0.0.0/0
삭제
규칙 추가
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
취소
변경 사항 미리 보기
규칙 저장


sg-0091b6128c16f8917 - ljk-pri-svr-sg
작업
세부 정보
보안 그룹 이름
ljk-pri-svr-sg
보안 그룹 ID
sg-0091b6128c16f8917
설명
launch-wizard-1 created 2024-06-28T00:03:33.161Z
VPC ID
vpc-053d9694eb2b3665c
소유자
469817775548
인바운드 규칙 수
2 권한 항목
아웃바운드 규칙 수
1 권한 항목
인바운드 규칙
아웃바운드 규칙
태그
인바운드 규칙 (2)
태그 관리
인바운드 규칙 편집
검색
1
Name
보안 그룹 규칙 ID
IP 버전
유형
프로토콜
포트 범위
소스
-
sgr-0977edadc2de6b3...
IPv4
SSH
TCP
22
0.0.0.0/0
-
sgr-0e3431336f74bd8...
IPv4
사용자 지정 UDP
UDP
1194
0.0.0.0/0


클라이언트 VPN 엔드포인트 (1/5) 정보
작업
클라이언트 구성 다운로드
클라이언트 VPN 엔드포인트 생성
클라이언트 VPN을 속성 또는 태그로 찾기
Name
클라이언트 VPN 엔드포인트 ID
상태
클라이언트 CIDR
ljk-cvpn-ep
cvpn-endpoint-03c72b5a8cd1a5f92
Pending-associate
172.16.252.0/22
lsh-cvpn-ep
cvpn-endpoint-0ac9f756f4910312a
Pending-associate
172.16.252.0/22
HJM-cvpn-ep
cvpn-endpoint-00698c4a3d379a7e0
Pending-associate
172.16.252.0/22
ljb-cvpn-ep
cvpn-endpoint-00e19b5c95703eab9
Pending-associate
172.16.252.0/22
jyj-cvpn-ep
cvpn-endpoint-054fd508372bc02c5
Pending-associate
172.16.252.0/22
cvpn-endpoint-03c72b5a8cd1a5f92 / ljk-cvpn-ep
세부 정보
대상 네트워크 연결
보안 그룹
권한 부여 규칙
라우팅 테이블
연결
태그
권한 부여 규칙 정보
권한 부여 규칙 제거
권한 부여 규칙 추가
Find resources by attribute or tag
엔드포인트 ID
상태
설명
그룹 ID
모두 액세스
대상 CIDR
권한 부여 규칙 없음
이 리전에 클라이언트 VPN 권한 부여 규칙이 없습니다.
권한 부여 규칙 추가


VPC
클라이언트 VPN 엔드포인트
cvpn-endpoint-03c72b5a8cd1a5f92
권한 부여 규칙 추가
권한 부여 규칙 추가 정보
네트워크에 대한 액세스 권한을 클라이언트에 부여하는 권한 부여 규칙을 추가합니다.
세부 정보
클라이언트 VPN 엔드포인트 ID
cvpn-endpoint-03c72b5a8cd1a5f92
액세스를 활성화할 대상 네트워크
대상 네트워크의 IP 주소(CIDR 표기법)입니다.
172.16.0.0/16
다음에 대한 액세스 권한 부여:
모든 사용자에게 액세스 허용
특정 액세스 그룹의 사용자에게 액세스 허용
설명 - 선택 사항
권한 부여 규칙에 대한 간략한 설명입니다.
설명
취소
권한 부여 규칙 추가





vpn 에서 클라이언트 구성 다운로드한 뒤 내용 수

```
client
dev tun
proto udp
remote cvpn-endpoint-03c72b5a8cd1a5f92.prod.clientvpn.ap-southeast-2.amazonaws.com 1194
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIDNjCCAh6gAwIBAgIULVxYBk4RzEYJJGygvTpDWhCGHxEwDQYJKoZIhvcNAQEL
BQAwDzENMAsGA1UEAwwEaG9zdDAeFw0yNDA2MjcwNzQxMjFaFw0zNDA2MjUwNzQx
MjFaMA8xDTALBgNVBAMMBGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDXSgFISepr8GUWifXmbCRgJFSJ8rKJ9IGfAifYnsZy0lMlJSUhJMlStxKD
zwMzMdzTqTgJ4bCvfYQSGONHAEJVhRfYeLtggtcf0ut4CtQOFaf1IGHLtUKt256V
Jjzx+AUYHCxMxo1m/lfYtidbDh6mLXFC0ZlozjGIcKmhe+sOgaipB7cY0BF7w2f9
EdVvuX/uUmoAUuItifoDWLU2hJxxr9U4onvSXpf8bbLXSLLy6I2Ay2xQXoOw/1Vj
s+egfV35heHgFwLwik7CrOj/ISmYR+SKbQygROhN5g+fv6WoNQTFLVRb5H48BKGk
DW/BzHoxvy0xNQAoBcoujwuyaM6BAgMBAAGjgYkwgYYwHQYDVR0OBBYEFIvIqeXx
qAz5+63yLYlRw09mwAGeMEoGA1UdIwRDMEGAFIvIqeXxqAz5+63yLYlRw09mwAGe
oROkETAPMQ0wCwYDVQQDDARob3N0ghQtXFgGThHMRgkkbKC9OkNaEIYfETAMBgNV
```

remote ljk.cvpn-endpoint-03c72b5a8cd1a5f92.prod.clientvpn.ap-southeast-2.amazonaws.com 1194

호스트명을 붙인다.

또

<cert>

클라이언트 인증서

</cert>

<key>

클라이언트 키

</key>

를 추가해준다.

해당 ovpn으로 어디서든 접속이 가능하다.

- openvpn3 설치하기
  $ sudo mkdir -p /etc/apt/keyrings && curl -fsSL

https://packages.openvpn.net/packages-repo.gpg | sudo tee /etc/apt/keyrings/openvpn.asc
$ DISTRO=$(lsb_release -c | awk '{print $2}')
$ echo "deb [signed-by=/etc/apt/keyrings/openvpn.asc]

https://packages.openvpn.net/openvpn3/debian $DISTRO main" | sudo tee /etc/apt/sources.list.d/openvpn-packages.list
$ sudo apt update
$sudo apt install openvpn3

- openvpn연결하기

$ openvpn3 session-start --config downloaded-client-config.ovpn

요약

1. 각 리전의 public subnet에 EC2 1대, private subnet에 EC2 1대
2. WSL 우분투에서 ca 생성, server/client 인증서 생성
3. server/client 인증서 AWS Certificate Manager에 등록(인증서 가져오기)
4. Client VPN 엔드포인트 생성하기
5. 클라이언트 구성 다운로드하기
6. 클라이언트 구성 내용 수정하기
   임의의 호스트명 추가
   클라이언트 인증서 추가 <cert></cert>
   클라이언트 키 추가 <key></key>
7. openvpn 클라이언트 프로그램 설치
8. 클라이언트 구성 파일을 이용하여 vpn 접속

DHCP

호스트에 IP관련 정보(IP 주소, 서브넷마스크, 게이트웨이, DNS 주소 등)들을 자동으로 할당할 수 있도록 하는 프로토콜, 서비스.

DHCP는 4가지 메시지를 이용해서 클라이언트와 서버간에 통신을 함.

DHCP는 UDP를 사용하고, 포트번호는 클라이언트(68번), 서버(67번)을 사용함.

DHCP는 목적지주소로 브로드캐스트와 유니캐스트 모두 사용함. DHCP 프로그램 설정에 따라서 정해짐.

클라이언트(68번) 서버(67번)

Discover : 클라이언트가 서버를 찾기 위한 메세지

offer: 서버가 클라이언트에게 할당할 정보를 담은 메세지

request: 해당 정보를 사용하겠다는 클라이언트 요청 메세지

ack : 사용을 승인하는 서버 메시지