모듈 프로젝트 3-2

저축은행 회원 서비스 클라우드 구축

2021년 12월 09일 주지현

내용

[vpc 생성 4](#_Toc91752565)

[서브넷 생성 6](#_Toc91752567)

[게이트웨이 생성 8](#_Toc91752568)

[EC2생성 9](#_Toc91752569)

[탄력적 IP주소 12](#_Toc91752571)

[NACL 13](#_Toc91752572)

[NACL 분리 15](#_Toc91752573)

[보안 그룹 설정 16](#_Toc91752574)

[DB 생성 16](#_Toc91752575)

[Aurora DB를 사용할 때 17](#_Toc91752576)

[인스턴스로 AMI 이미지 만들기 22](#_Toc91752577)

[시작 템플릿 만들기 23](#_Toc91752578)

[오토 스케일링 25](#_Toc91752579)

[NLB 29](#_Toc91752580)

[Windows 원격 접속 연결(시도) 31](#_Toc91752581)

[Windows Server IIS 설치 34](#_Toc91752582)

[Bastion Host 설정 38](#_Toc91752583)

[NACL & 보안 그룹 설정 38](#_Toc91752584)

[Windows Server용 인스턴스 생성 39](#_Toc91752585)

[방화벽 생성 41](#_Toc91752586)

[네트워크 규칙 그룹 생성 41](#_Toc91752587)

[방화벽 정책 생성 44](#_Toc91752588)

[방화벽 생성 49](#_Toc91752589)

[WAF 생성 52](#_Toc91752590)

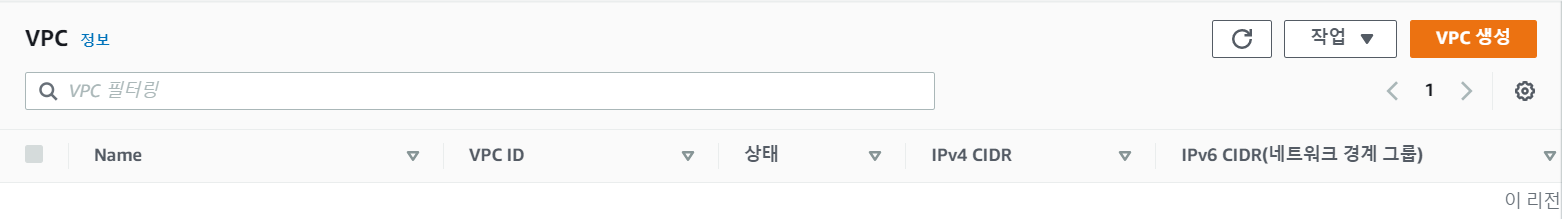
[+ISMS-P 충족여부 58](#_Toc91752591)

|  |  |  |  |
| --- | --- | --- | --- |
| 만든 사람 | 만든 날짜 | 버전 | 설명 |
| 주지현 | 2021.12.09 | 0.0.1 | 문서 생성 |
| 주지현 | 2021.12.28 | 0.1.0 | 새로운 항목 추가 |
| 주지현 | 2021.12.29 | 0.2.0 | 새로운 항목 추가 |
| 주지현 | 2021.12.29 | 0.3.0 | 새로운 항목 추가 |
| 주지현 | 2021.12.29 | 0.4.0 | 새로운 항목 추가 |
| 주지현 | 2021.12.30 | 0.1.1 | 세부 사항 수정 |

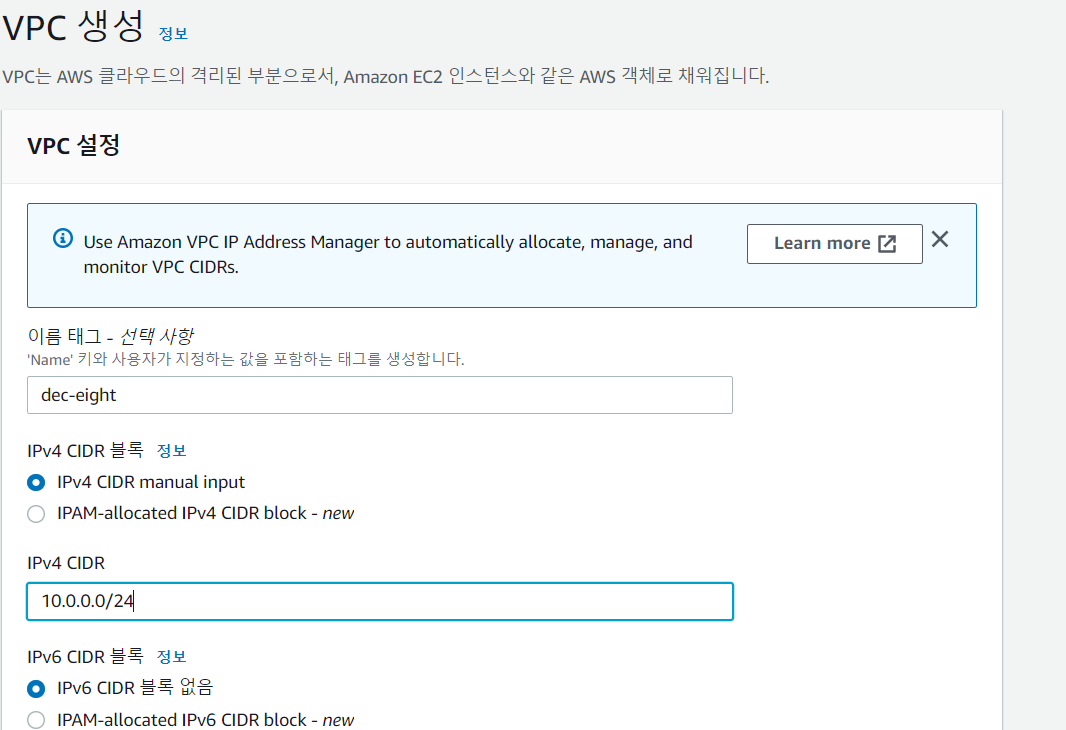
# vpc 생성

# 

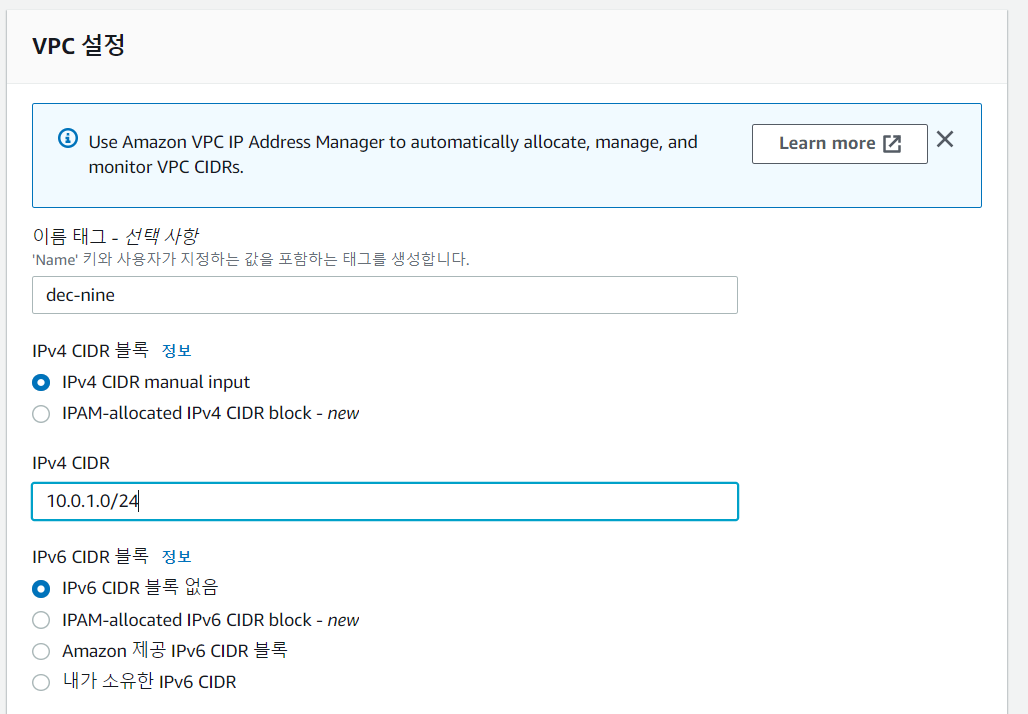
아무것도 없는 VPC 대시보드의 모습이다.



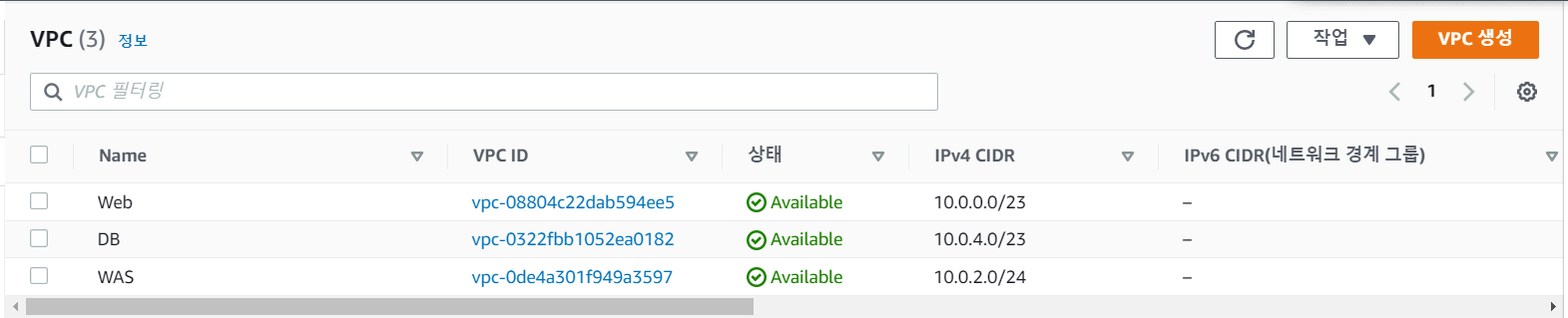
VPC를 생성한다.



웹 인스턴스가 들어갈 VPC를 생성한다.

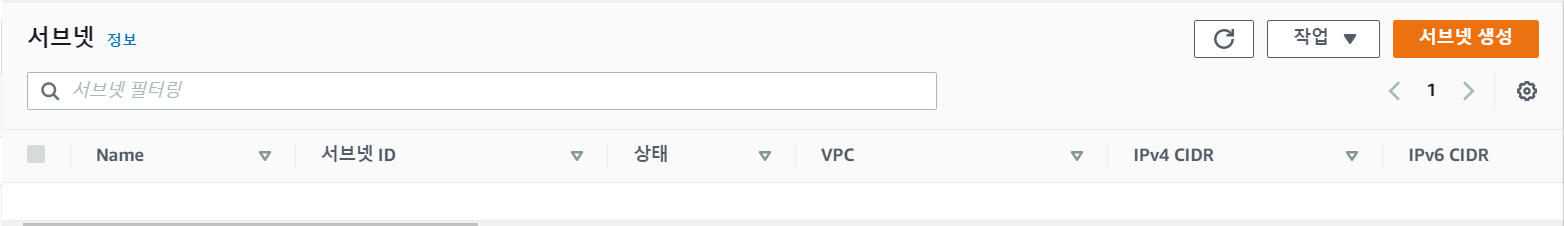


마찬가지로 WAS 인스턴스가 들어갈 VPC를 생성한다. DB가 들어갈 VPC도 같은 방법으로 작업한다. (12.28일 수정사항)

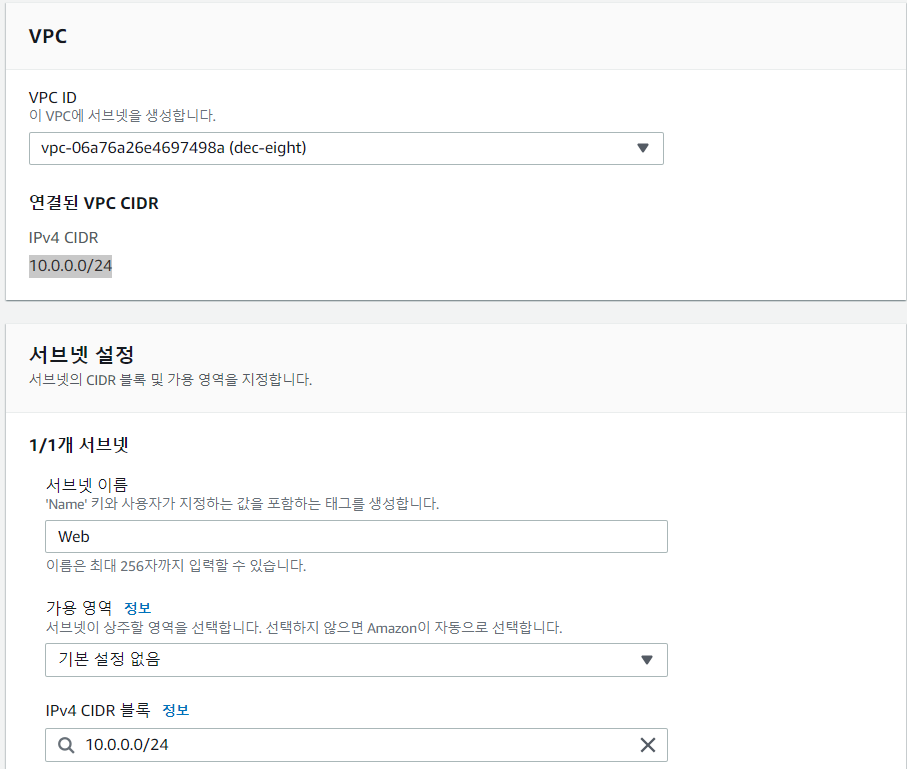


VPC 23가 생성된 것을 확인할 수 있다.

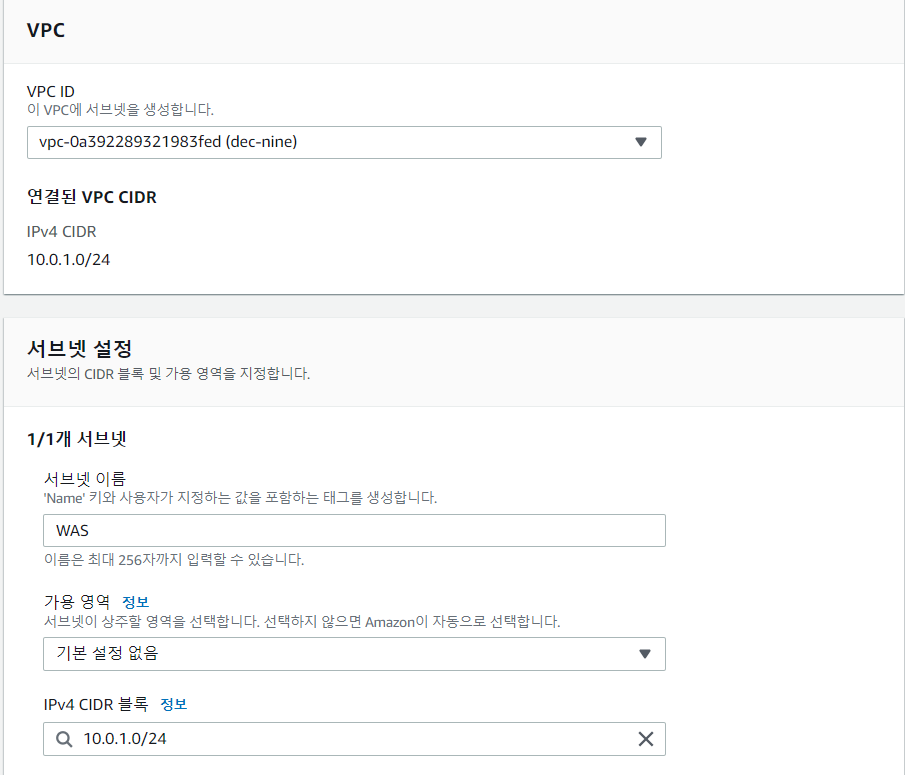
# 서브넷 생성



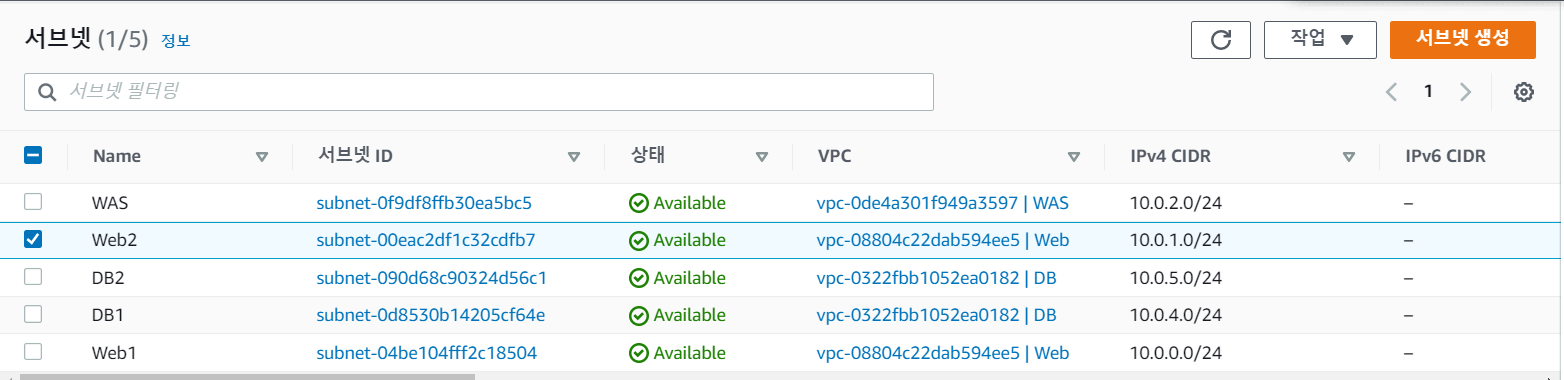
서브넷을 생성한다.



웹이 사용할 서브넷을 만들어준다. 이때 ALB를 사용할 것이라면 가용 영역을 다르게 해서 서브넷을 2개 만들어야 한다. (예.Web1 서브넷의 가용 영역이 us-a라면 Web2 서브넷의 가용 영역은 us-b여야 한다.)

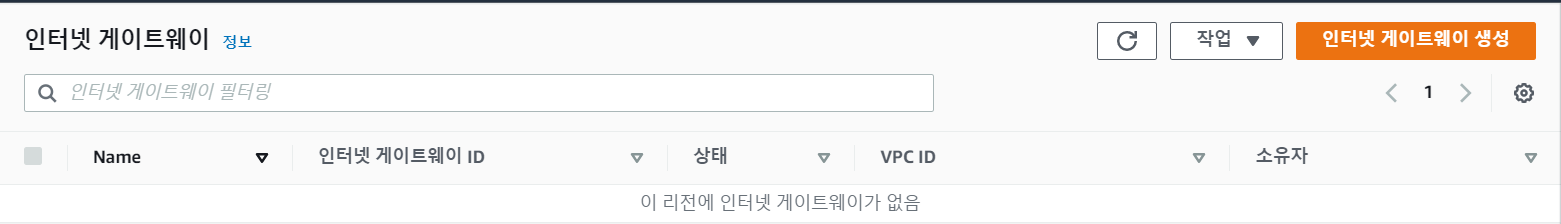


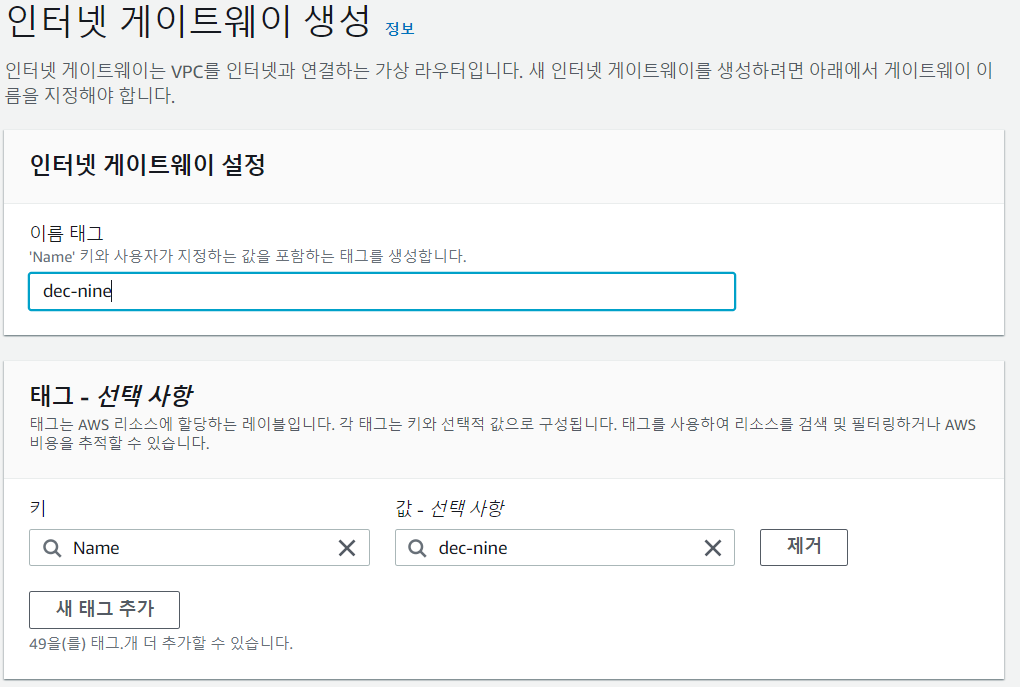
같은 방법으로 WAS와 DB가 사용할 서브넷을 만들어준다. DB도 클러스터링을 한다면 서브넷을 두 개 만들어야 한다.

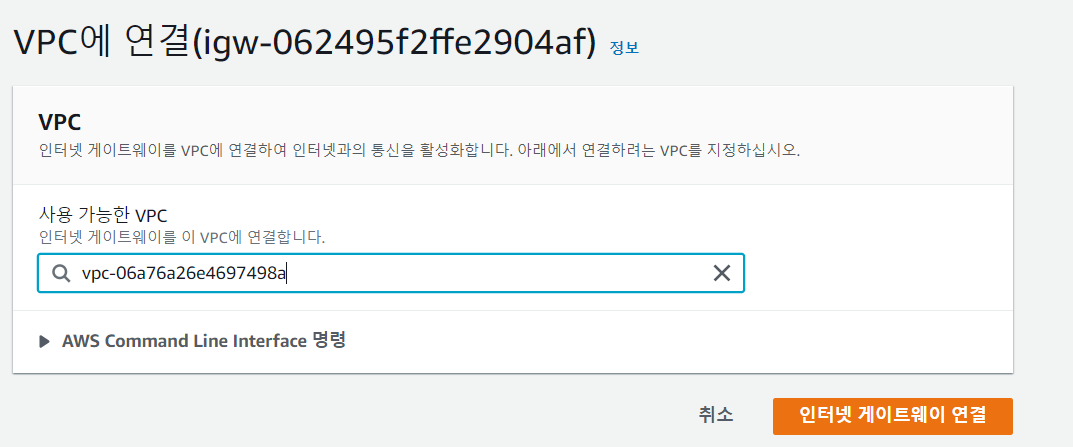


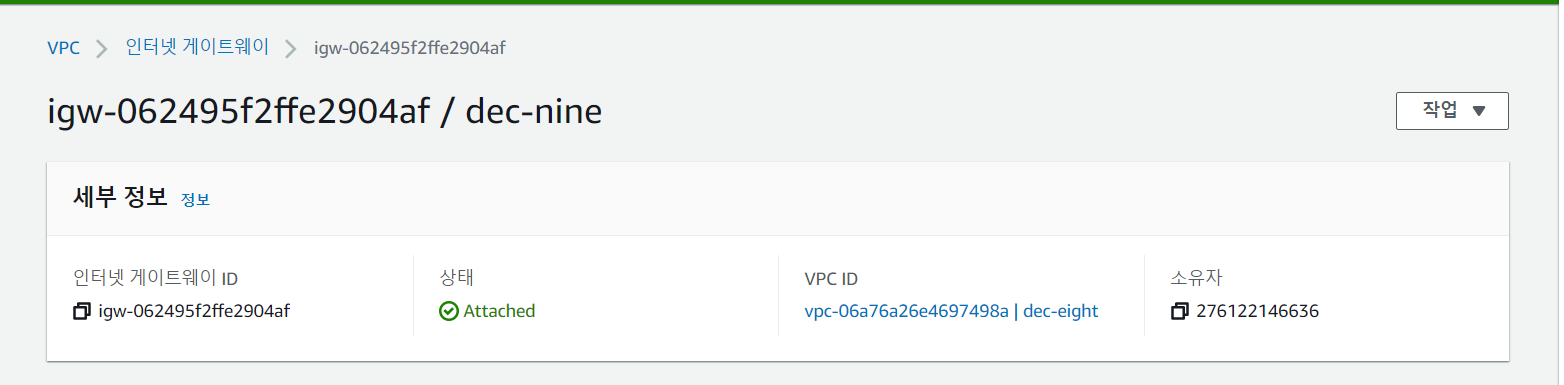
서브넷 5개가 생성된 것을 확인한다.

# 게이트웨이 생성







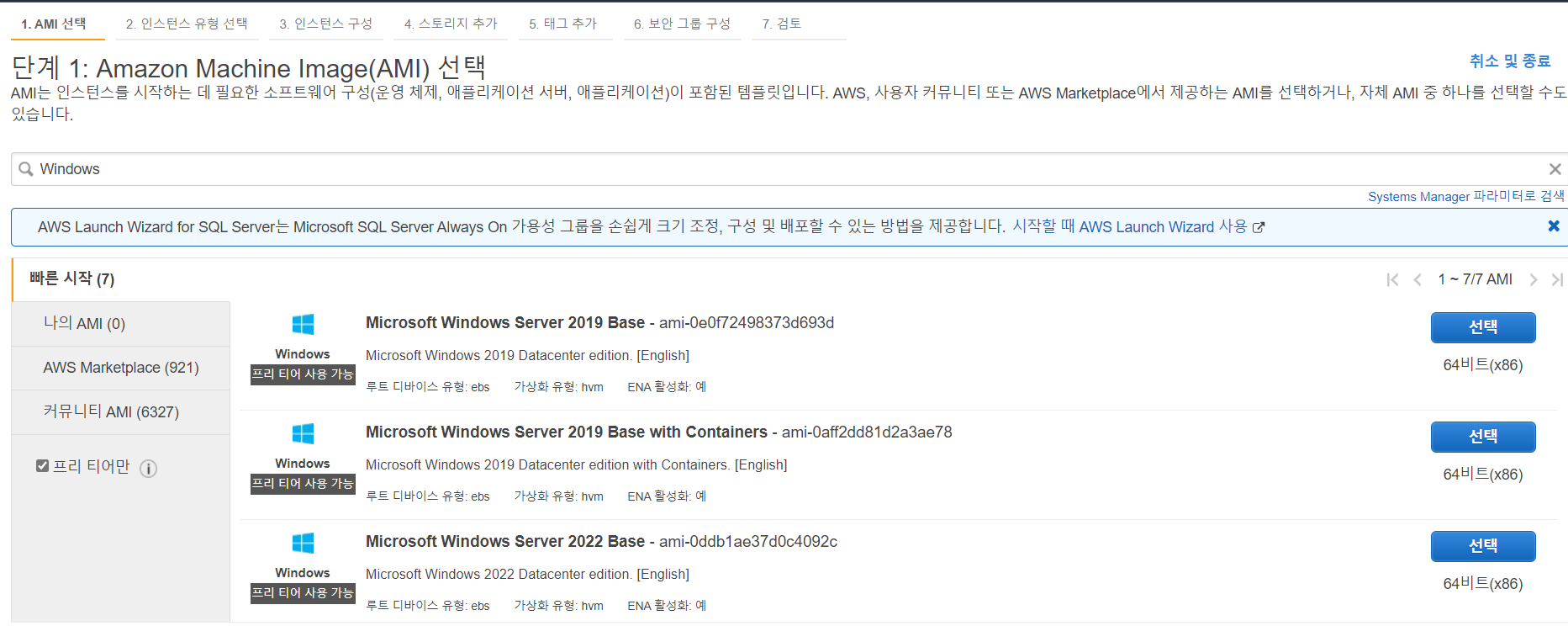


인터넷 게이트웨이를 생성해서 웹 인스턴스가 있는 VPC에 연결해 준다.

# EC2생성

# 

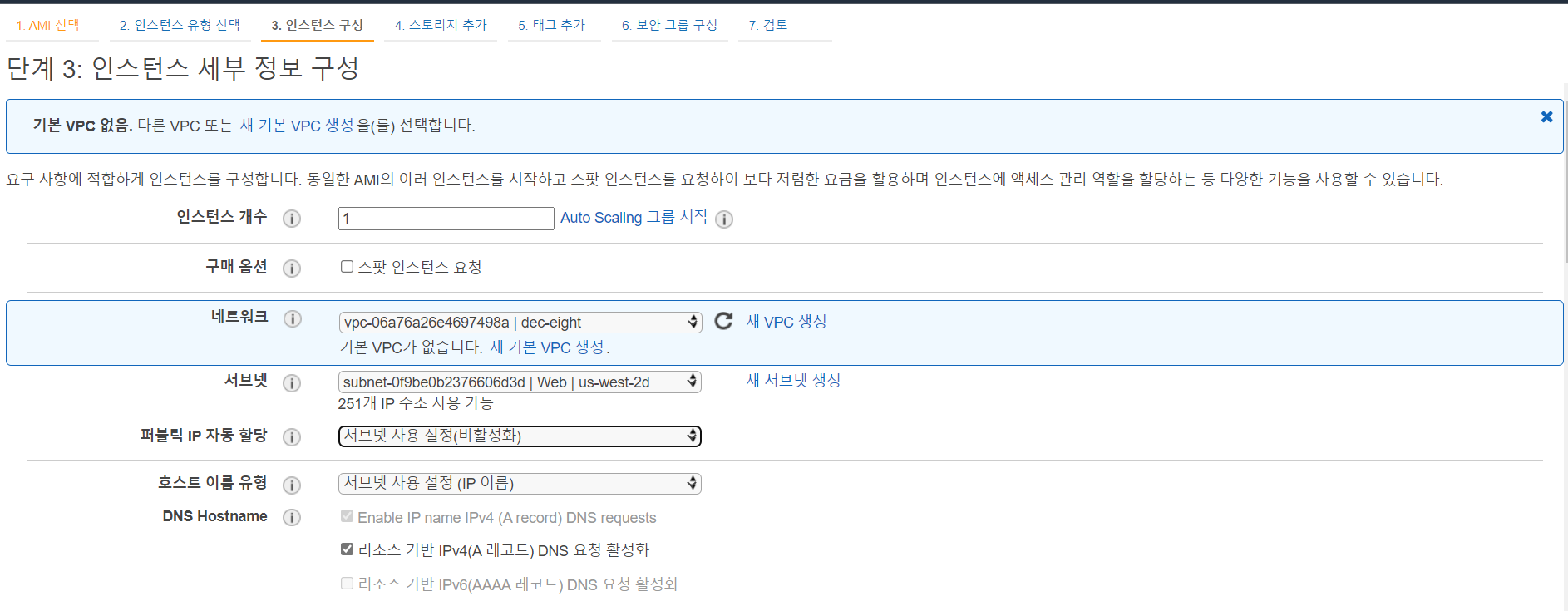
비어 있는 EC2 대시보드를 확인한다.(탄력적 IP는 이전에 만들었다.)



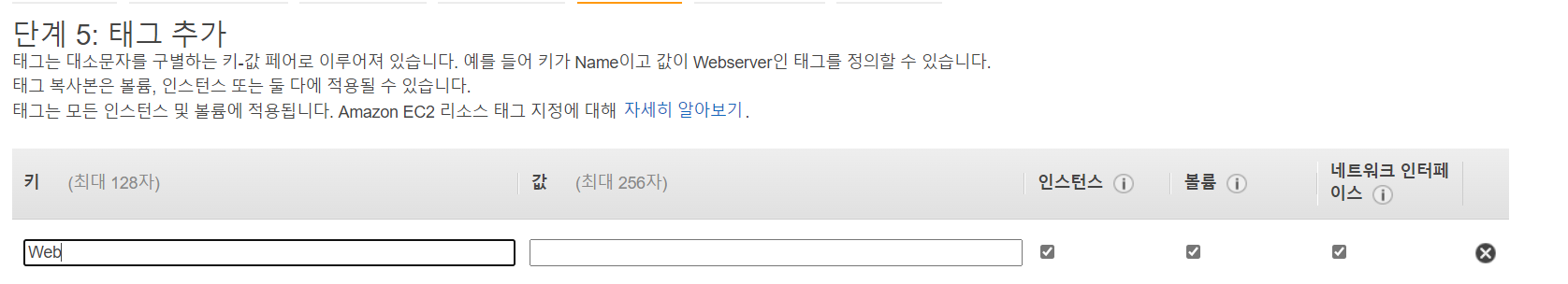
웹 인스턴스로 실행할 Windows Server 제품 중 프리 티어 가능 제품을 찾아 선택한다.



인스턴스 유형도 역시 프리 티어를 선택한다.



연결할 VPC와 서브넷을 확인한다.

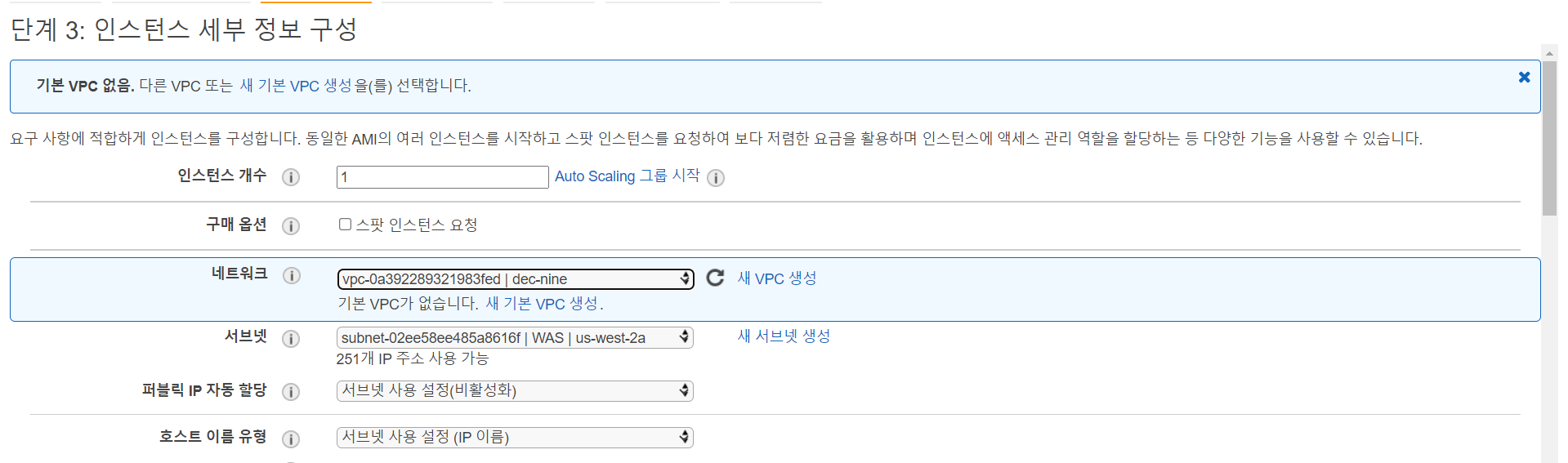


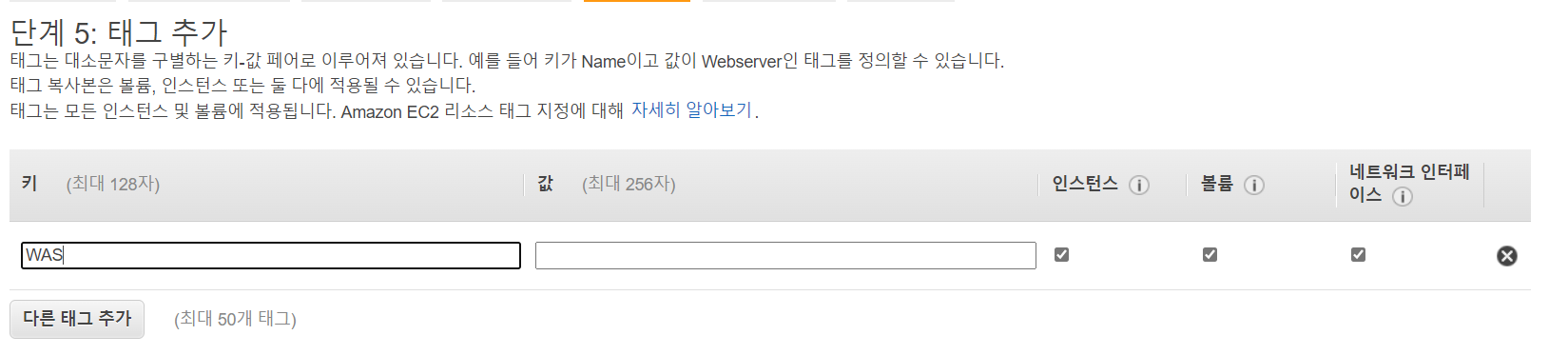
태그를 추가한다.



설정 사항을 검토하고 인스턴스 시작을 누른다. 이때 키 페어 선택창이 뜨면 키를 다운로드 받고 인스턴스를 시작한다.

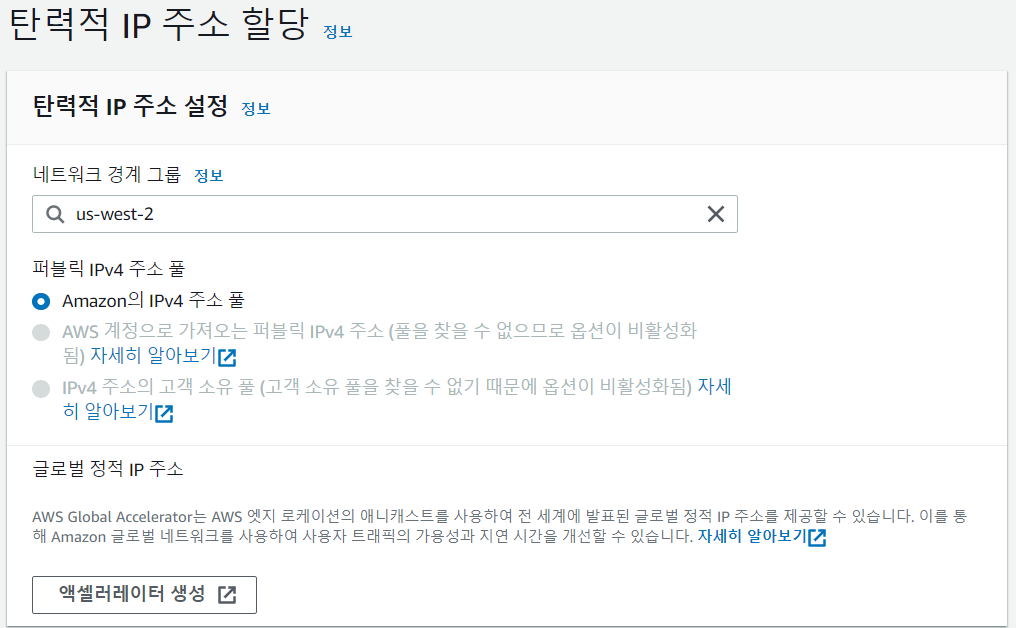


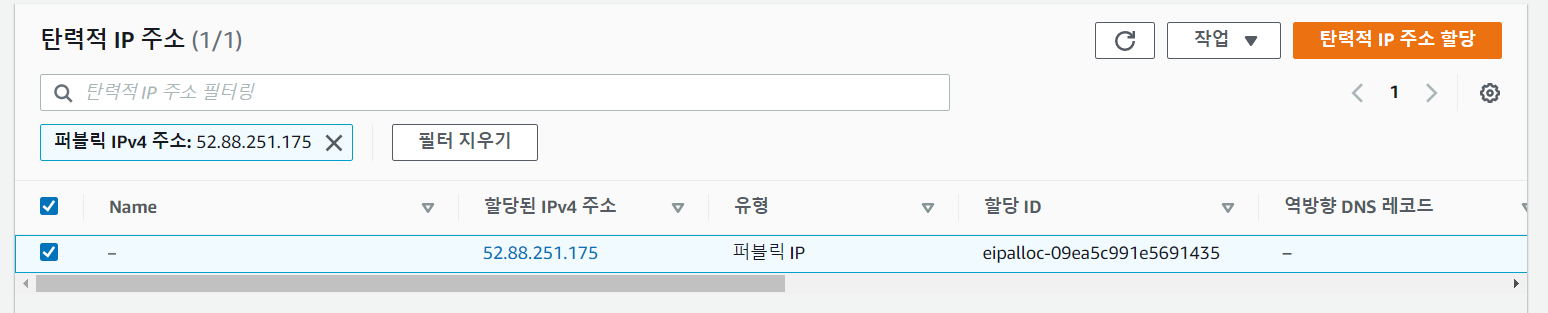




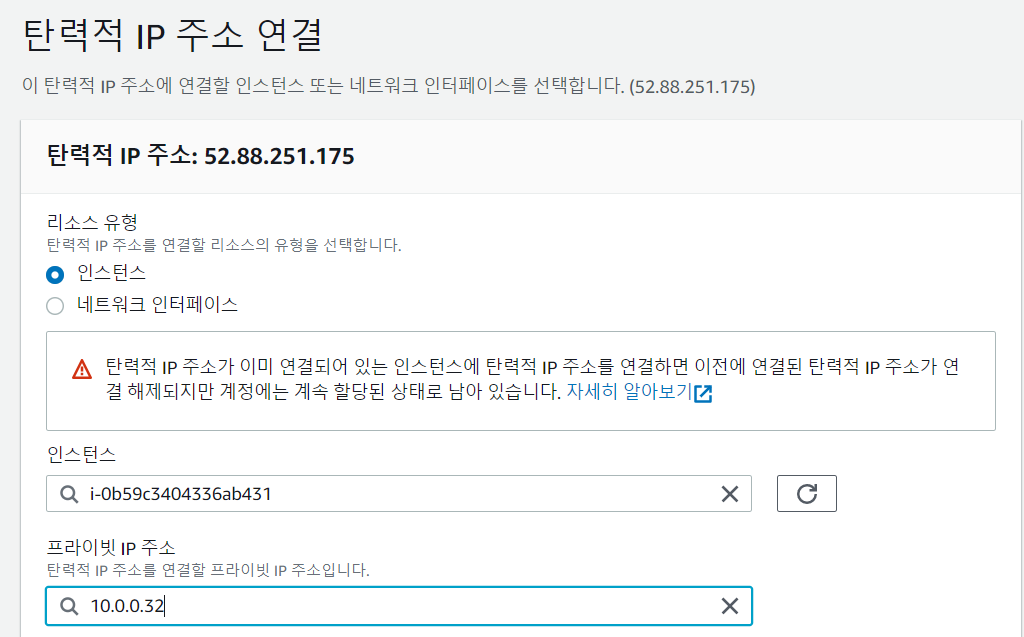
WAS 인스턴스도 세부 사항만 달리해서 같은 방법으로 생성한다.

# 탄력적 IP주소



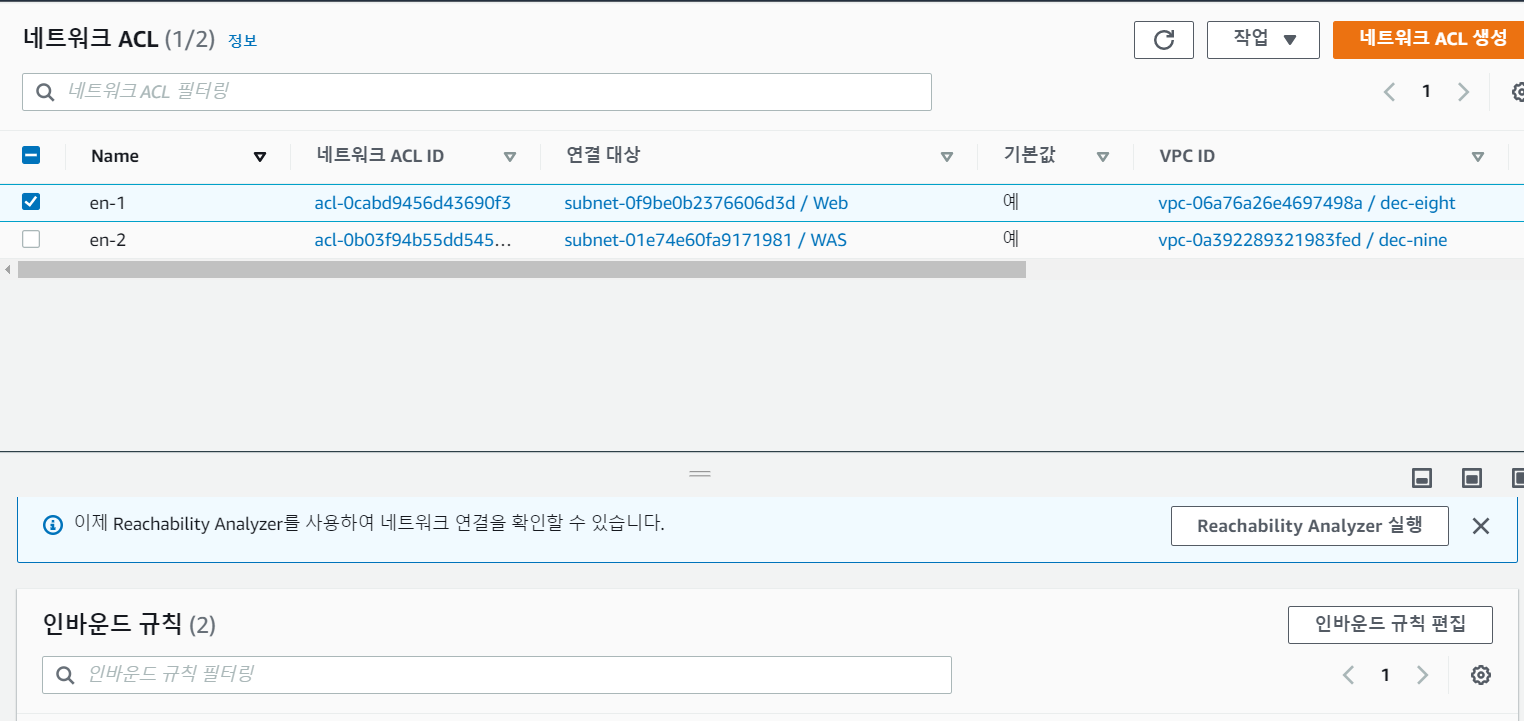


탄력적 IP 주소를 생성한다.



웹 인스턴스와 연결한다.

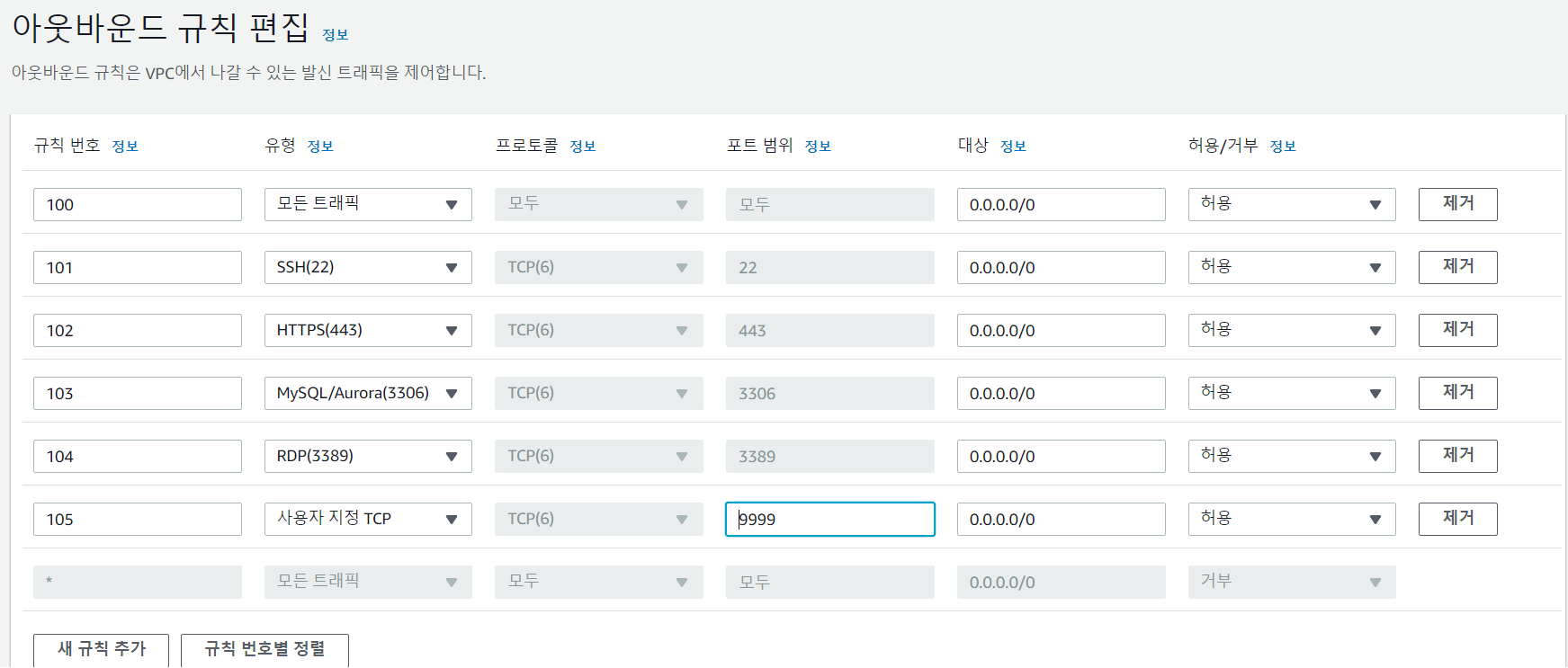
# NACL



서브넷 생성과 동시에 만들어진 NACL이다.

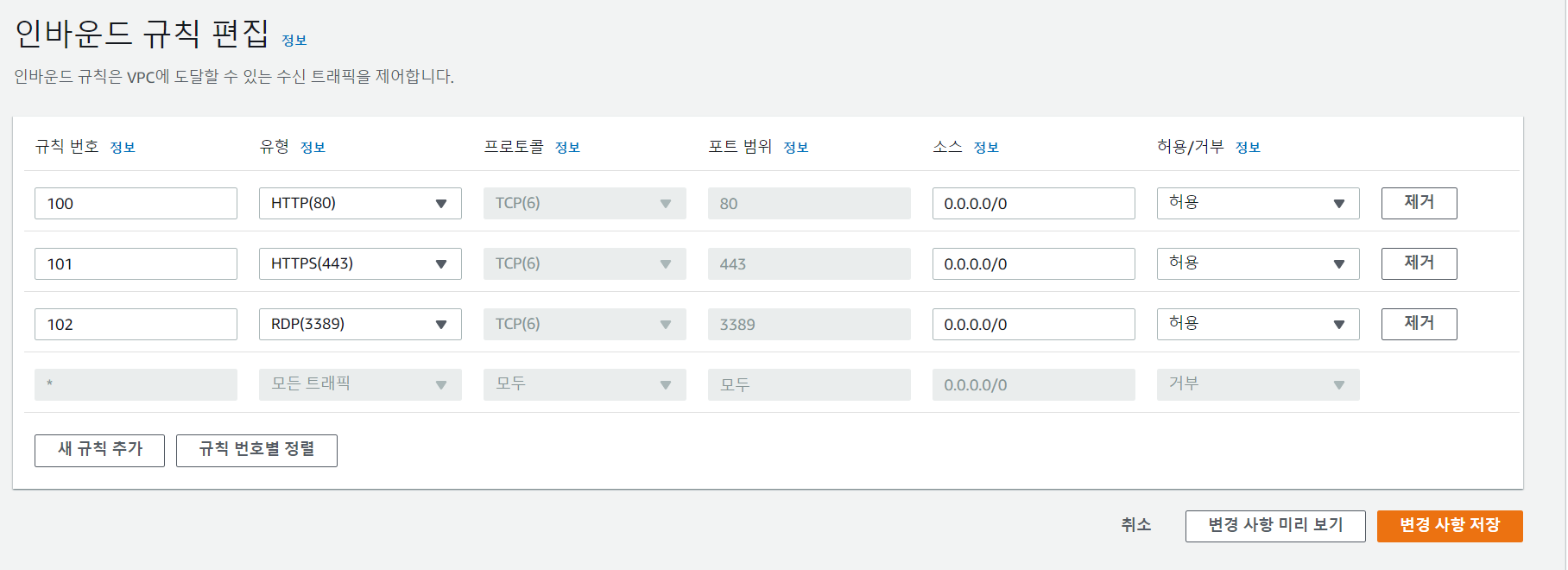


인바운드 규칙을 편집한다. 플라스크 포트는 목록에 없으므로 직접 기입한다.

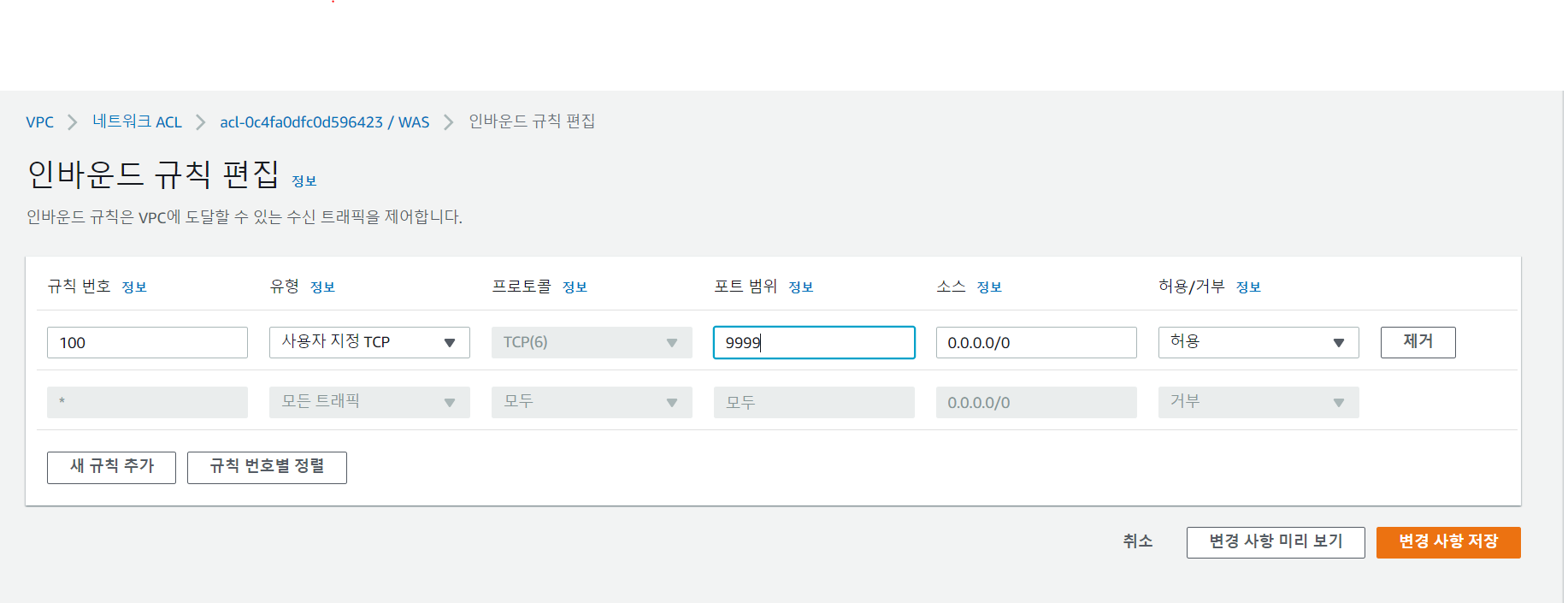


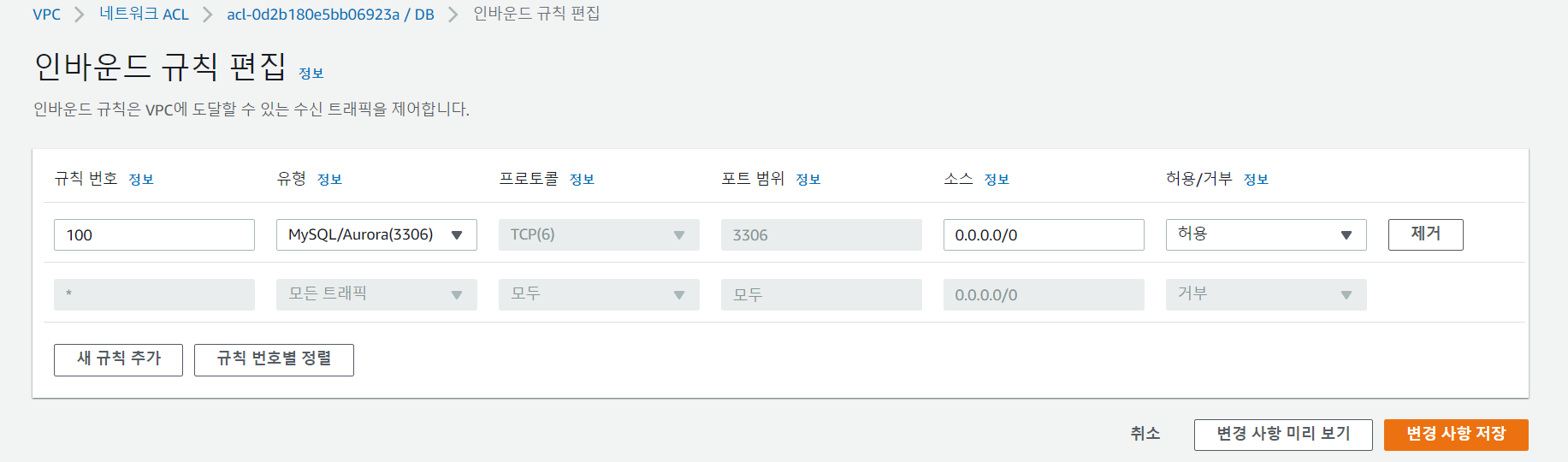
아웃바운드 포트도 마찬가지로 한다. VPC가 3개이기 때문에(서브넷은 5개이지만 Web과 DB에 할당된 서브넷이 두개씩) 이 과정을 3번 반복한다.

## NACL 분리



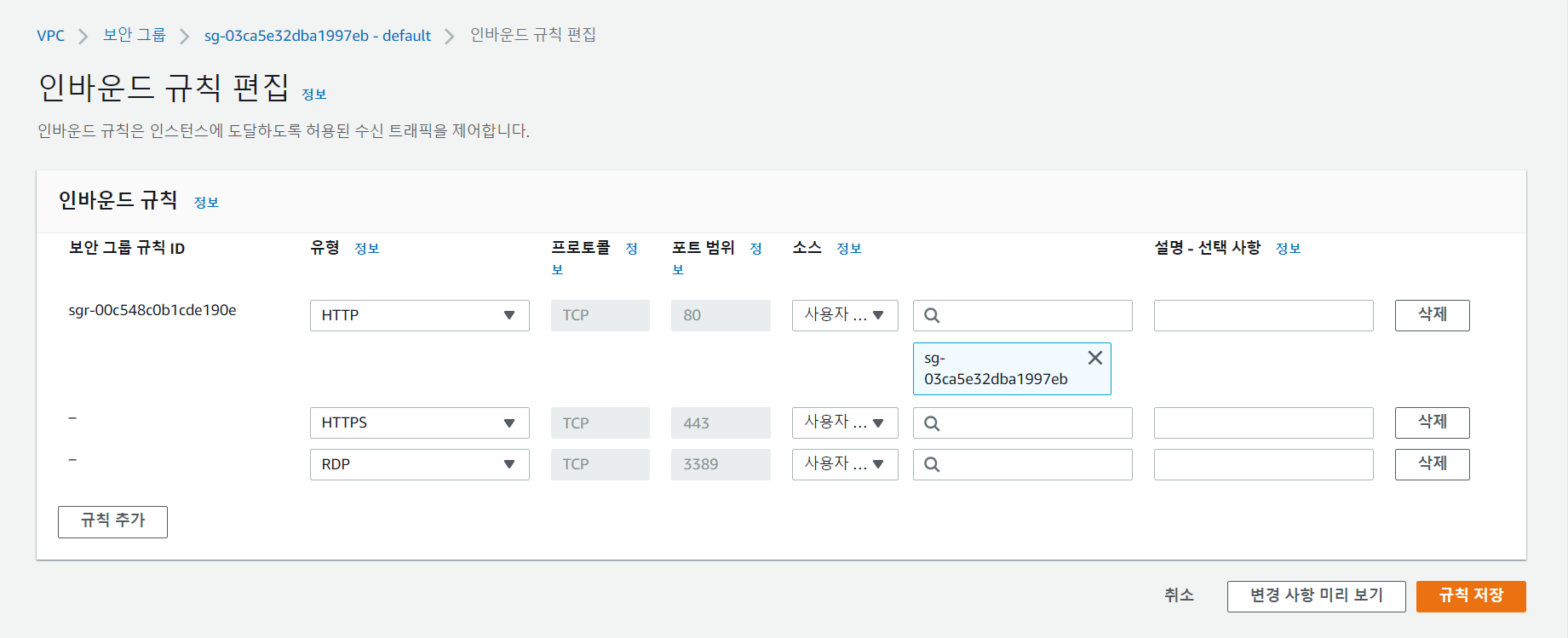
보안을 위해 위에서 했던 NACL을 분리하는 작업을 거쳐야 한다. 각 VPC가 접속해야 할 포트를 연결하고 나머지는 닫는다.





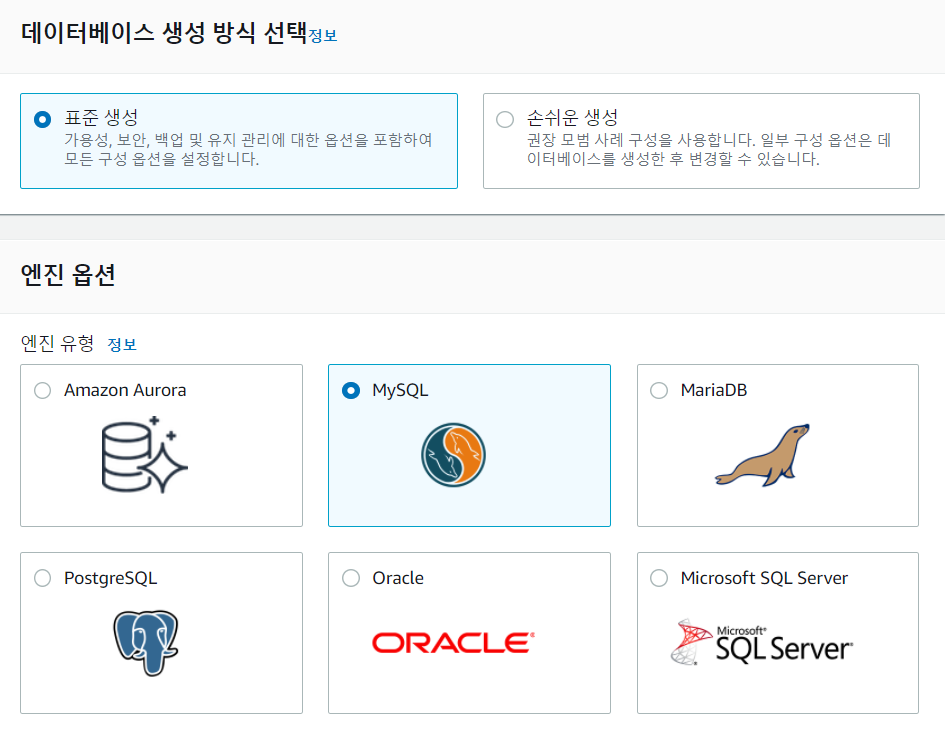
아웃바운드도 같은 방식으로 수정하는데, 이때 웹으로 접속하는 포트를 제외하고는 동적 포트로 빠져나가게 하는 방법으로 하기 위해 모든 트래픽을 열어놓는다.

# 보안 그룹 설정



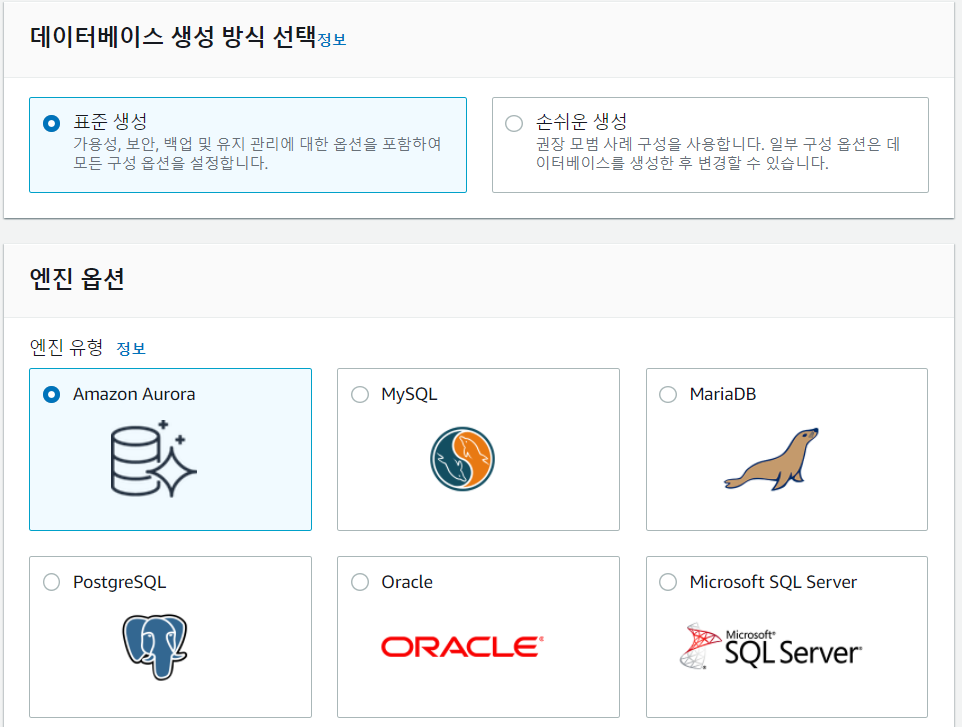
보안 그룹 설정 중 인바운드 편집을 하는 부분이다. NACL 설정과 마찬가지로 하면 된다.

# DB 생성

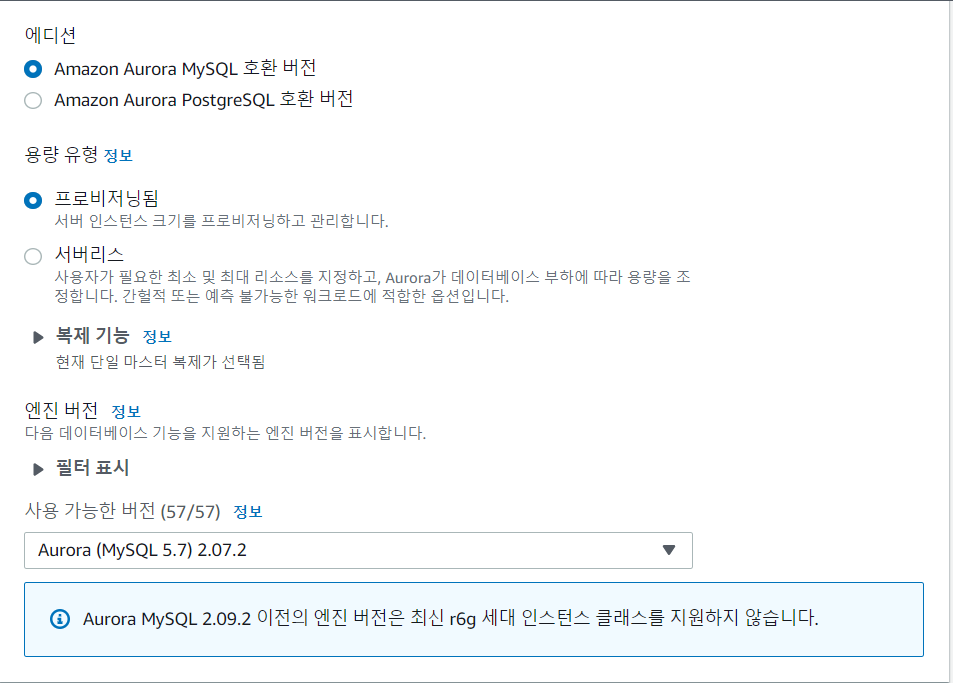


MySQL DB 서비스를 이용하기 위해 RDS 상품을 선택한다. 사용하려는 DB 인스턴스를 선택한 다음 사양에 맞는 제품을 고른다. (실습 상황에서는 최하 프로덕션 제품을 골랐다.) 나머지 값도 사양에 맞게 설정한다.

## Aurora DB를 사용할 때



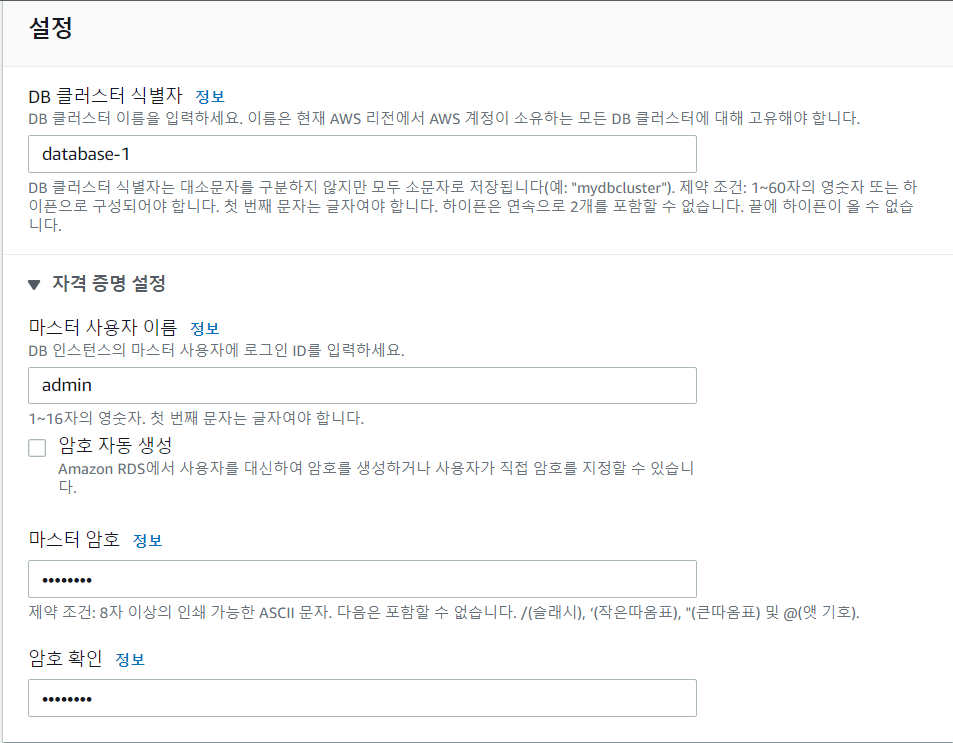
RDS메뉴로 들어가서 데이터베이스 생성 버튼을 누르면 나오는 화면이다. 여기서 Amazon Aurora를 선택한다.



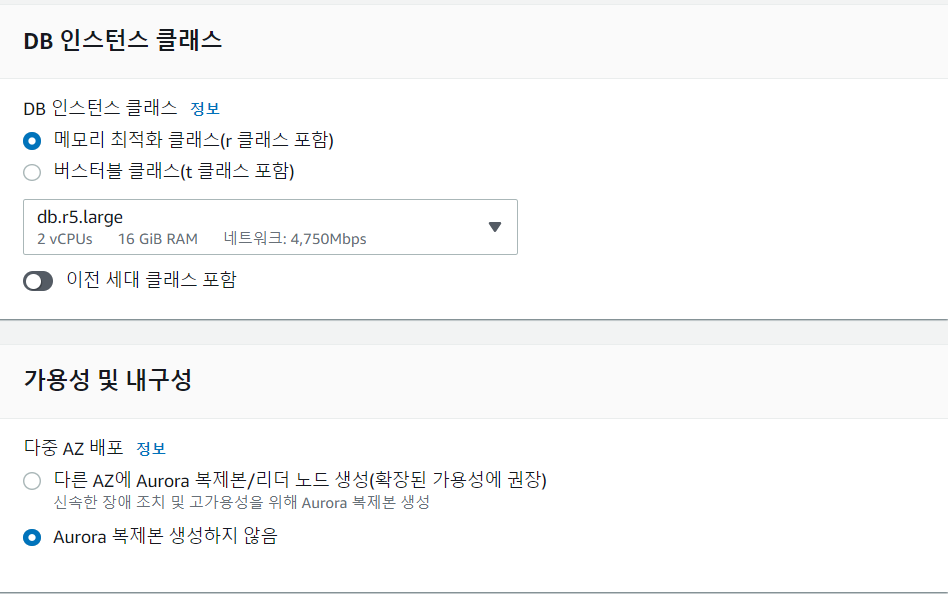
오로라 DB가 호환할 DB의 종류를 선택해야 한다. 위에서 MySQL을 사용하였으므로 MySQL DB 호환 버전을 선택한다. 요구사항에 맞게 호환성을 선택한다. 복제 기능은 클러스터링과 관련 있는데 요구사항에 클러스터링이 있으면 다중 AZ를 선택하면 된다. 여기서는 선택하지 않겠다.



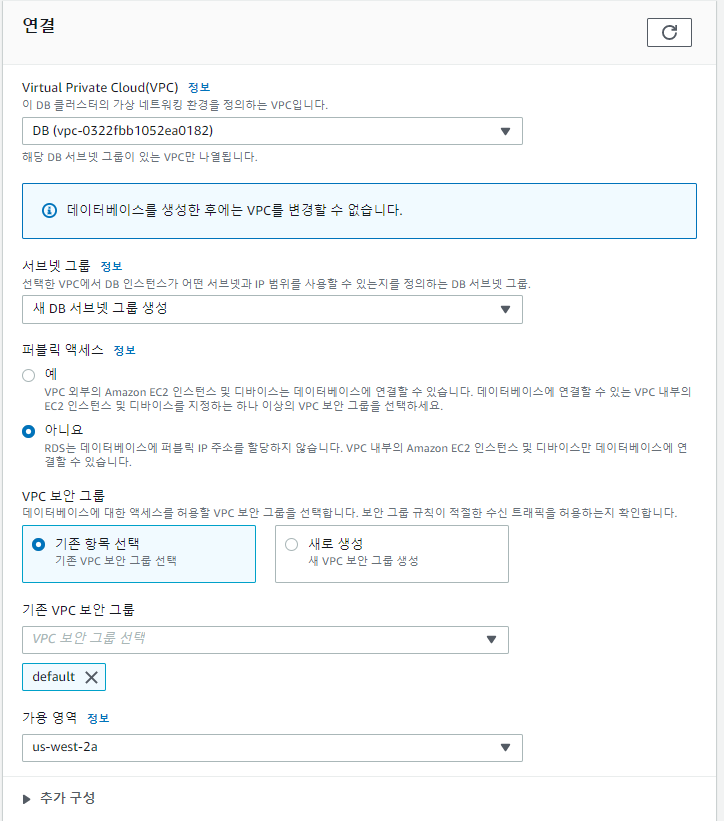
템플릿을 선택하는 화면이다. 프로덕션을 선택한다. 테스트용 DB라면 개발/테스트를 선택해도 된다.



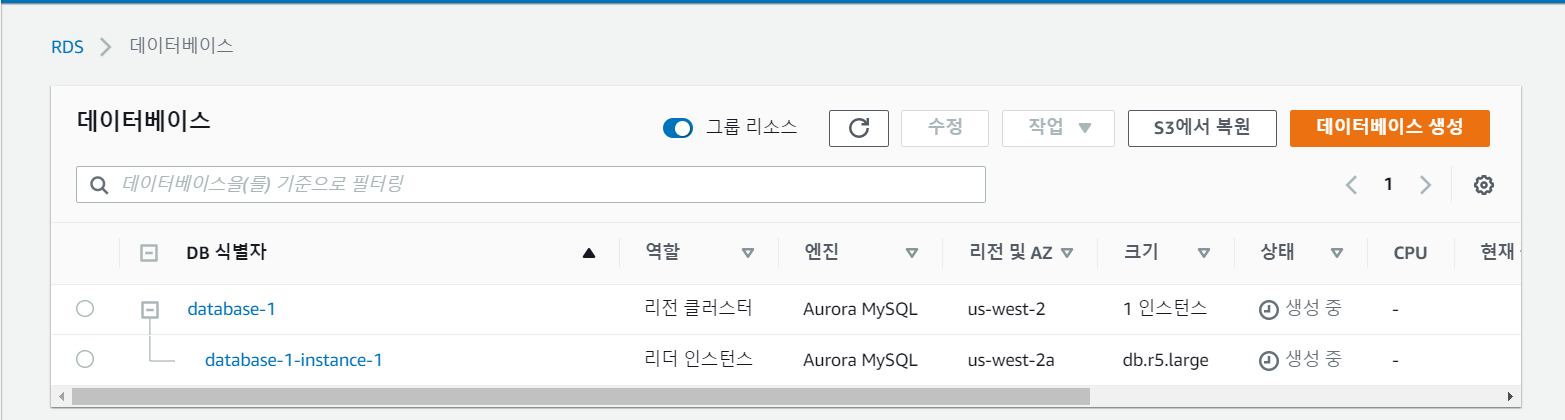
DB에 사용할 암호를 입력한다.



DB 인스턴스와 가용성을 설정하는 화면이다. 최하 상품을 선택하고 클러스터링을 하지 않으므로 복제본 생성하지 않음에 체크한다.



DB 인스턴스에 연결할 VPC를 선택하고 서브넷과 퍼블릭 액세스, 보안 그룹을 설정하는 화면이다. DB에서 제공하는 보안 그룹이 있기 때문에 화면과는 다르지만 새로 생성을 눌러서 보안 그룹을 생성해도 된다. 서브넷은 새로운 DB 서브넷을 생성하는 것이 기본값이므로 이것을 알고 있으면 DB를 연결할 VPC에 서브넷을 따로 만들지 않아도 된다.

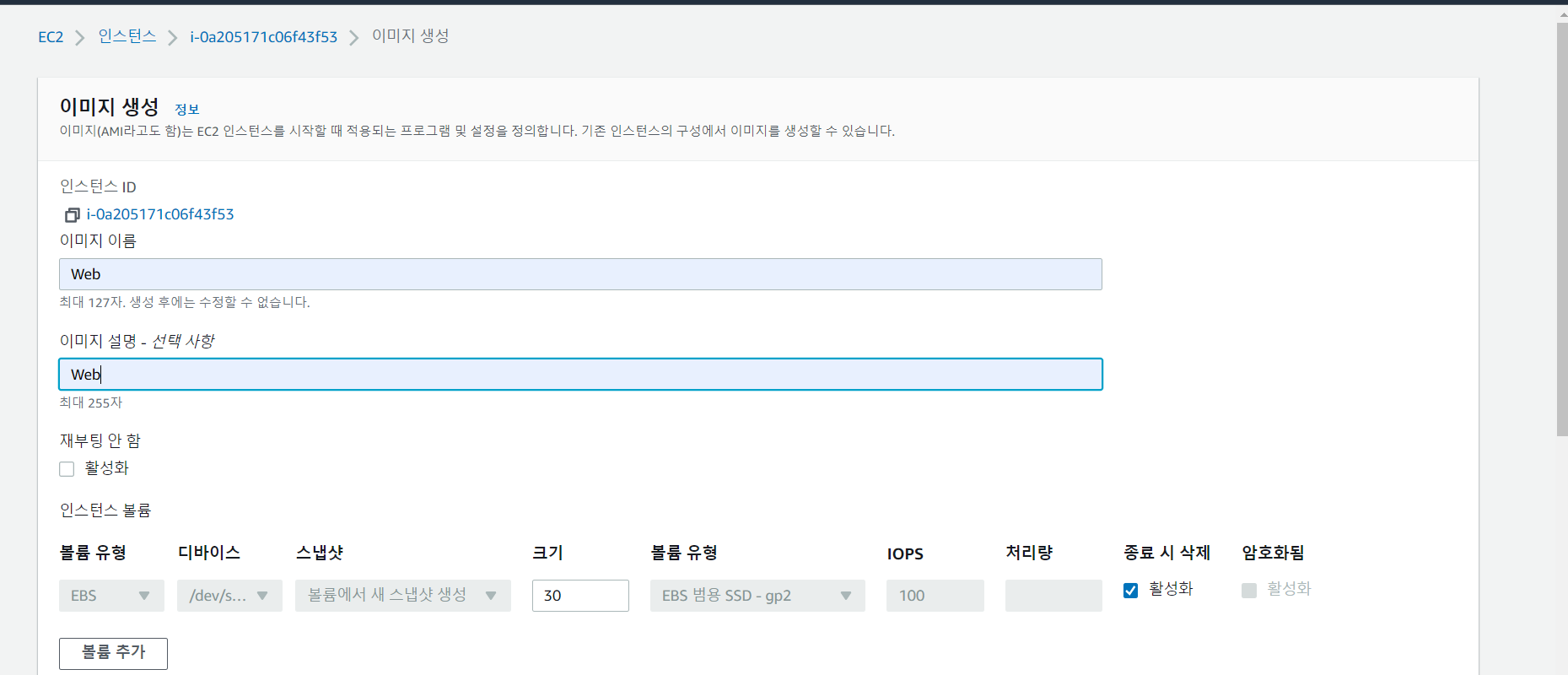


요구사항에 맞게 잘 구성되었는지 확인하고 데이터베이스 생성을 누르면 DB가 생성된다.

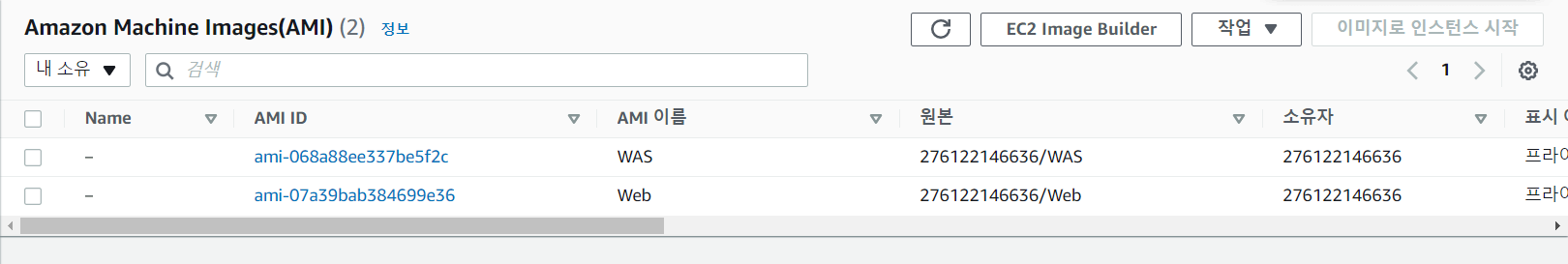
# 인스턴스로 AMI 이미지 만들기



이전에 만들어 둔 인스턴스를 클릭하고 작업 버튼을 누른다. 이미지 및 템플릿에서 이미지 생성을 클릭한다.

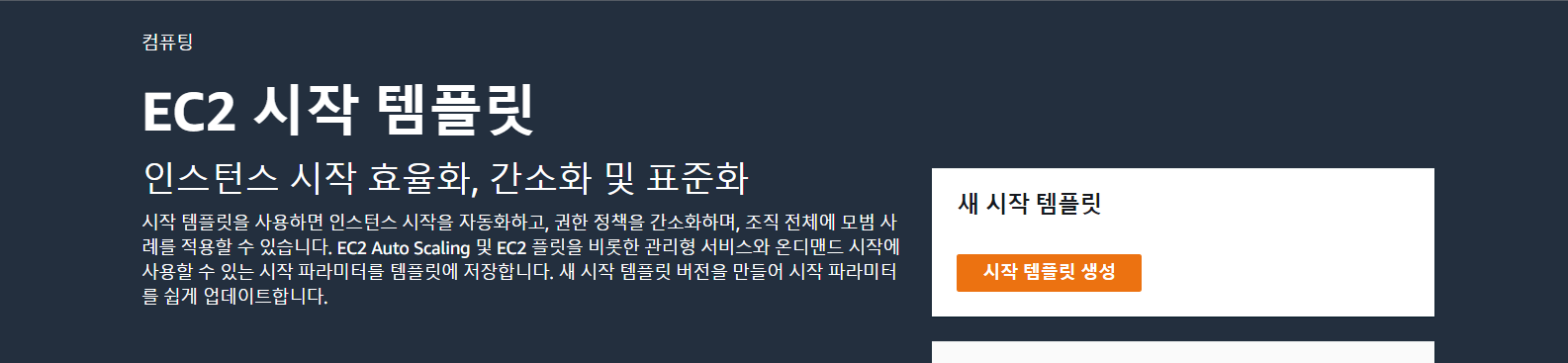


이미지를 생성하는 화면이다. 작업하려는 사항에 맞게 항목들을 기입한다.



이런 식으로 2개를 만든다.

# 시작 템플릿 만들기



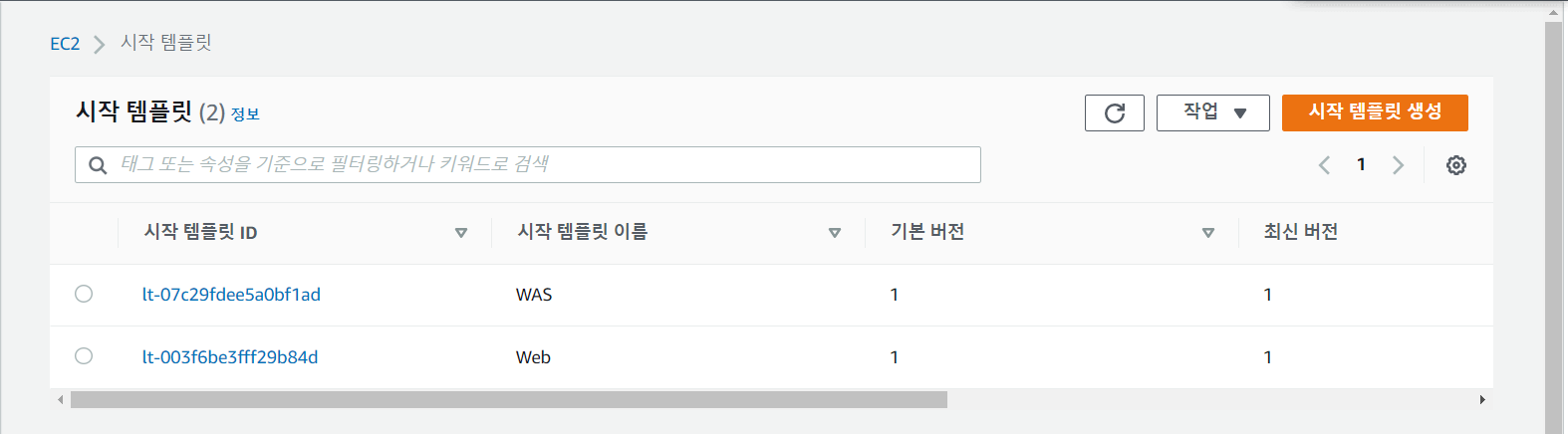
시작 템플릿 시작 화면이다. 시작 템플릿 생성 버튼을 누른다.



사항에 맞게 이름과 설명을 기입한다.

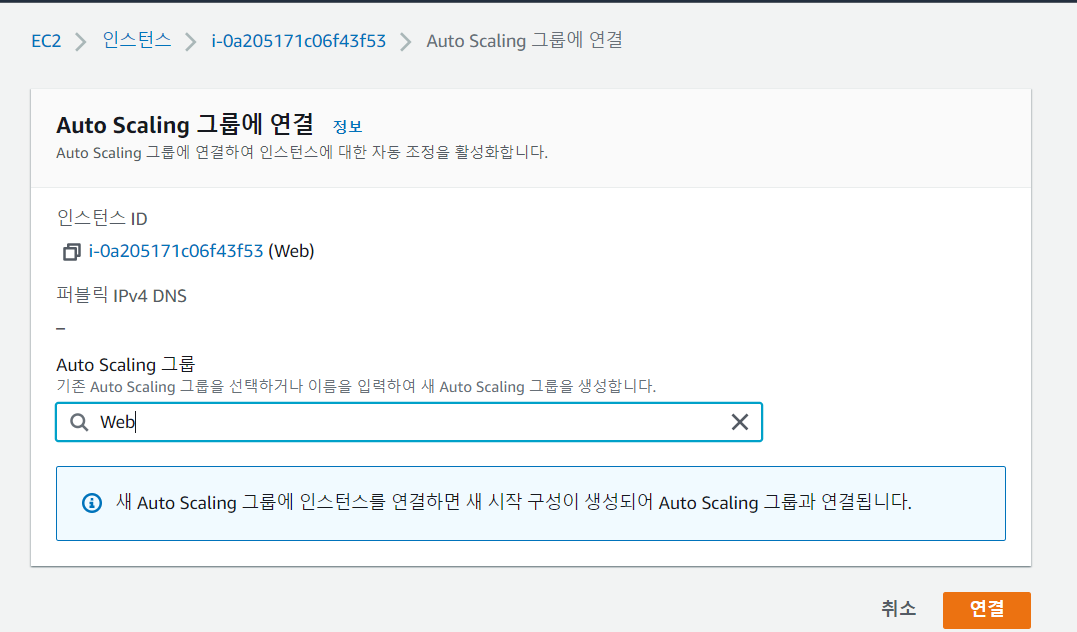


시작 템플릿으로 쓸 머신 이미지와 인스턴스 유형을 선택한다.

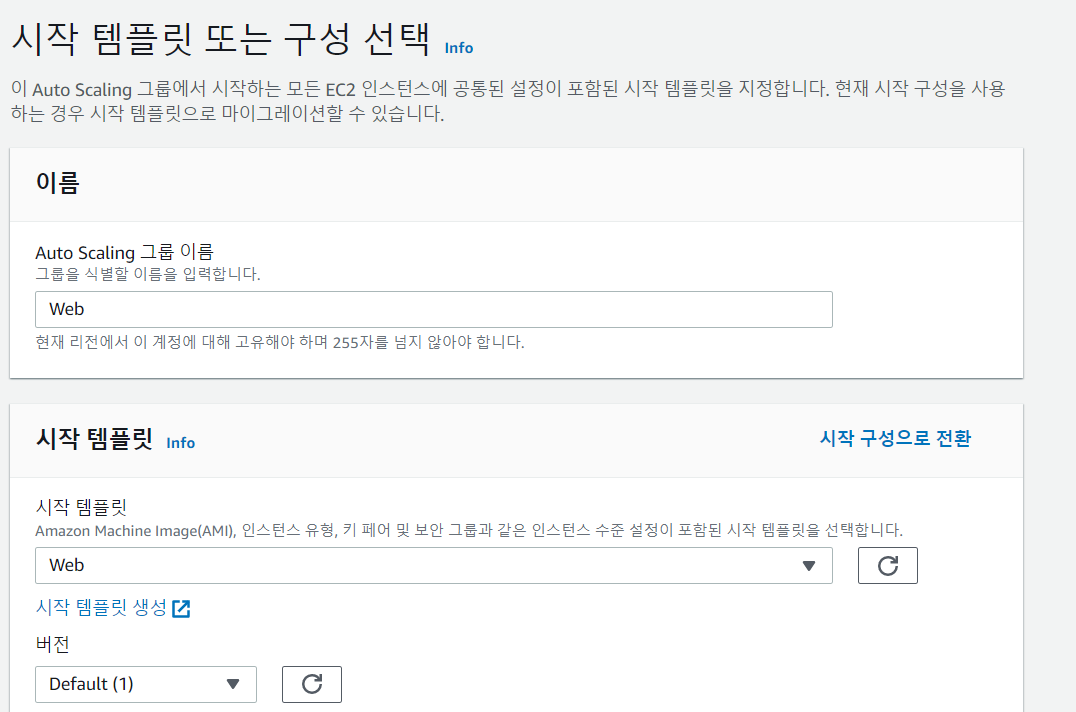


이렇게 2개를 만들면 된다.

# 오토 스케일링



EC2 메뉴의 오토 스케일링 그룹에서 새로 만들어도 되지만 이번에는 인스턴스에서 오토 스케일링 그룹을 새로 만들고 거기에 연결하는 방식으로 해 보았다.

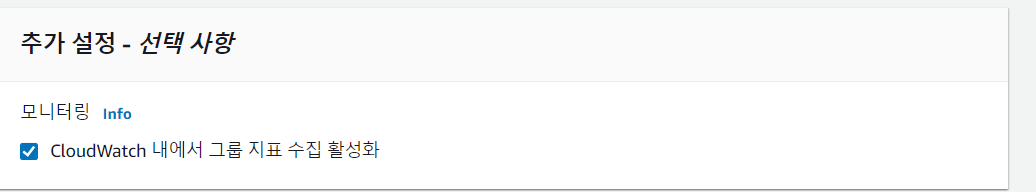


기존의 방식대로 하려면 EC2메뉴에서 오토 스케일링 그룹 메뉴를 눌러 오토 스케일링 그룹을 생성하면 된다.

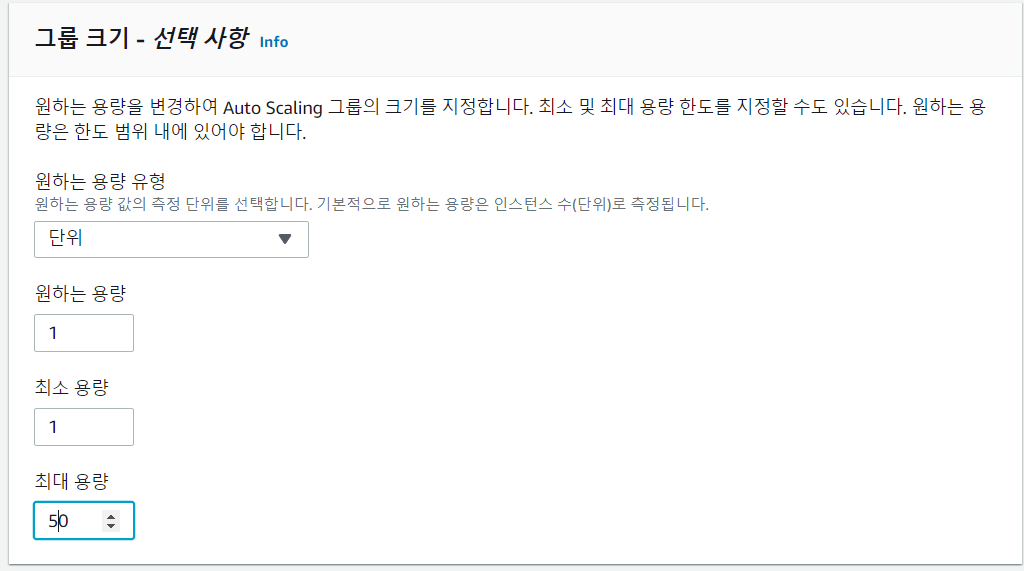




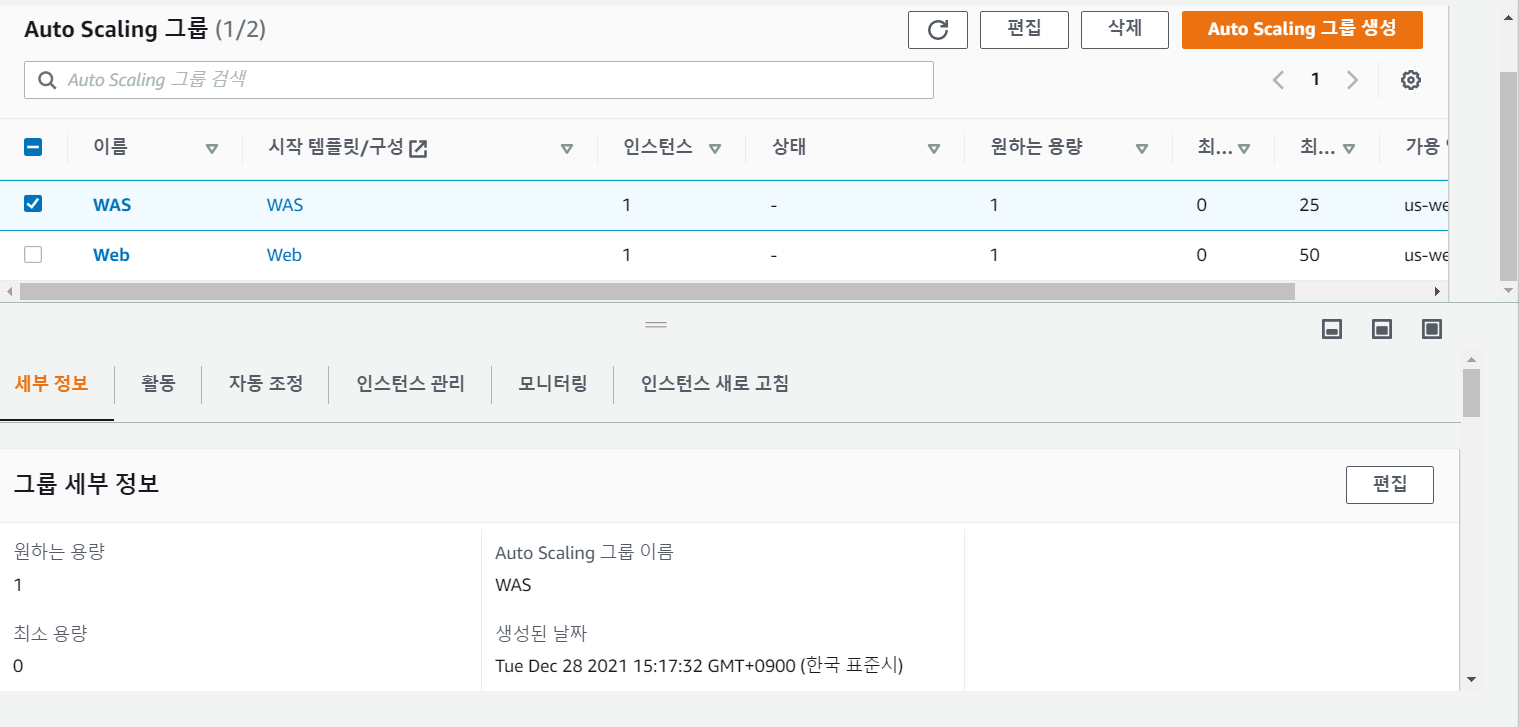
로드 밸런서는 나중에 만들 것이기 때문에 없음으로 설정한다.



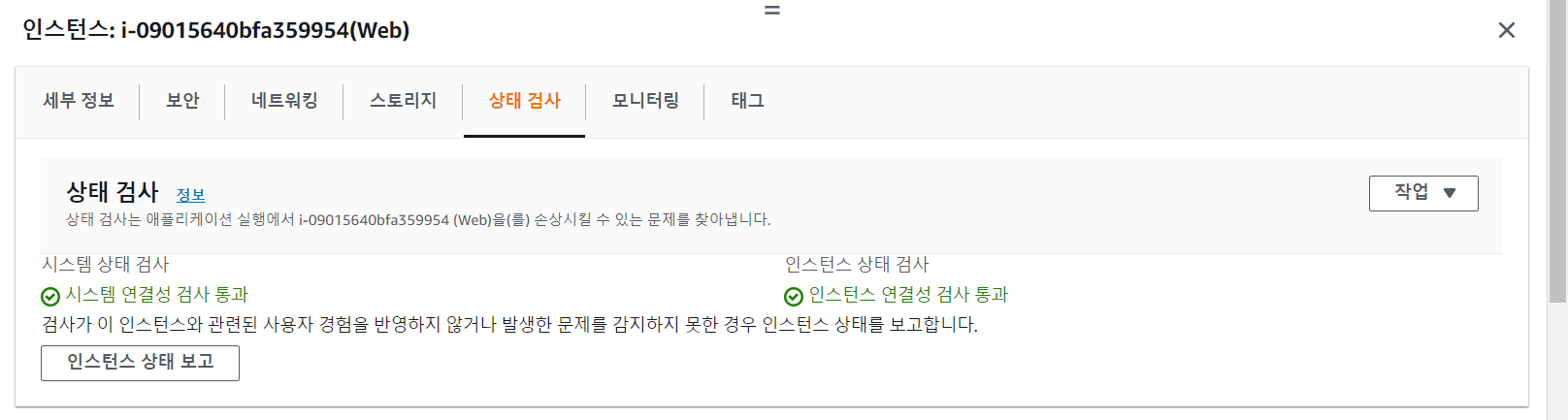
모니터링을 편하게 하기 위해 클라우드워치 내 그룹 지표 수집 활성화를 켠다.

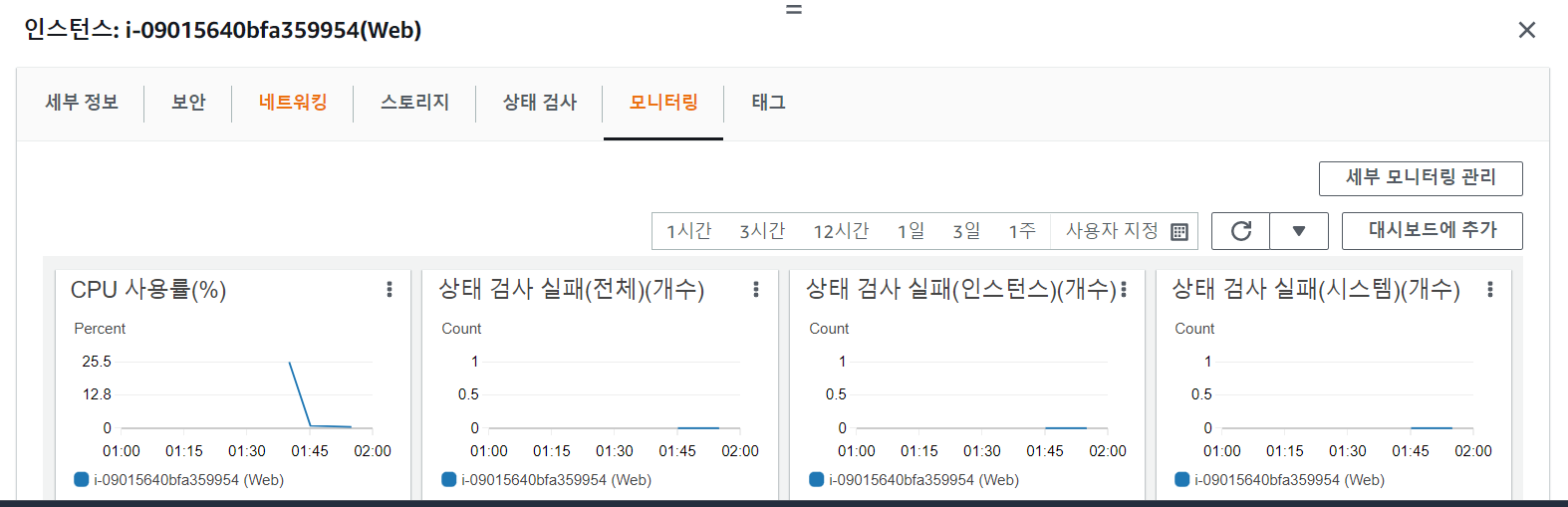


늘려야 하는 인스턴스 개수를 최대 용량으로 설정한다.



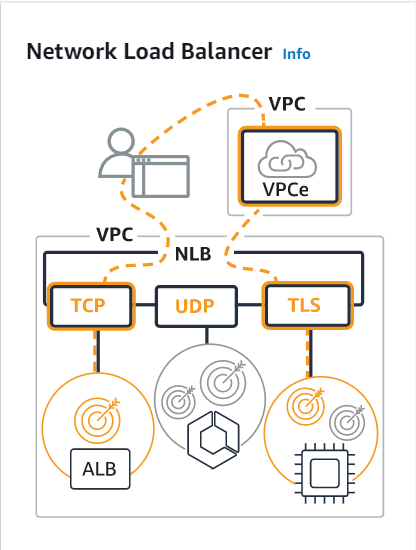
이렇게 오토 스케일링 그룹을 만들면 된다.



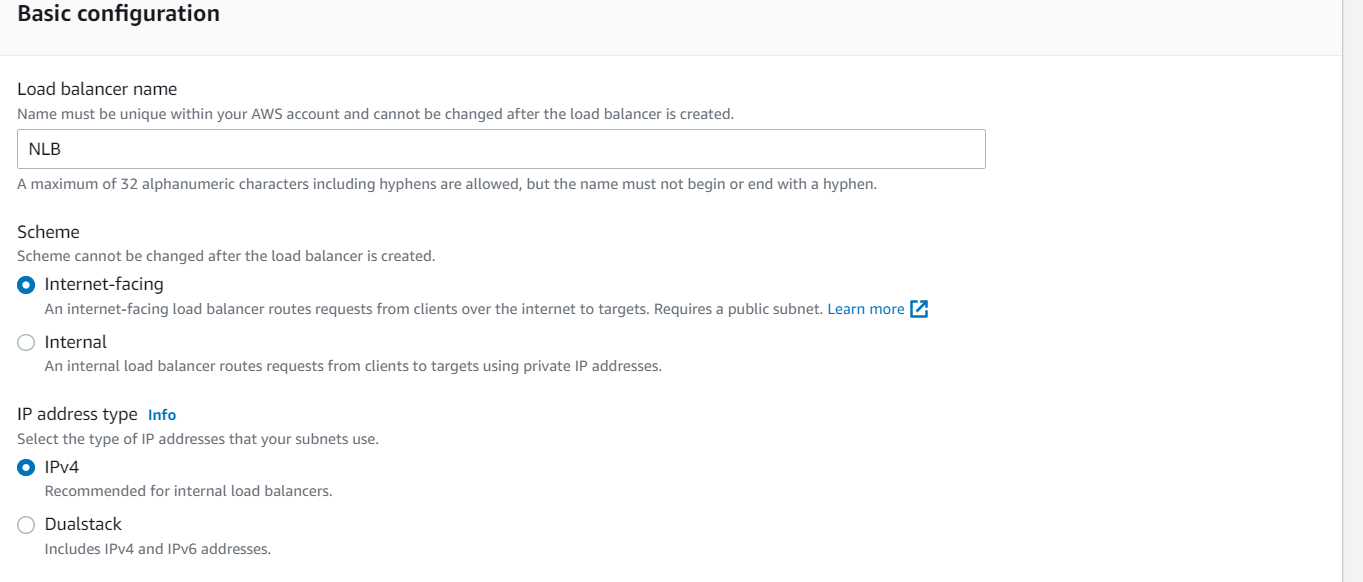


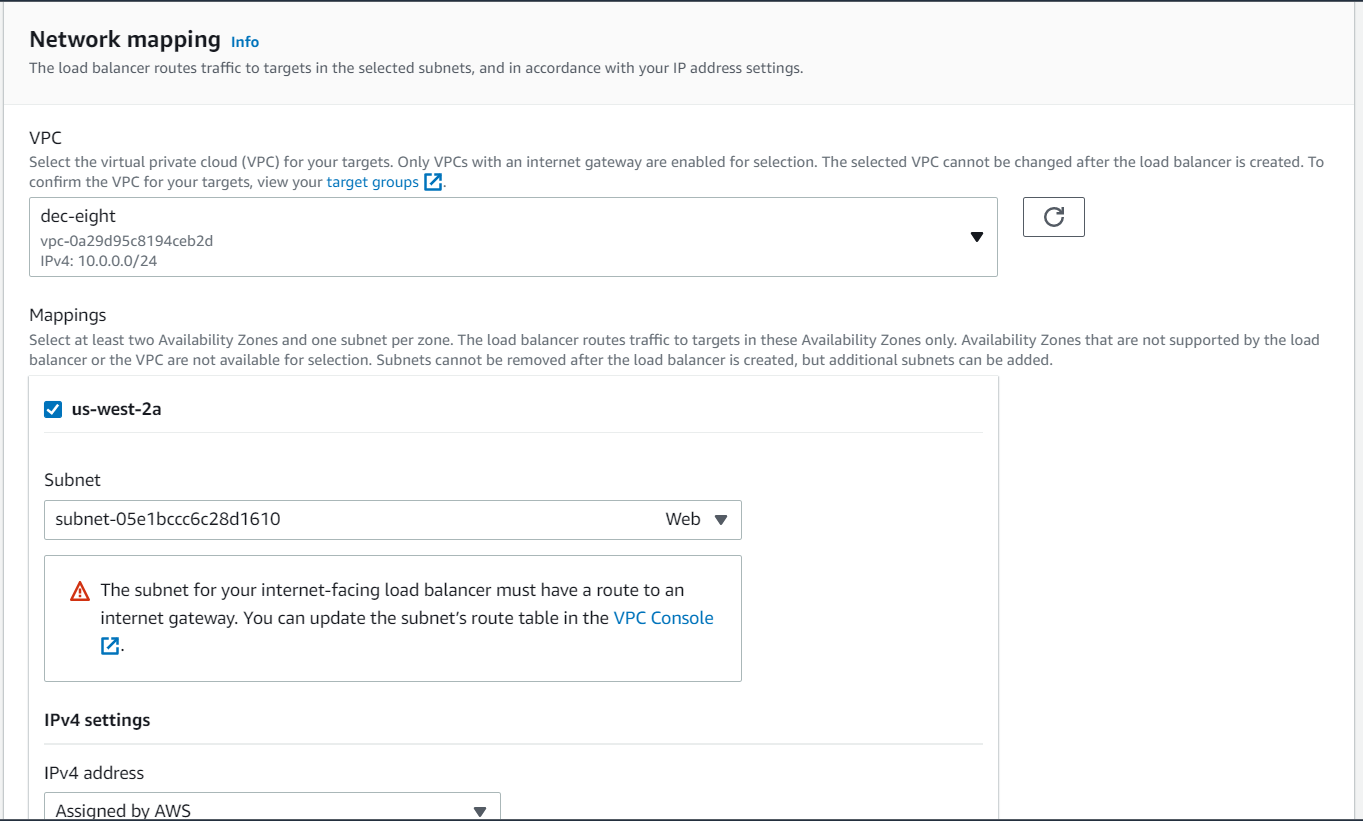
인스턴스 메뉴로 돌아가면 상태 검사와 모니터링을 통해 오토 스케일링이 잘 돌아가고 있는지 확인할 수 있다.

# NLB

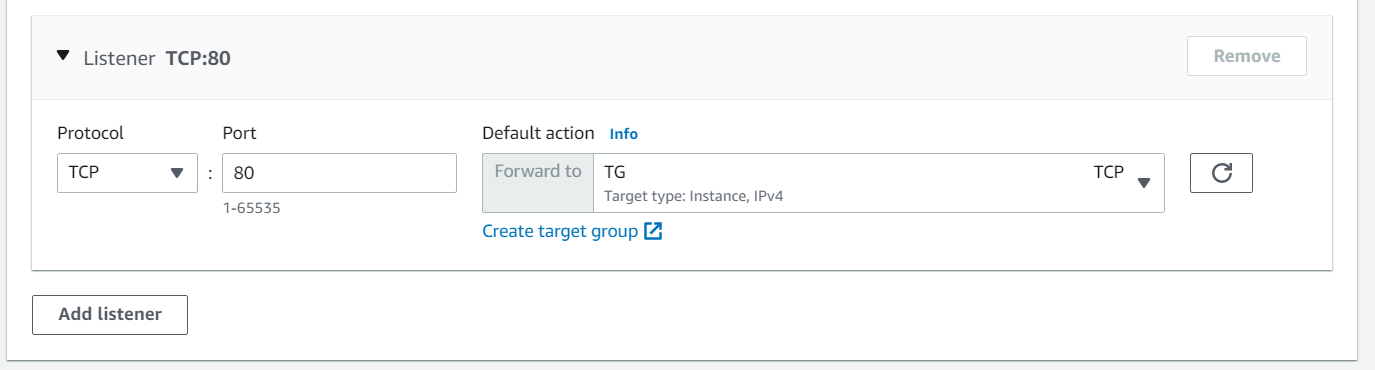


로드 밸런서 생성 메뉴에서 NLB를 선택한다.

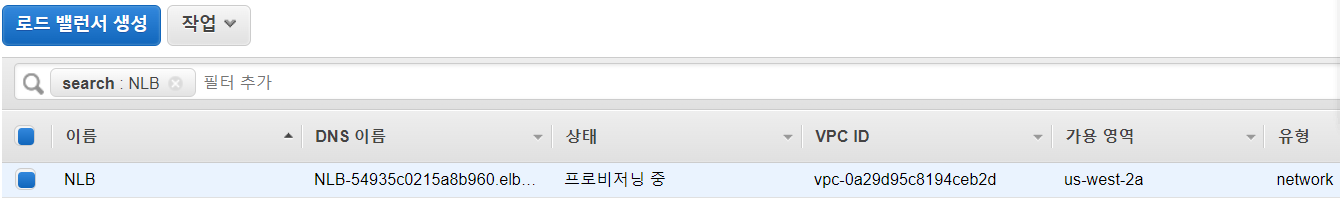




매핑할 VPC와 서브넷을 선택한다.

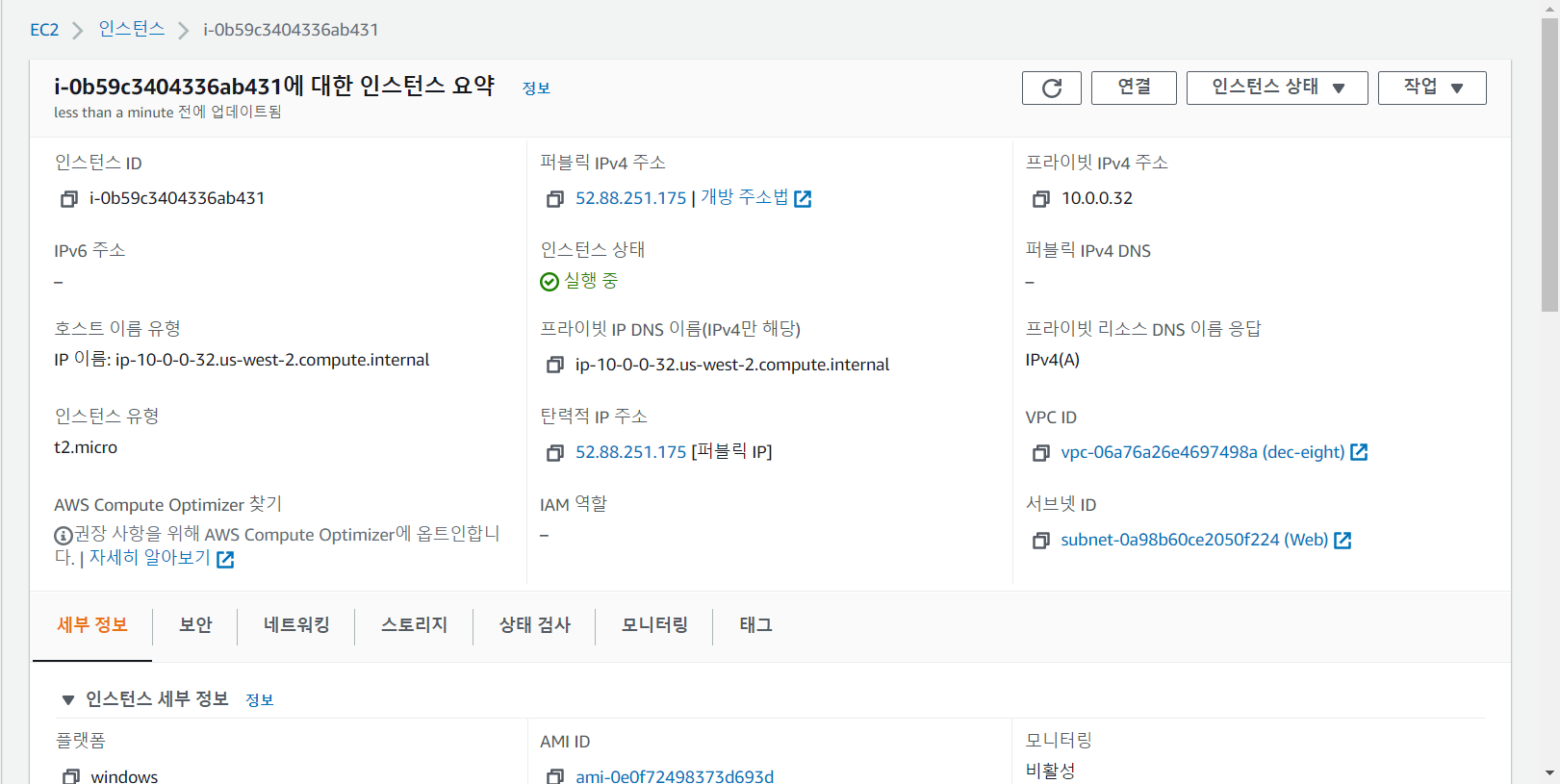


연결할 포트를 선택하고 대상 그룹을 지정한다. 대상 그룹이 없다면 아래 Create Target Group을 눌러 만들고 재설정할 수 있다.

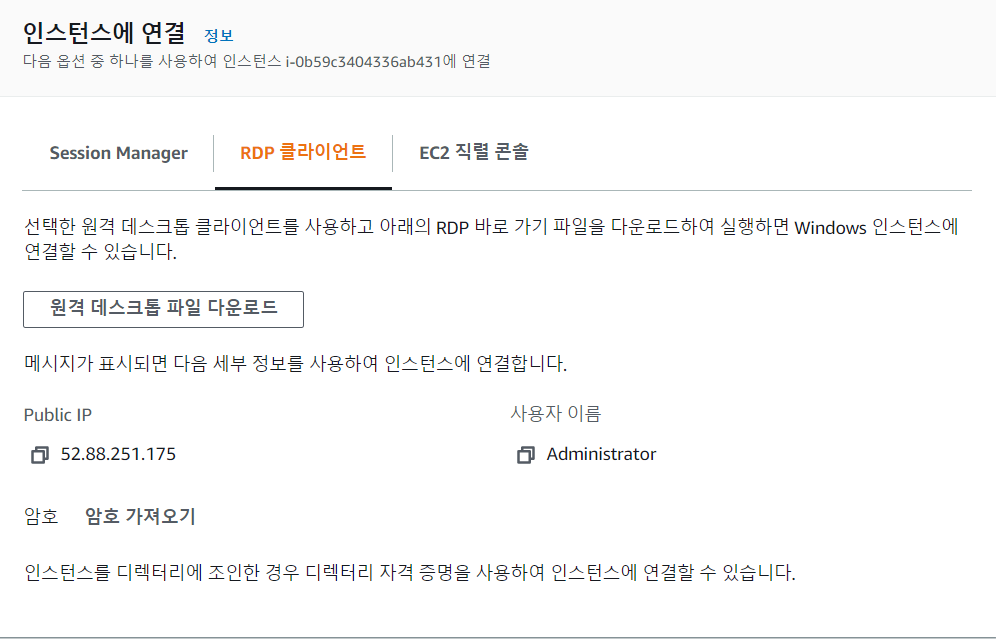


이렇게 로드밸런서가 만들어진 모습이다.

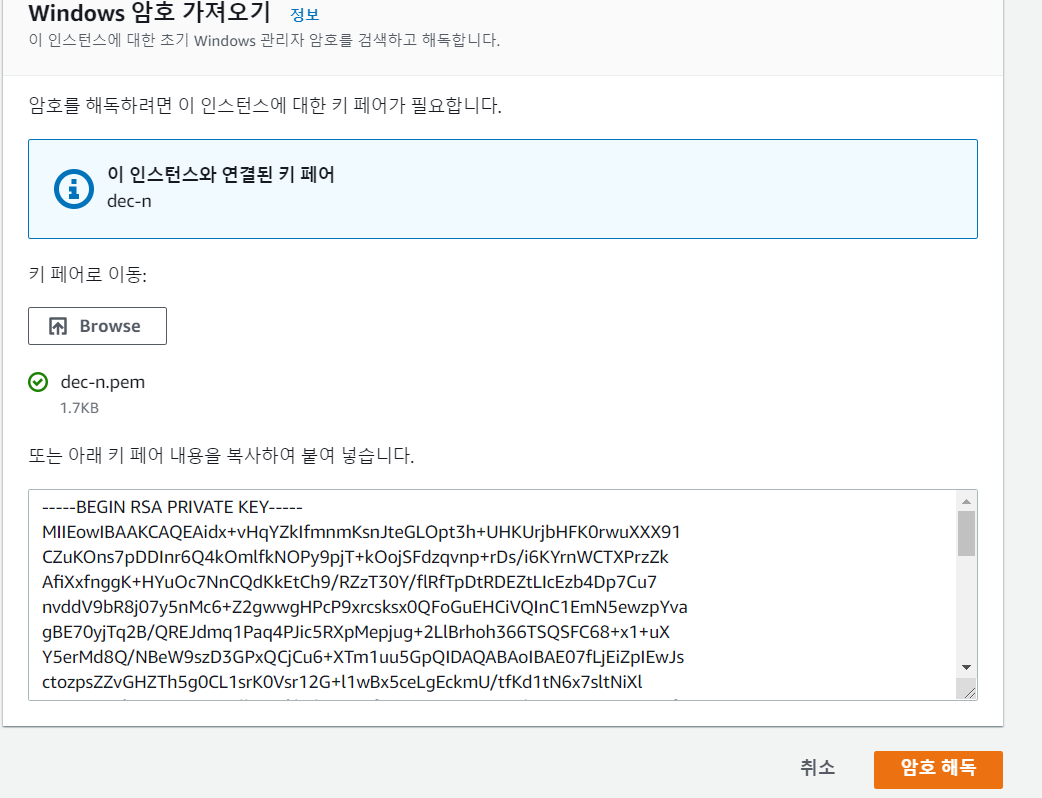
# Windows 원격 접속 연결(시도)



인스턴스 연결 메뉴를 클릭한다.



RDP 클라이언트를 선택하고 암호 가져오기를 클릭한다.

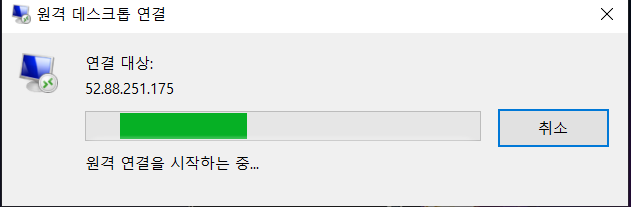


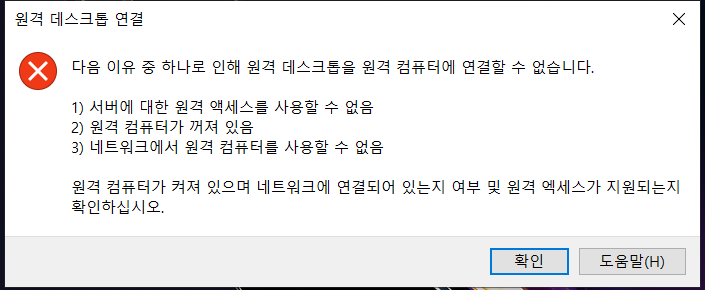
Browse버튼을 눌러 다운로드 받은 키페어를 선택하면 암호 해독을 누른다.

그러면 암호가 나타난다. 아까의 인스턴스 연결화면에서 원격 데스크톱 파일을 다운로드 받는다.

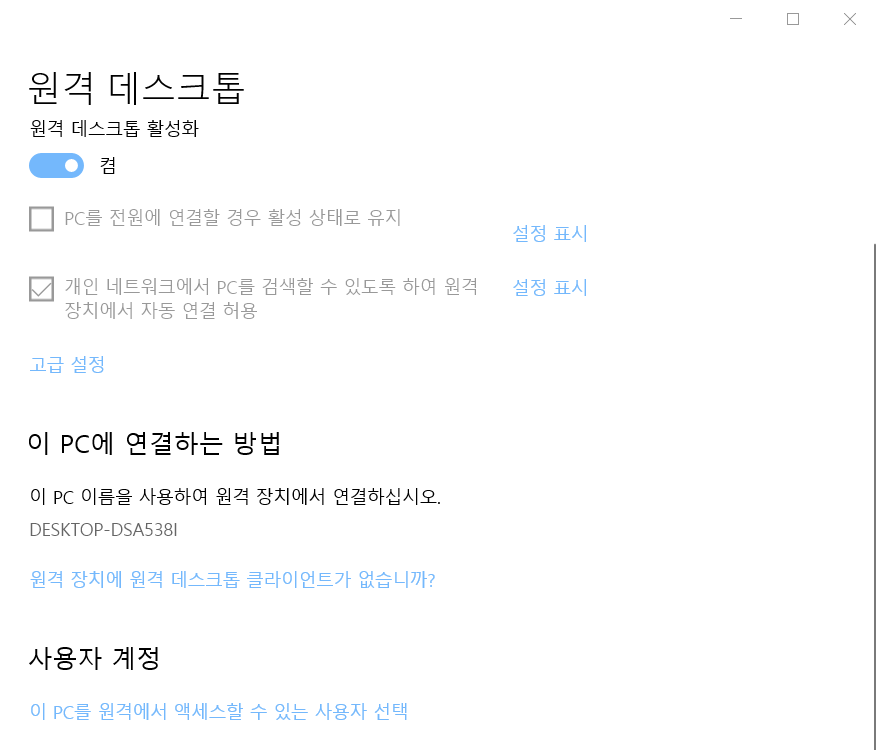


더블클릭한다.

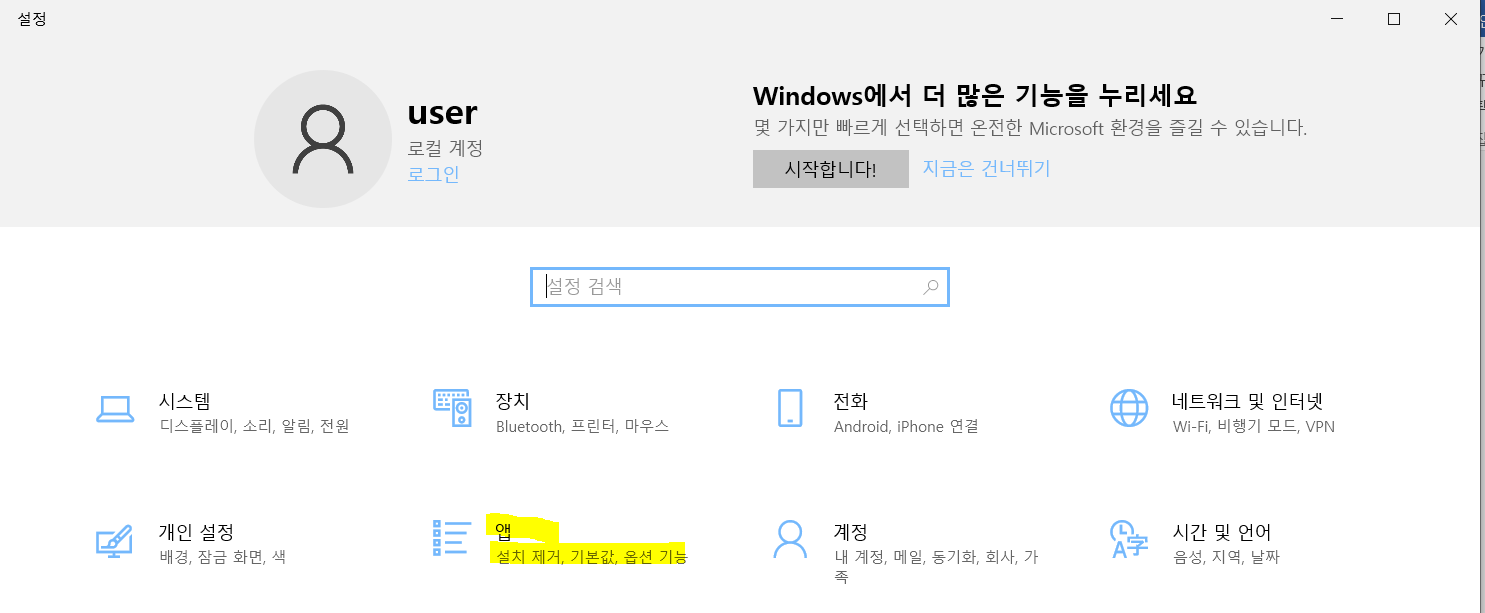




원격 데스크톱을 연결할 수 없다는 창이 떴다. 원격 데스크톱 사용은 활성화 되어 있는 상태이다.



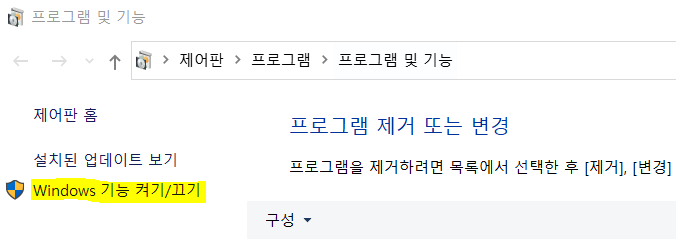
## Windows Server IIS 설치



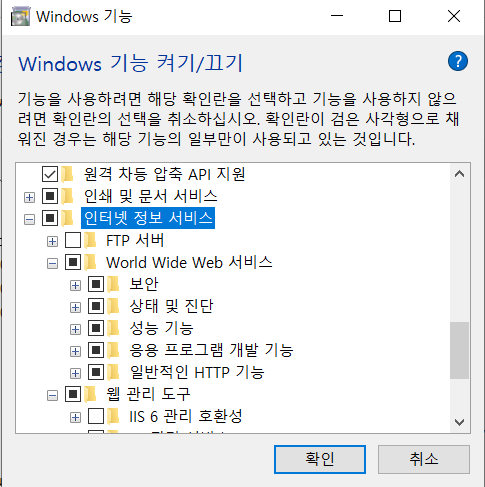
시작 메뉴에서 설정(톱니바퀴 모양 아이콘)을 누르면 설정 창이 뜬다. 여기서 앱으로 들어간다.



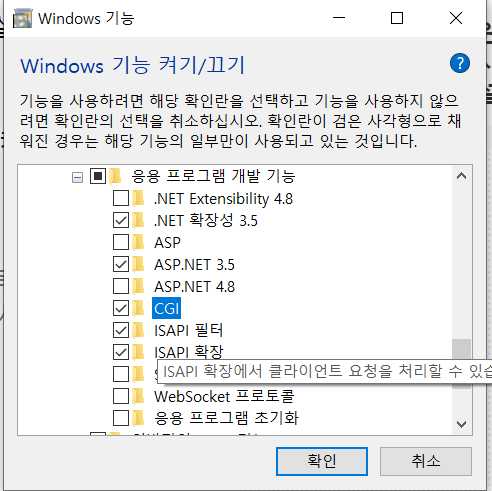
앱 및 기능 창이 뜬다. 여기서 프로그램 및 기능을 클릭한다. (형광펜으로 표시한 곳을 클릭하면 된다.)



프로그램 및 기능 창에서 Windows 기능 켜기/끄기를 누른다.

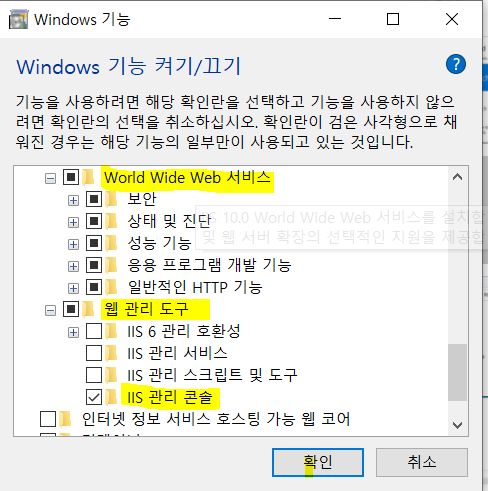


기능 창에서 인터넷 정보 서비스를 클릭한 다음 응용 프로그램 개발 기능에서

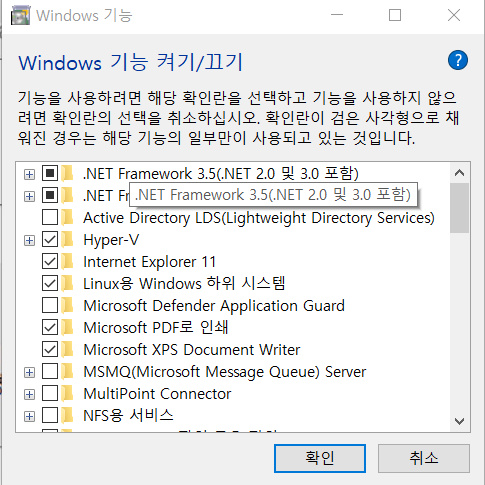


하위 메뉴들 중 .NET 확장성 4.8/3.5(둘 중 하나만 선택), ASP.NET3.5/4.8(역시 둘 중 하나만 선택)

, CGI, ISAPI 확장 메뉴를 클릭한다.



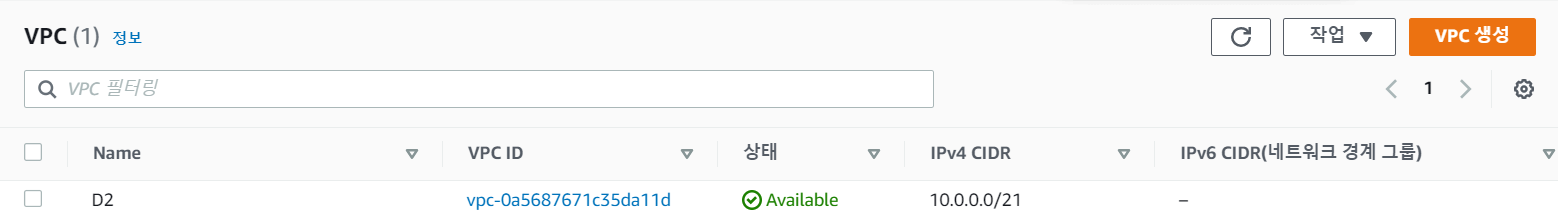
WWW서비스에서는 웹 관리 도구의 IIS 관리 콘솔만 선택한다.

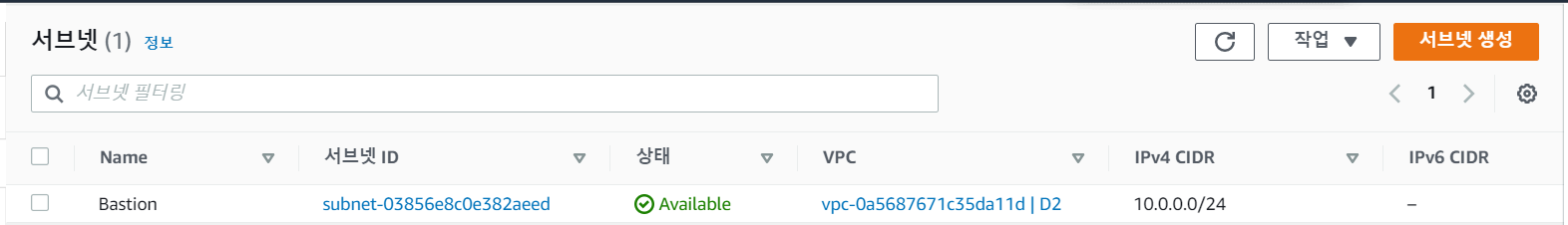


그리고 .NET Framework 3.5를 선택하고 확인을 눌러 설치를 한다. 보통은 재부팅할 필요가 없다고 하는데 일부 컴퓨터에서는 이러한 설정들을 변경하면 컴퓨터를 재부팅해야 한다고 할 수 있으니 그럴 땐 재부팅하면 된다.

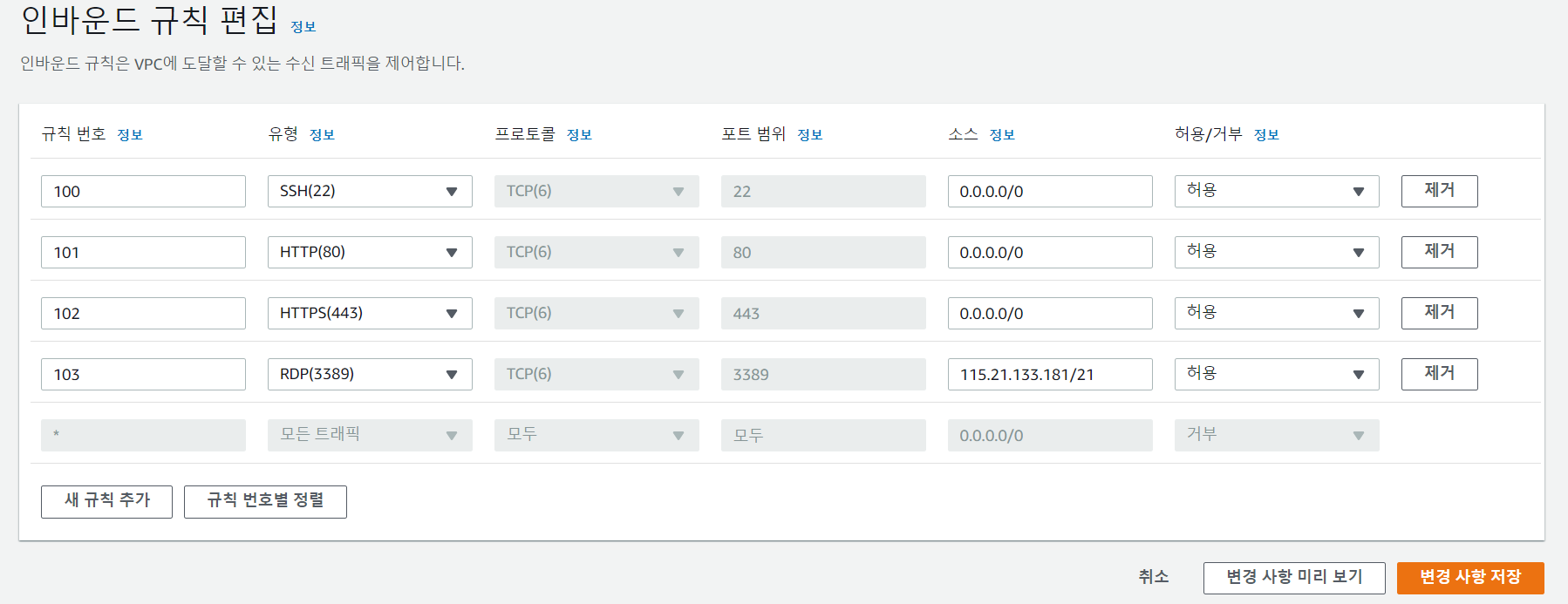
# Bastion Host 설정

## NACL & 보안 그룹 설정

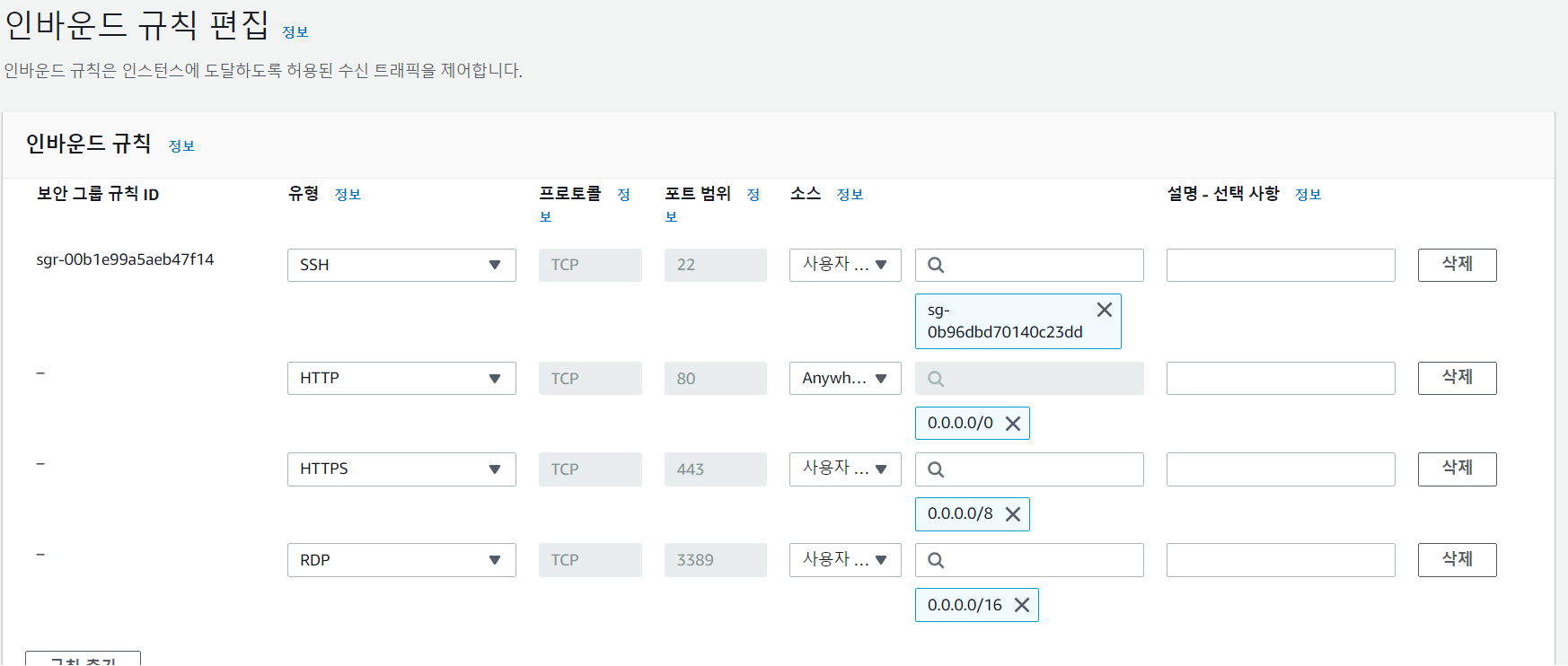


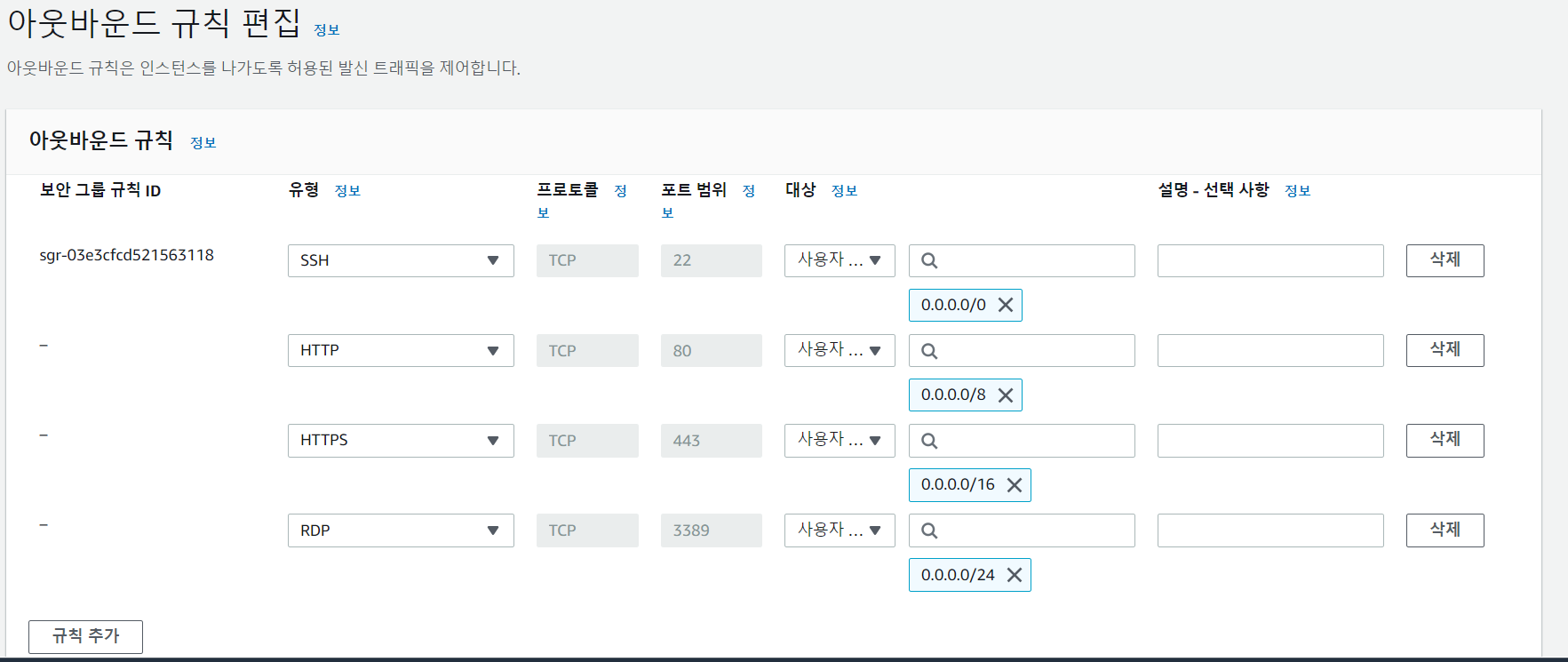


Bastion Host용 VPC와 서브넷을 만들어 둔다.



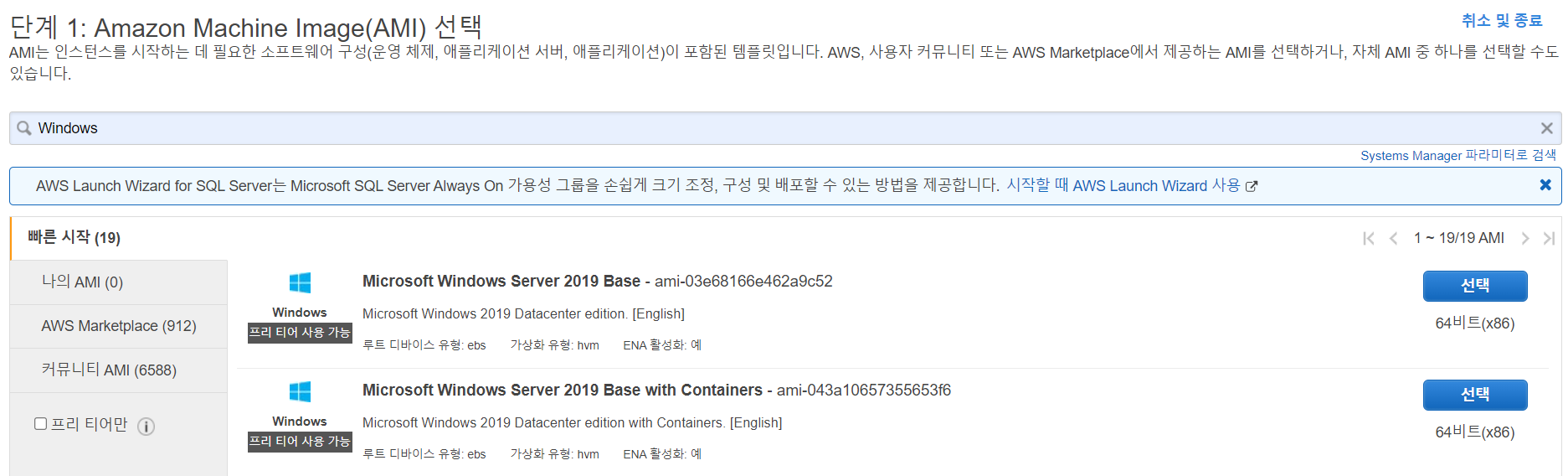
NACL 인바운드 규칙 편집화면이다. 22번 포트로 모든 서브넷을 연결해야 하기 때문에 가장 먼저 열어둘 포트로 22번을 지정한다. Windows Server는 HTTP/HTTPS로 통신하므로 80/443포트도 열어놓는다. 마지막으로 Bastion Host에서 붙을 3389번 포트를 열어두고 소스에 접속할 IP주소를 입력한다. (위에 있는 IP주소는 예시로 넣은 주소이다.) 아웃바운드 규칙도 같은 방법으로 수정한다.



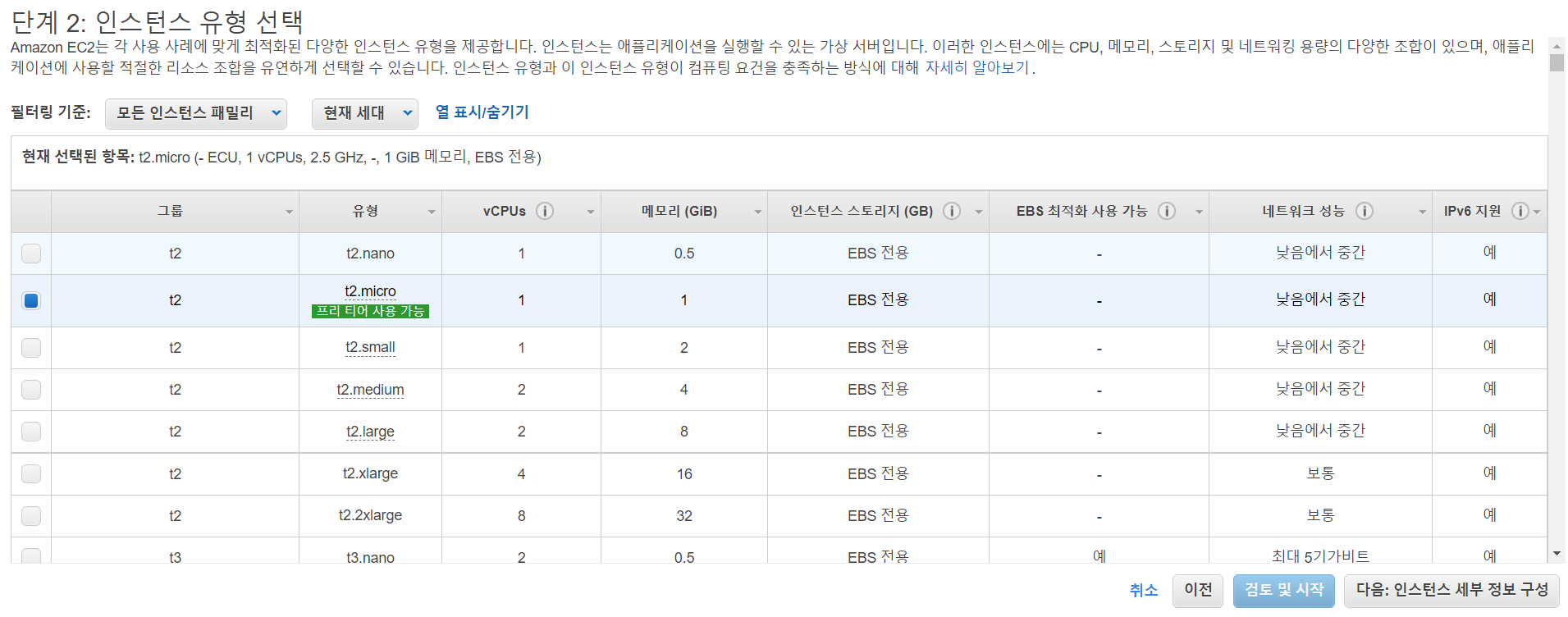


보안 그룹 인바운드/아웃바운드 규칙 편집 화면이다. 요구사항에 맞게 유형을 선택하고 소스에 사항에 있는 포트번호를 넣는다. (위에 있는 포트는 예시이다.)

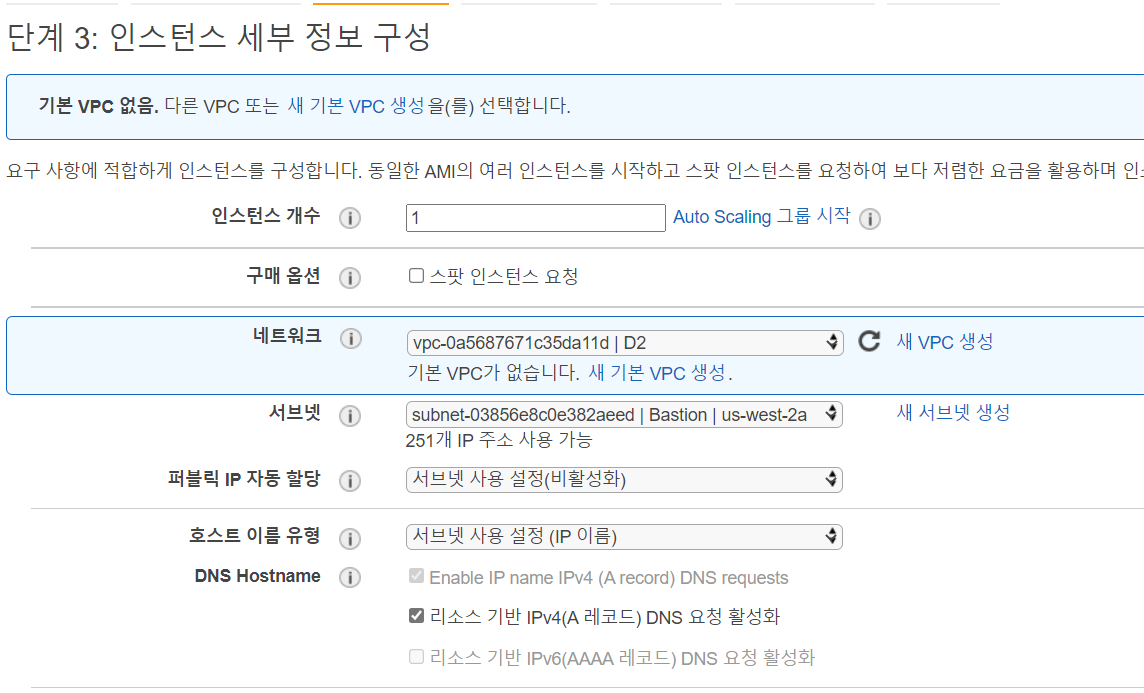
## Windows Server용 인스턴스 생성



인스턴스 메뉴에서 인스턴스 생성을 누르면 AMI를 선택할 수 있는 화면이다. Windows Server를 설치하기 위해 검색 창에 넣으면 관련 상품들이 나온다. 요구사항에 맞게 프리 티어를 선택한다.



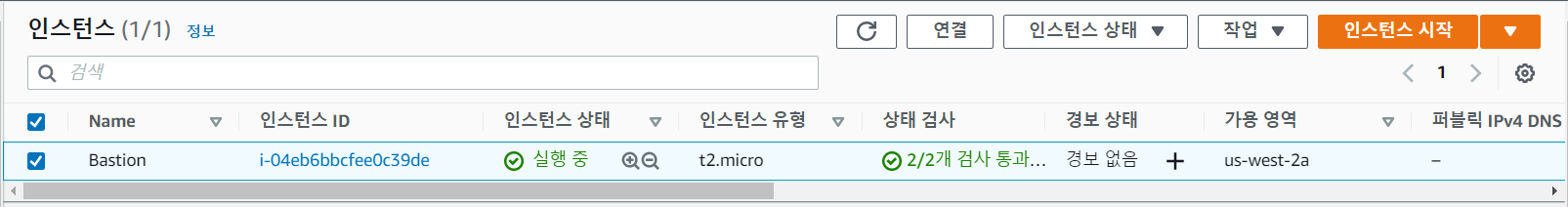
인스턴스 유형도 역시 프리 티어를 선택한다.



VPC와 서브넷 연결을 확인한다. 확인을 누르면 스토리지 용량 항목이 있는데 기본값으로 둔다.



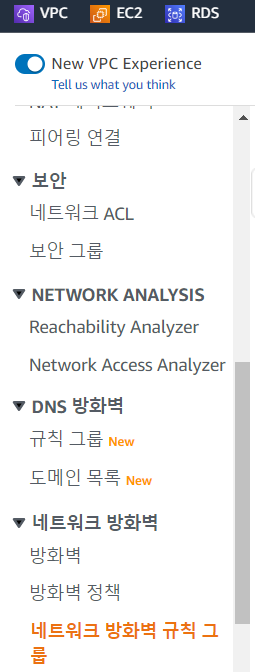
태그를 달고 보안 그룹을 설정할 때 앞에서 설정한 보안 그룹을 선택한다. 다음 화면은 검토화면이므로 사항에 맞게 인스턴스가 잘 구성되었는지 확인하면 된다.



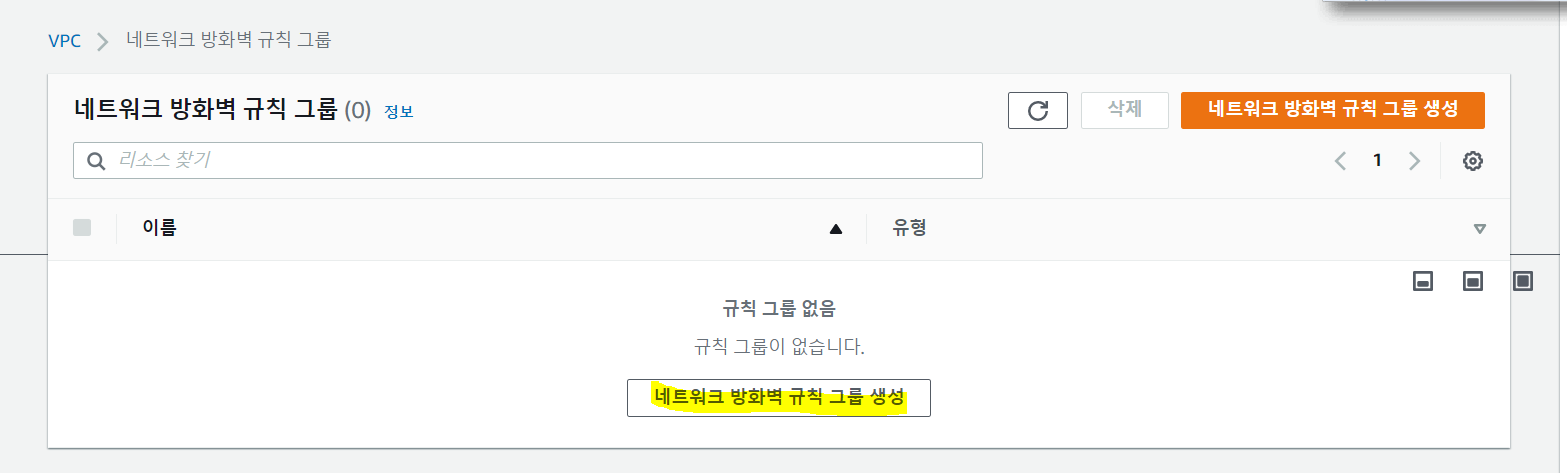
Windows Server용 인스턴스가 생성된 모습이다.

# 방화벽 생성

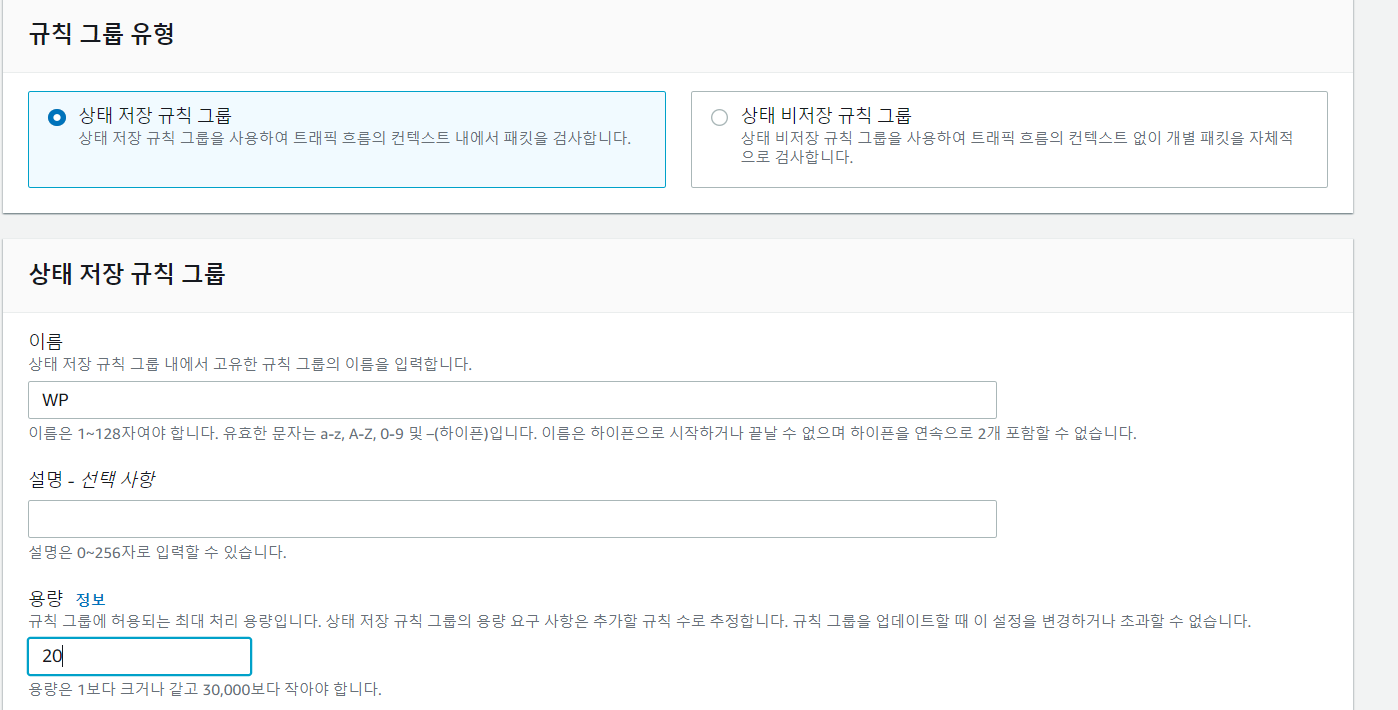
## 네트워크 규칙 그룹 생성



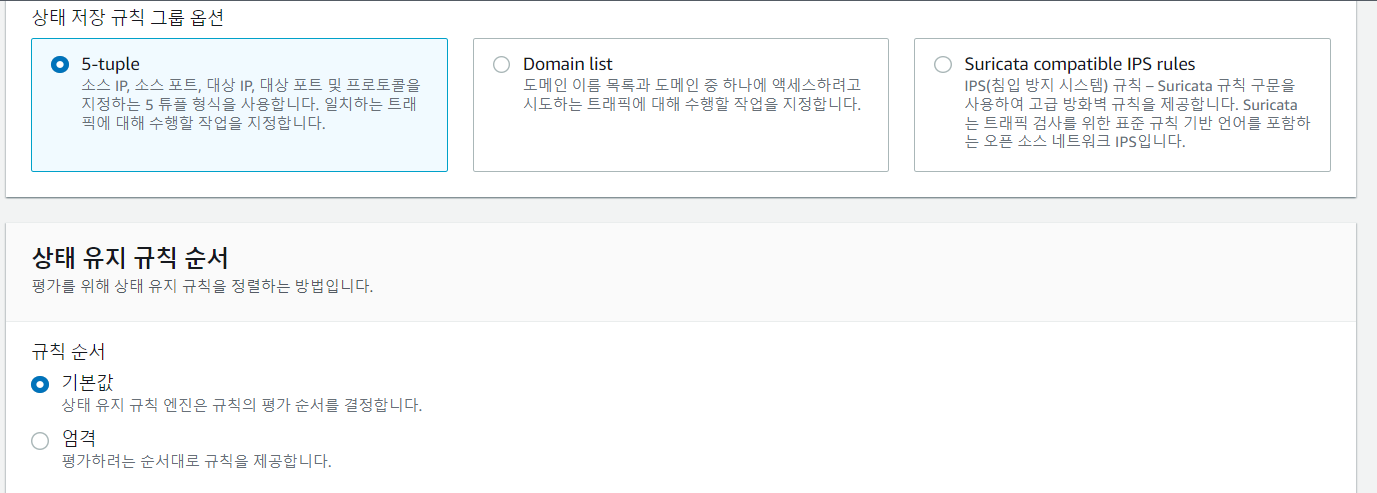
StateFull 방식으로 방화벽을 만드는 과정을 설명한다. 우선 VPC 메뉴에서 네트워크 방화벽 메뉴 안의 네트워크 방화벽 규칙 그룹으로 들어간다.



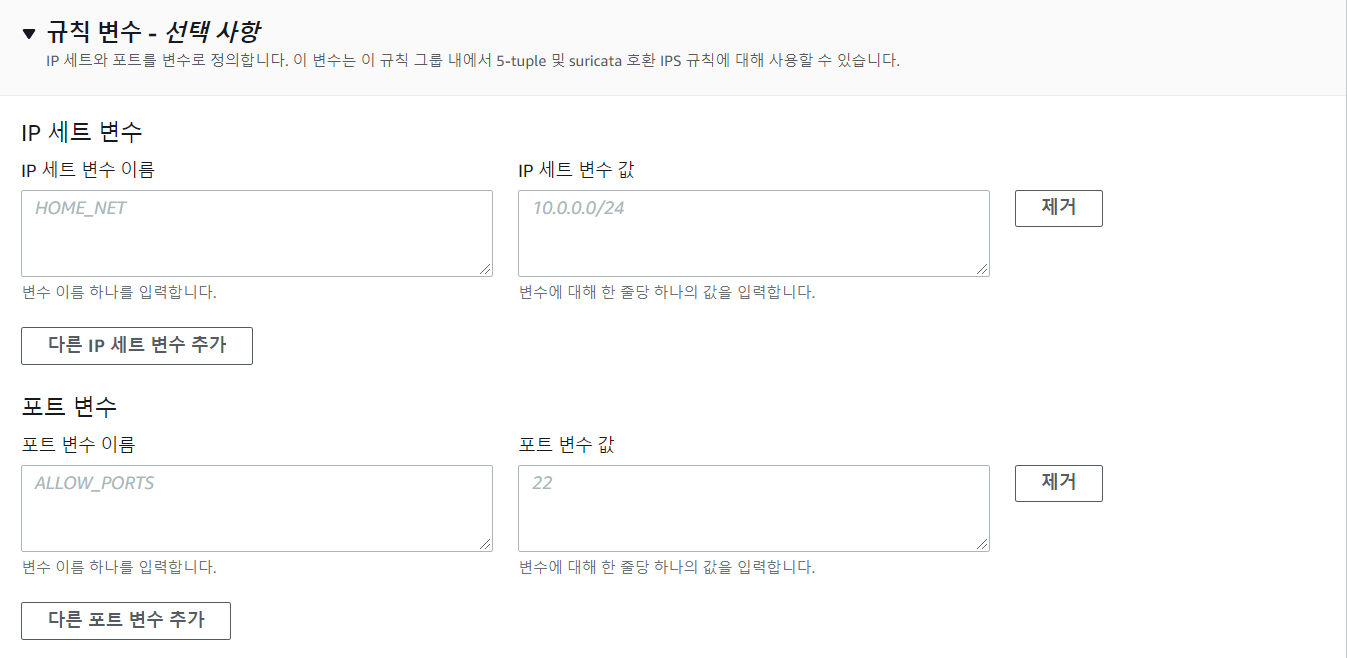
위의 주황색 버튼이나 형광펜으로 칠한 버튼을 누르면 네트워크 방화벽 규칙 그룹을 생성할 수 있다.

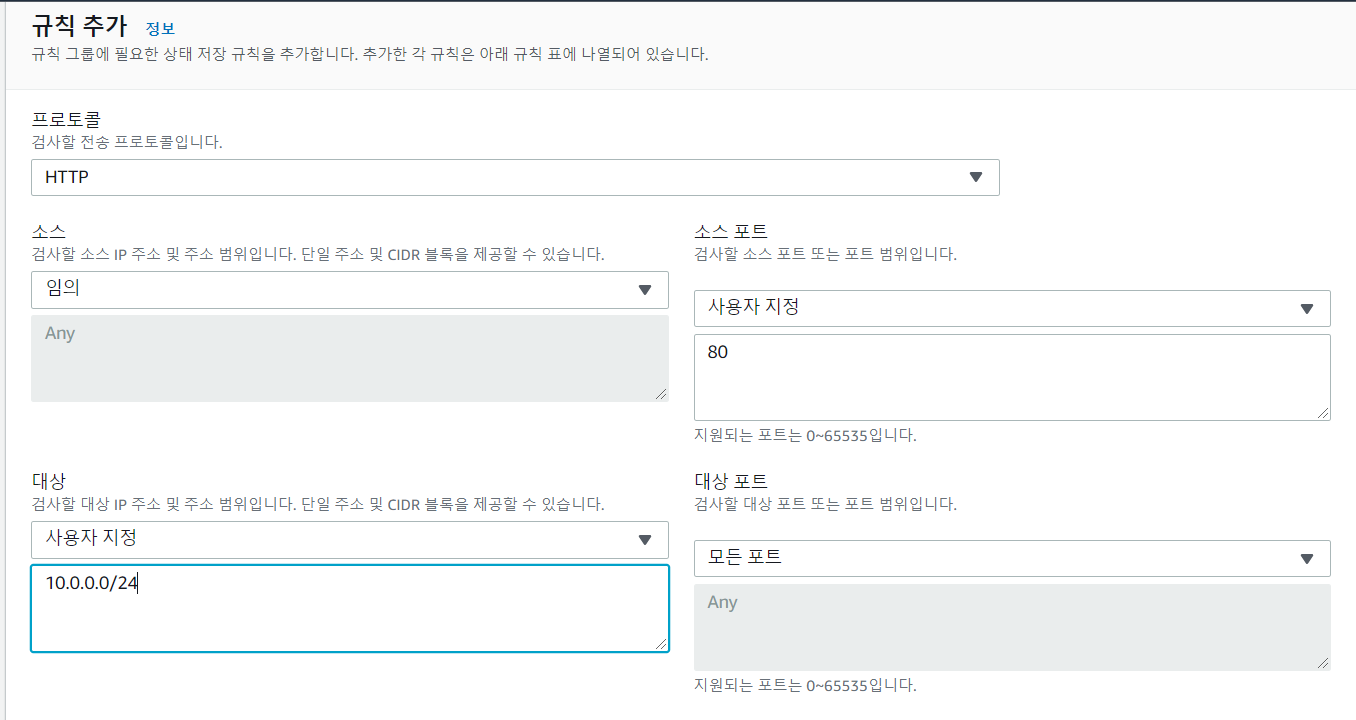


이름과 방화벽의 규칙 개수를 설정해 준다. 화면에 보이는 것은 임의의 값으로, 요구사항에 맞게 설정하면 된다.

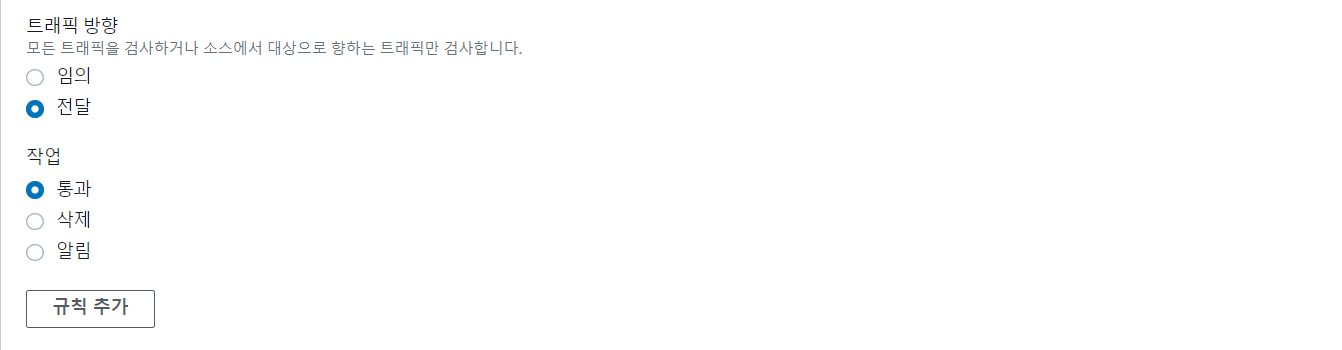


상태 저장 규칙 그룹 옵션 화면이다. 기본적으로 사용하는 5-tuple 방식을 선택했다. 요구사항에 맞게 선택하면 된다.

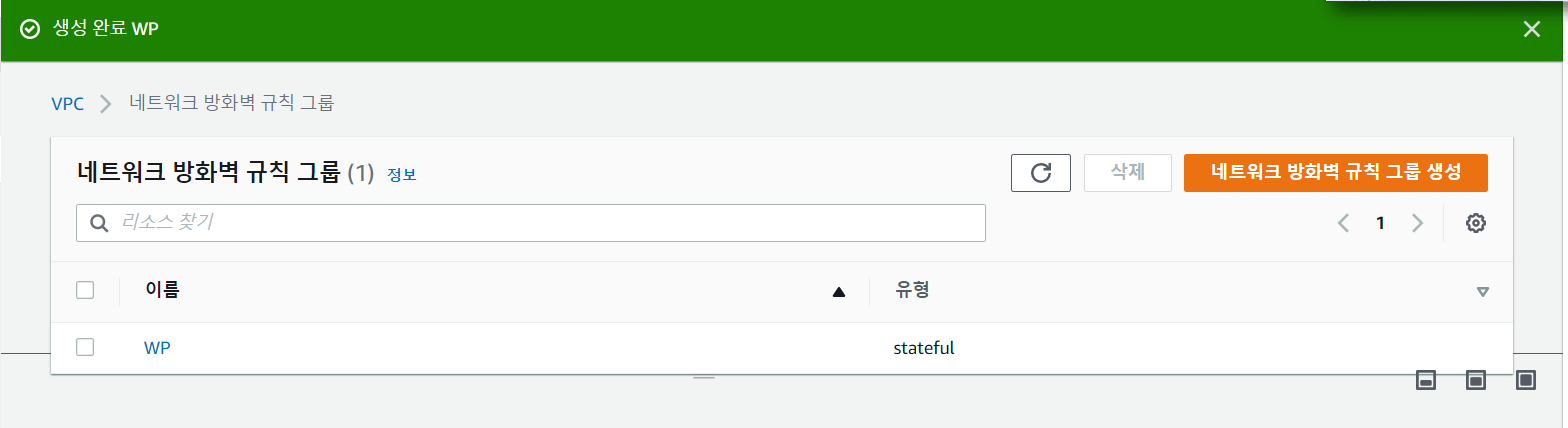




규칙 변수는 선택 사항이니 필요할 때 하고 규칙 추가에는 방화벽이 작용할 대상, 그리고 포트와 프로토콜을 선택하면 된다.

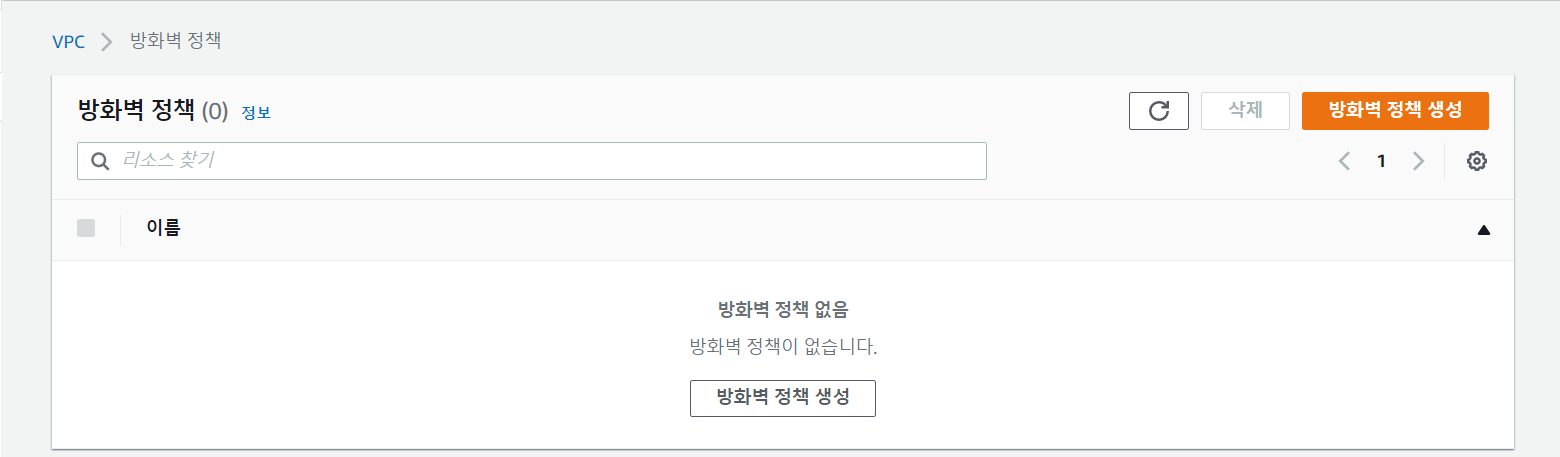


트래픽 관련 항목이다. 요구사항에 맞게 작업하면 된다.

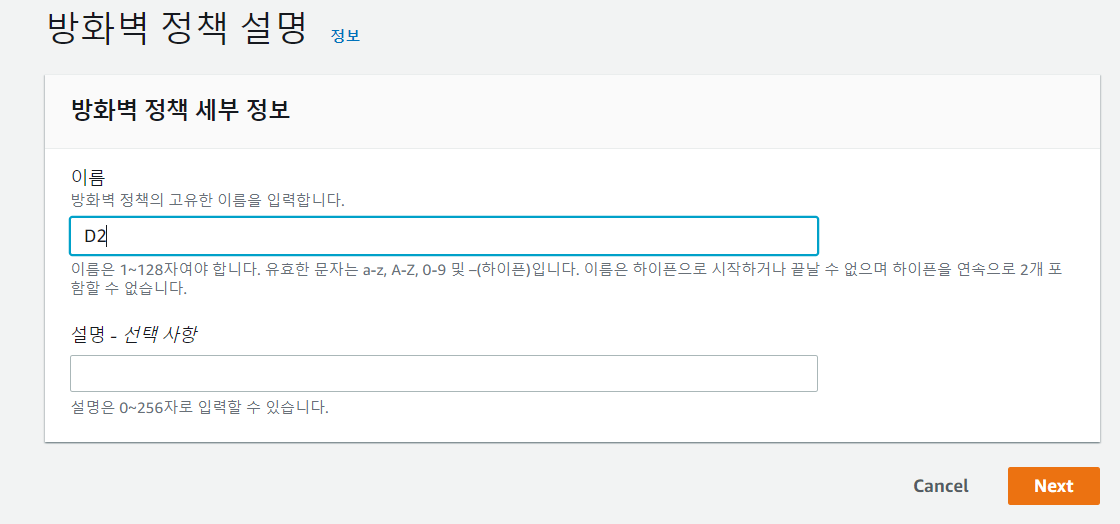


네트워크 규칙 그룹이 생성된 모습이다.

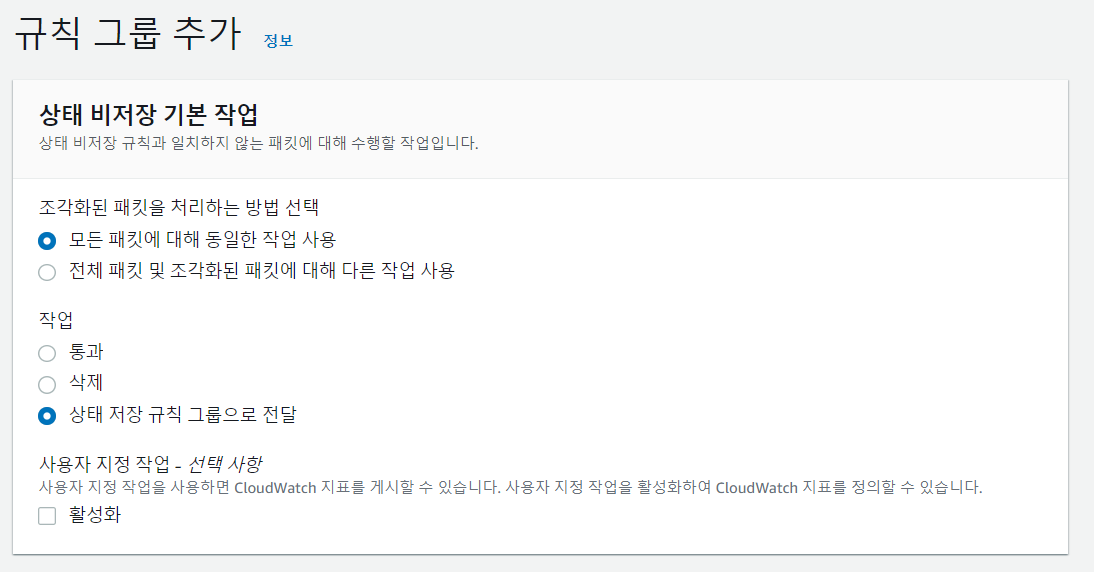
## 방화벽 정책 생성



방화벽 정책 생성을 누르면 방화벽 정책을 생성할 수 있다.



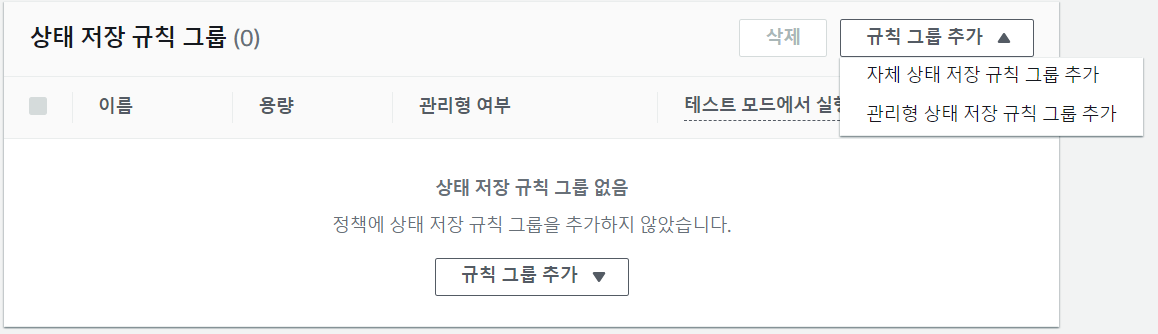
방화벽 정책의 이름을 입력한다.



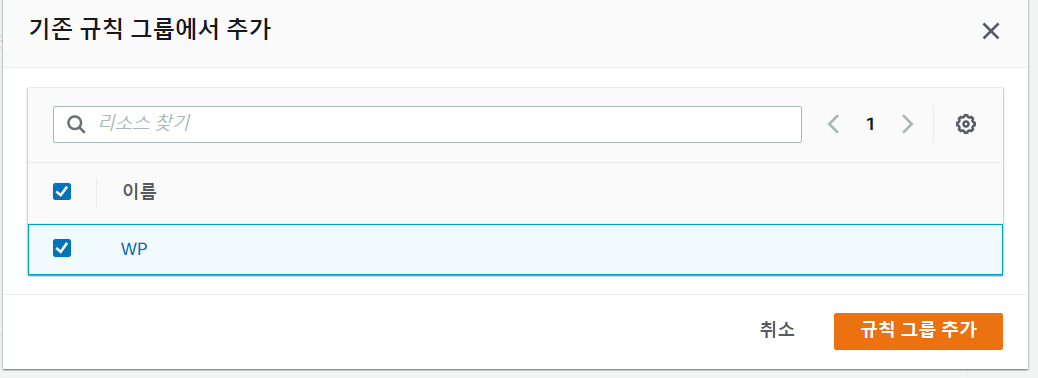
규칙 그룹 추가 화면이다. 상태 저장 규칙 그룹으로 전달을 선택한다.



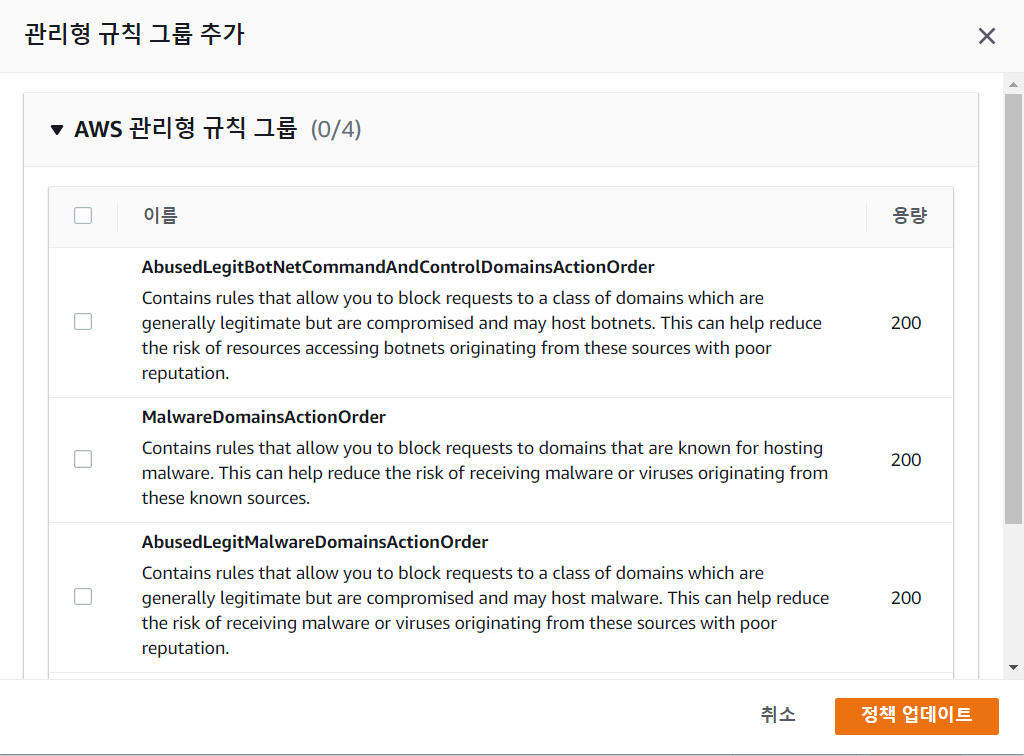
앞서 만들었던 네트워크 규칙 그룹을 적용할 수 있는 화면이다.



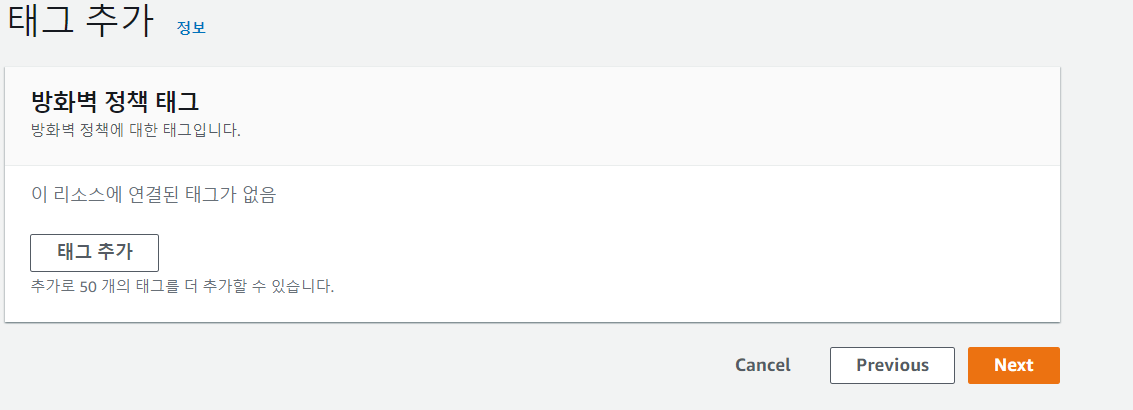
규칙 그룹은 AWS에서 제공하는 기본 항목과 자체적으로 만들어 놓은 규칙 그룹을 선택할 수 있다.



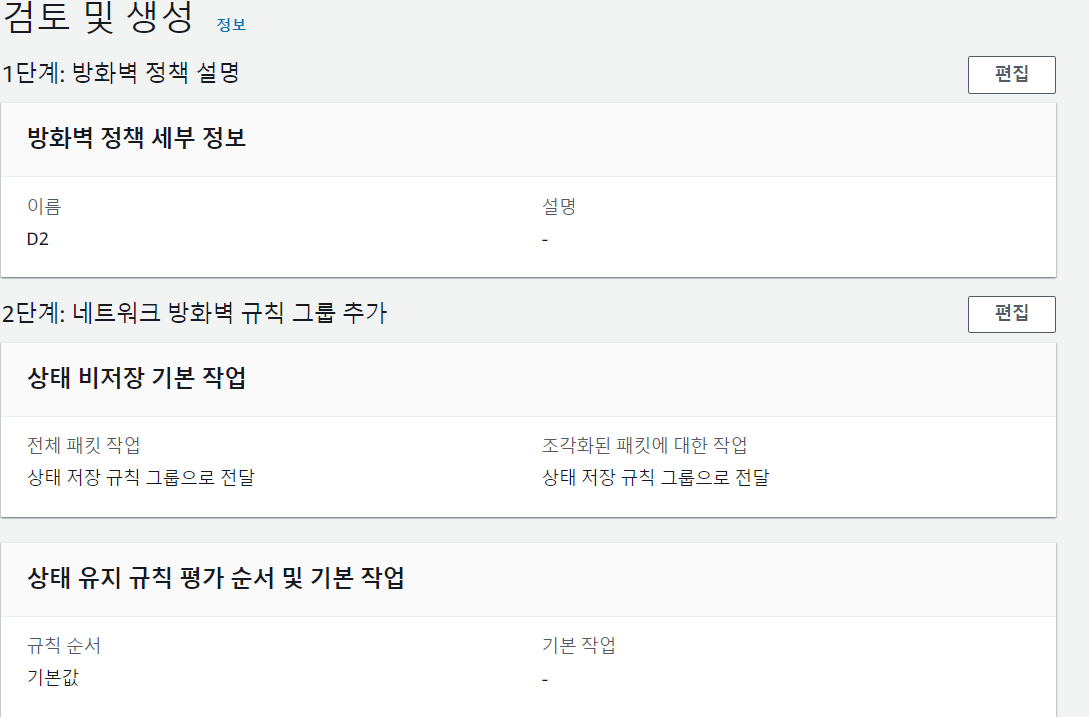
기존 규칙 그룹에서 아까 만들었던 규칙 그룹을 선택한다.



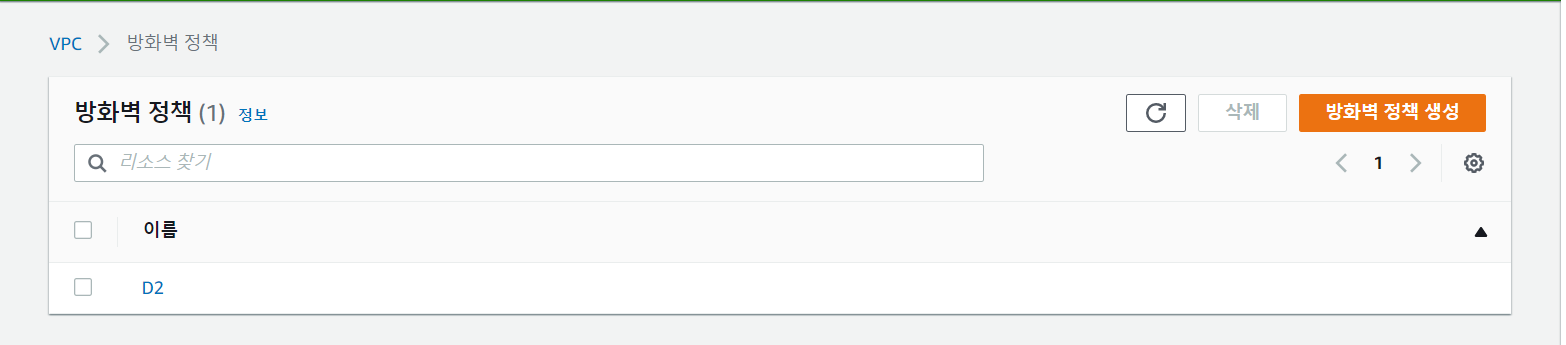
AWS에서 제공하는 규칙 그룹이다. 테스트용으로 사용할 수 있으니 체크해서 관찰해본다. 정책 업데이트를 누르면 적용된다.



태그 추가 화면이다. 알기 쉬운 태그를 붙인다.

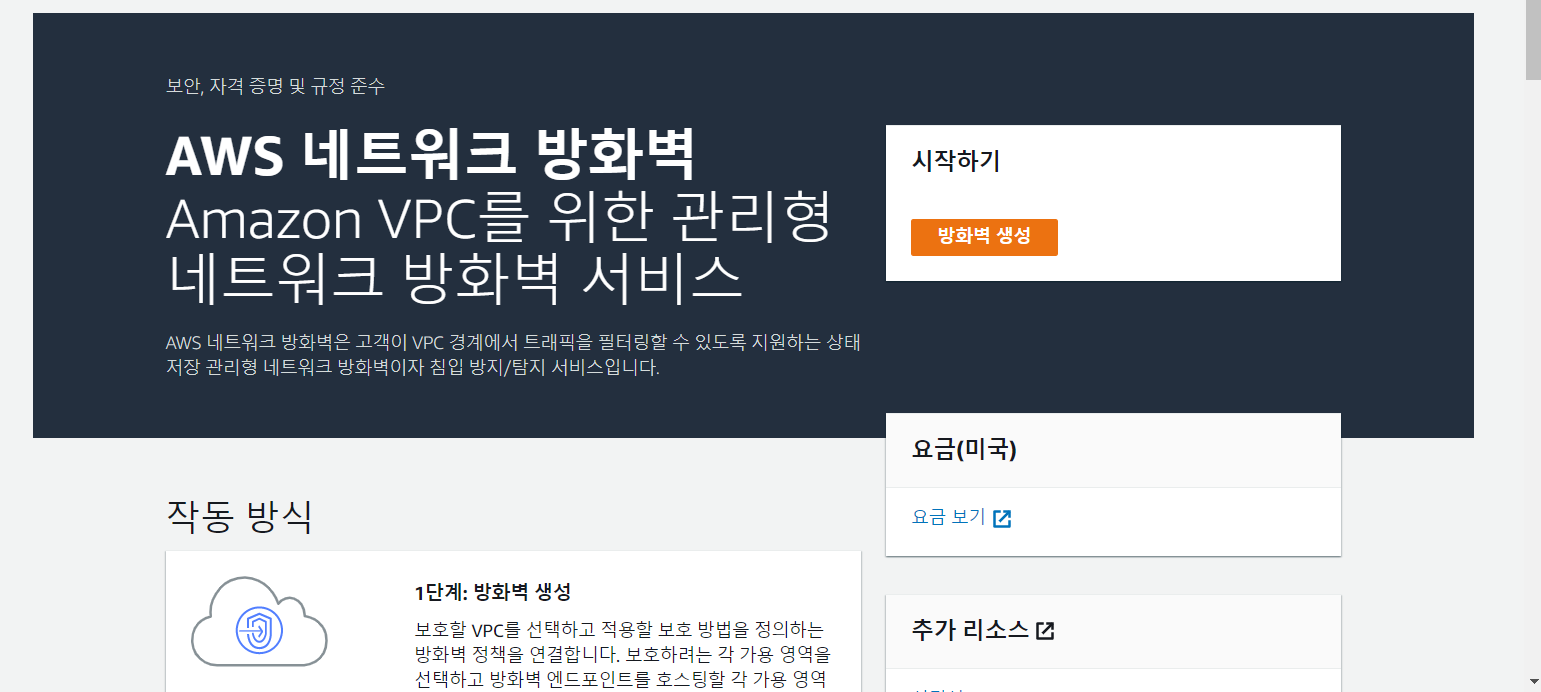


검토 화면이다. 자신이 설정해 놓은 사항들이 맞는지 검토하고 생성을 누른다.

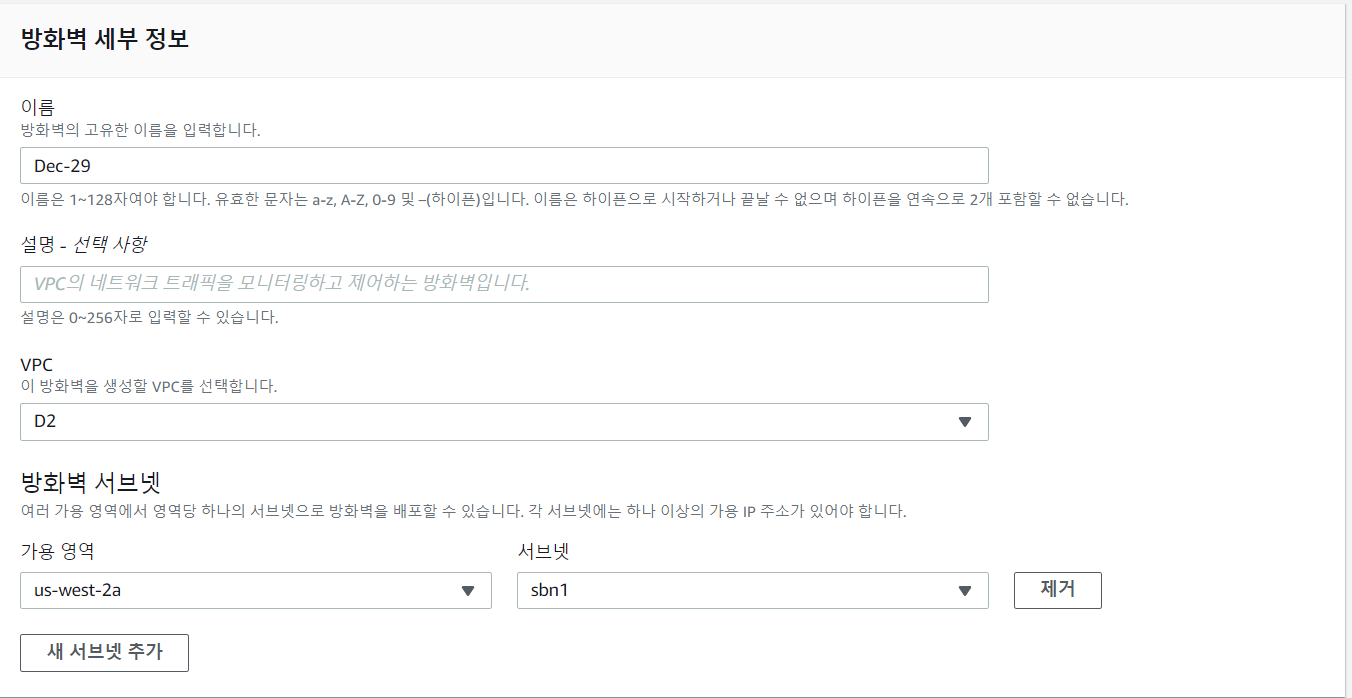


방화벽 정책이 생성된 모습이다.

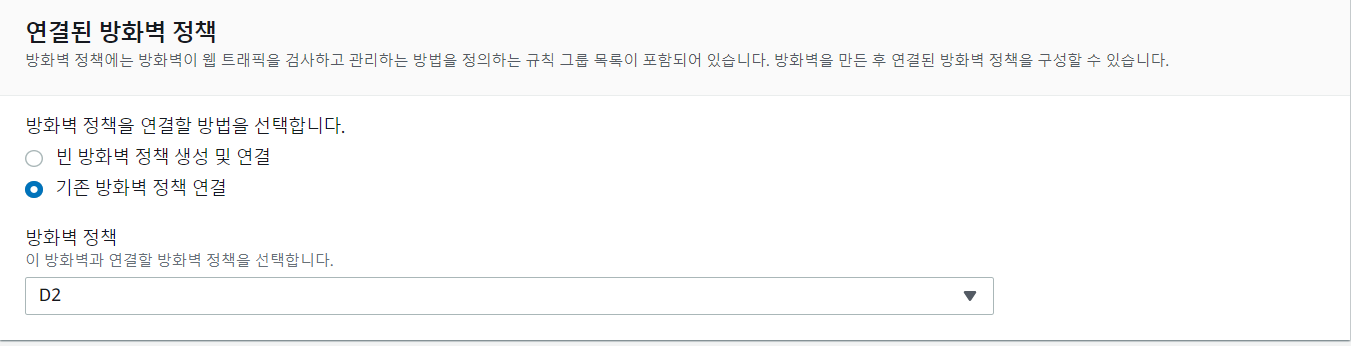
## 방화벽 생성



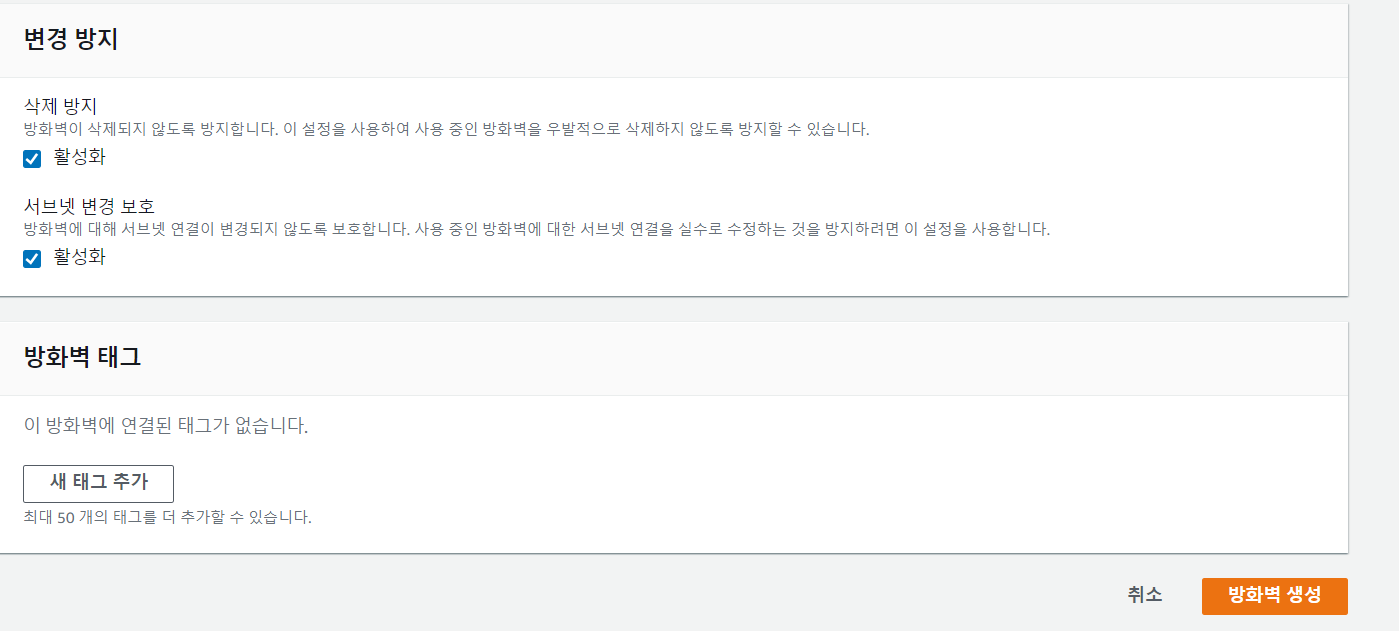
방화벽 생성 버튼을 눌러 방화벽을 생성하는 화면으로 들어간다.



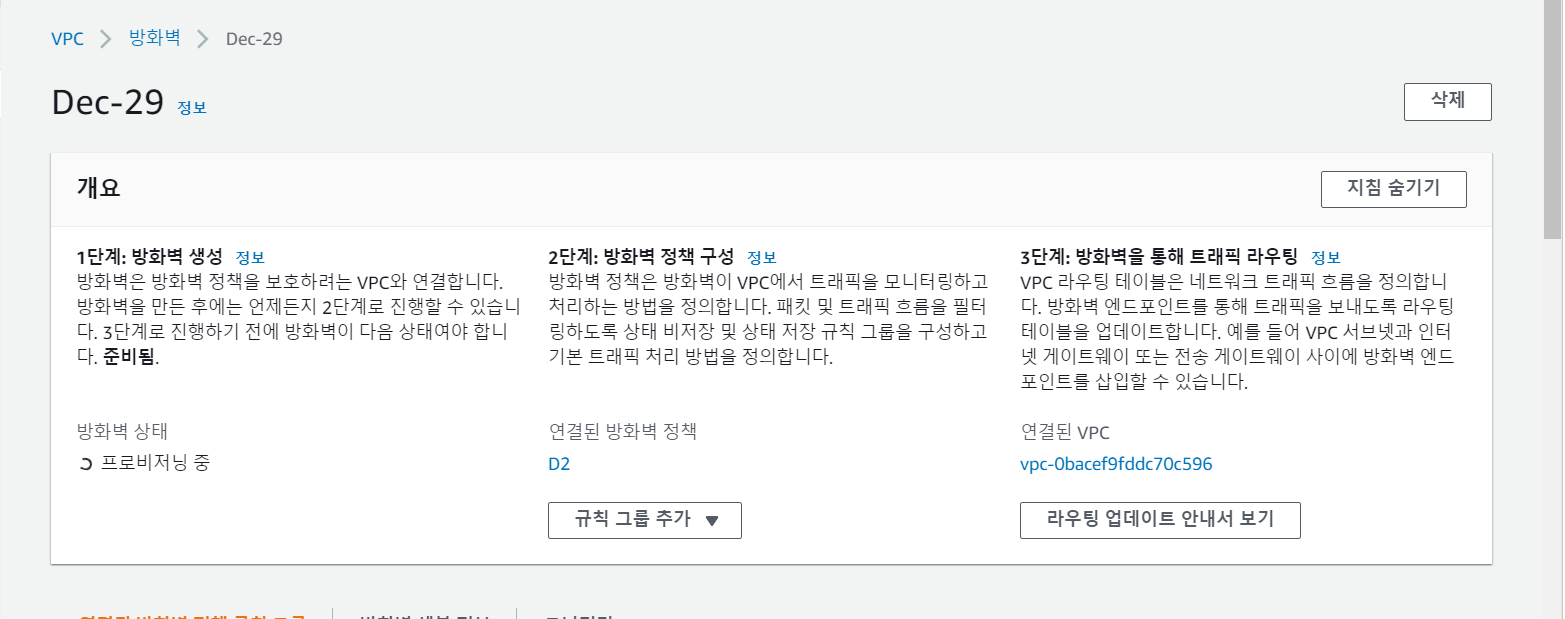
방화벽 이름을 입력하고 방화벽을 적용할 VPC, 서브넷을 선택한다.



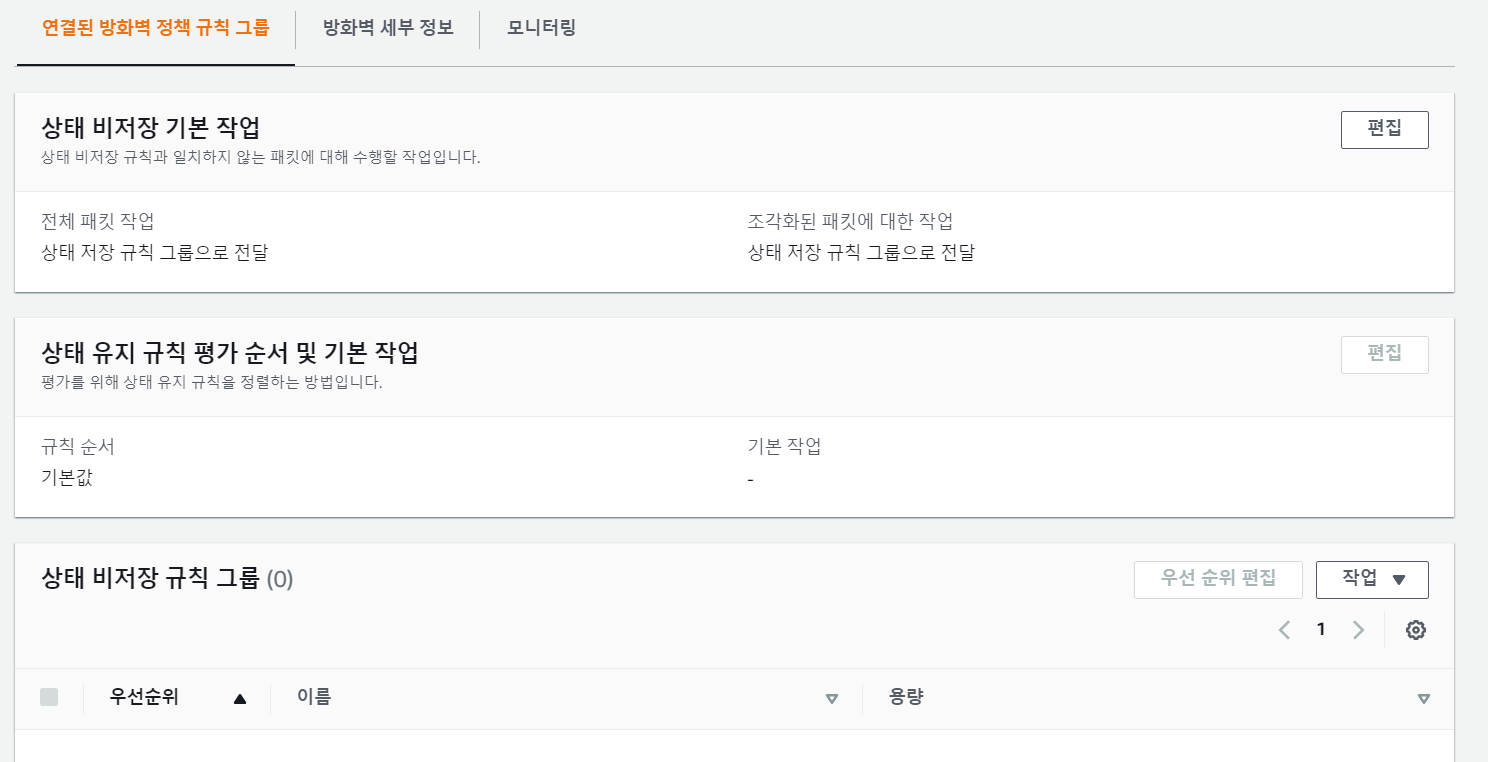
방화벽 정책을 선택하는 화면이다. 만들어놓은 방화벽 정책을 선택한다.



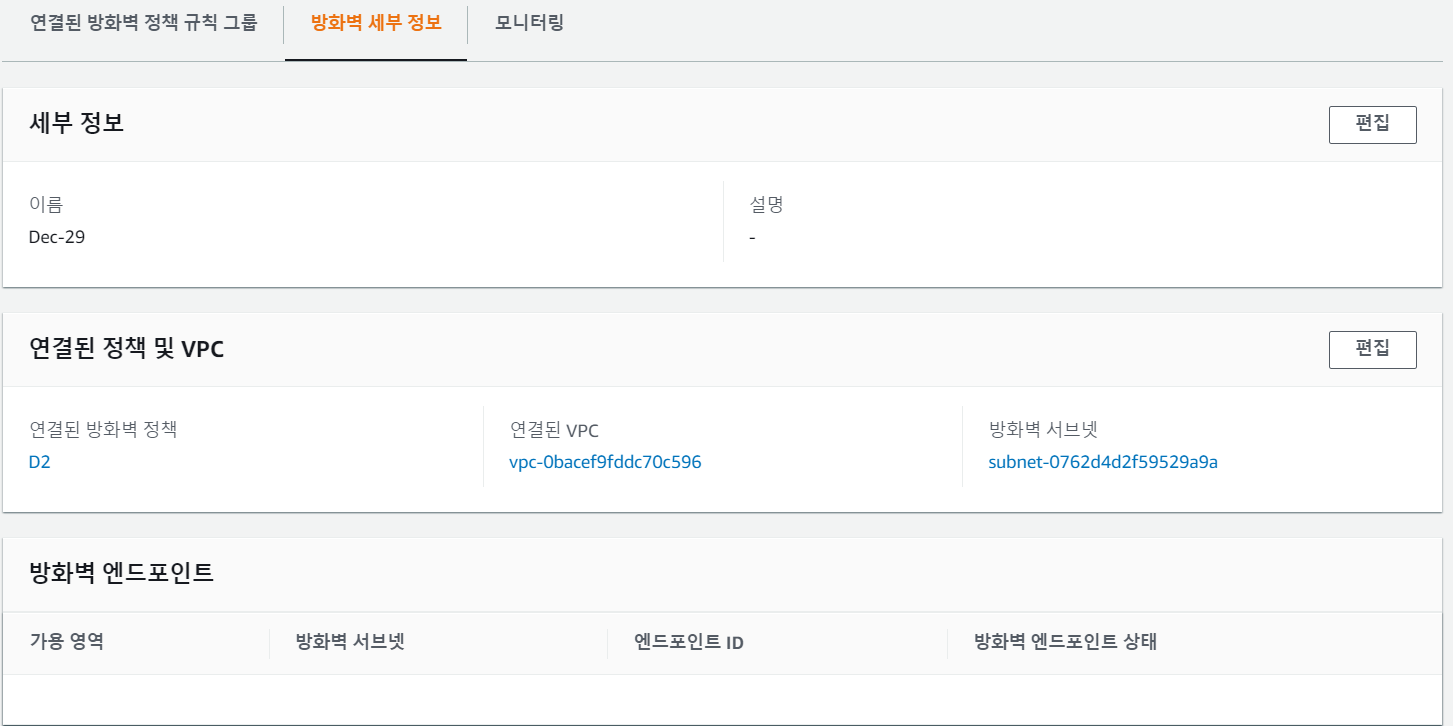
방화벽 태그를 설정하는 화면이다. 알기 쉬운 태그를 붙인다. 방화벽 생성 버튼을 누르면 방화벽이 생성된다.



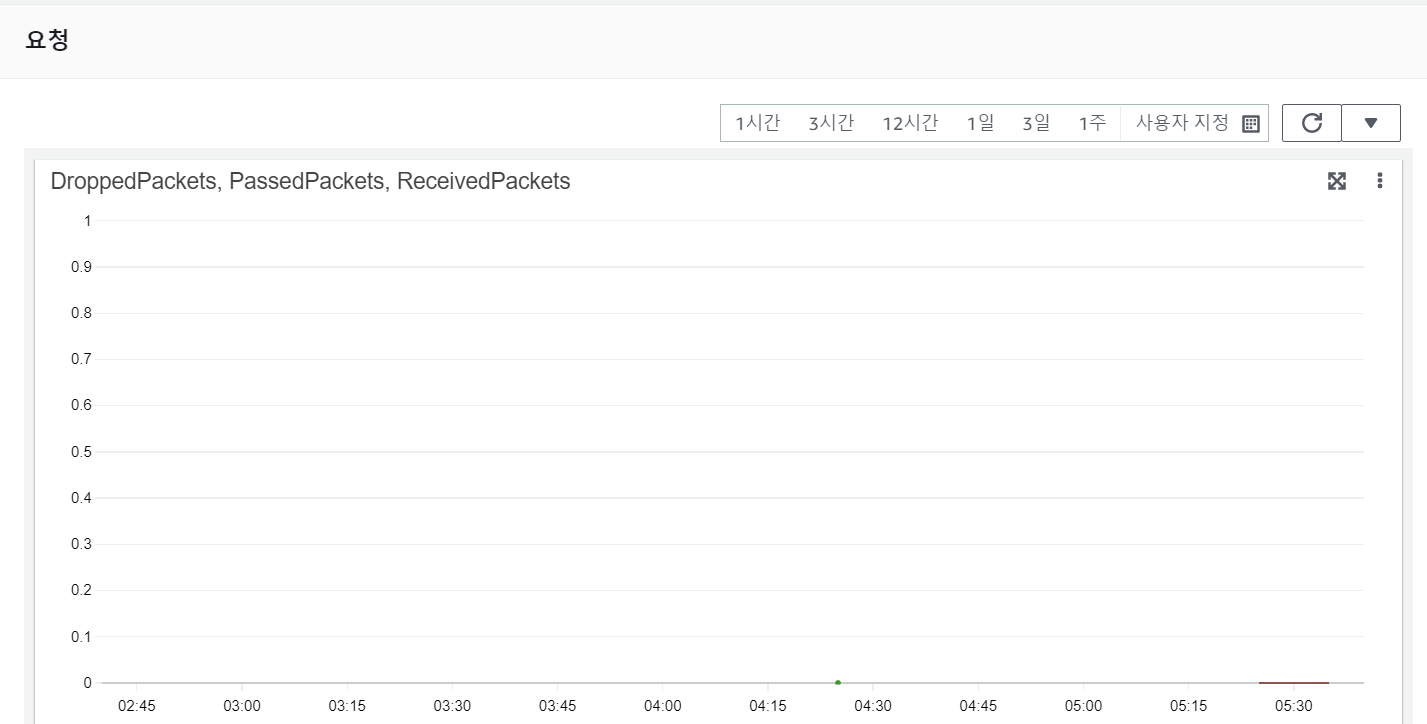
방화벽이 생성된 모습이다.



방화벽의 세부 설정 메뉴 중 하나인 연결된 방화벽 정책 규칙 그룹이다. 방화벽을 먼저 만들어놓고 여기서 규칙 그룹을 생성해도 된다.(이땐 Stateless방식이라고 한다.)

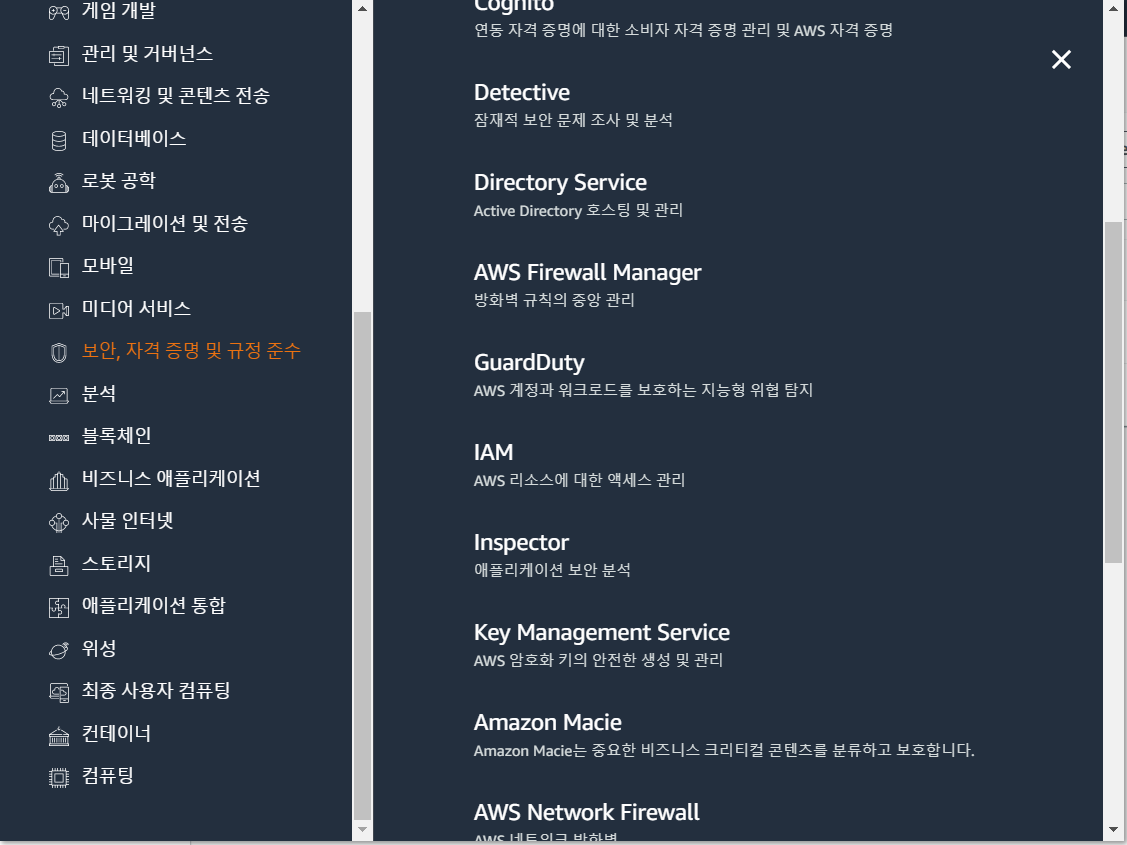


방화벽 세부 정보 화면이다. 방화벽과 연결된 정책, VPC 등을 확인할 수 있다.

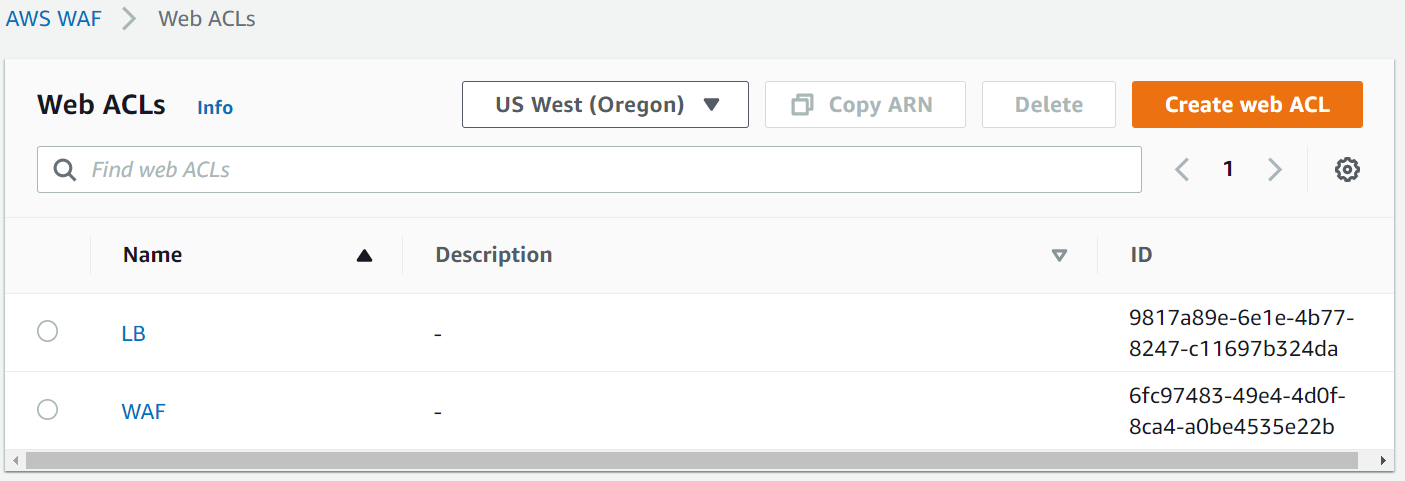


모니터링 화면이다. 방화벽의 활동을 그래프로 볼 수 있다.

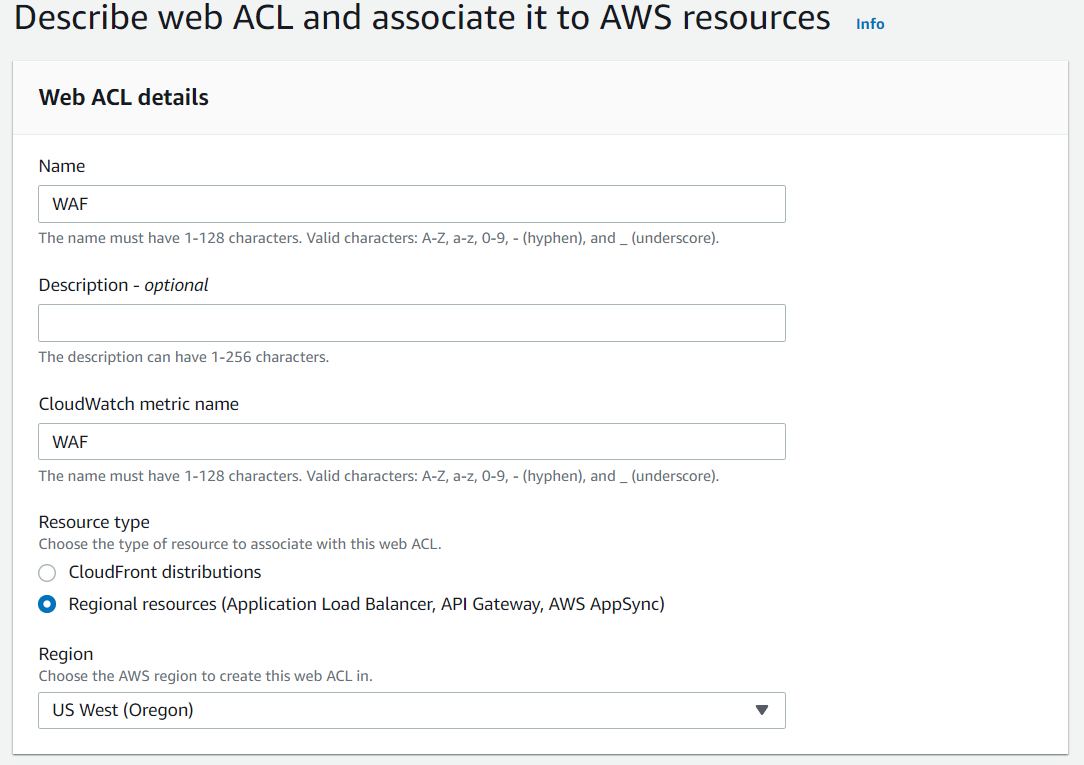
# WAF 생성



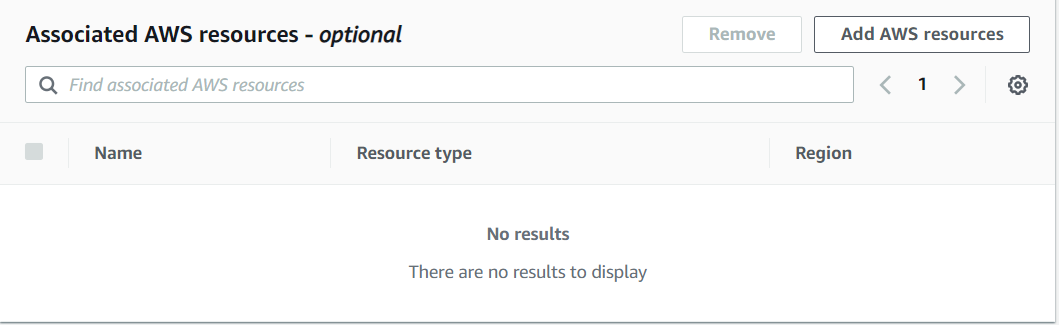
AWS 메뉴의 보안, 자격 증명 및 규정 준수 항목에서 AWS Firewall Manager항목을 클릭하면 WAF 설정을 할 수 있는 창으로 넘어간다.



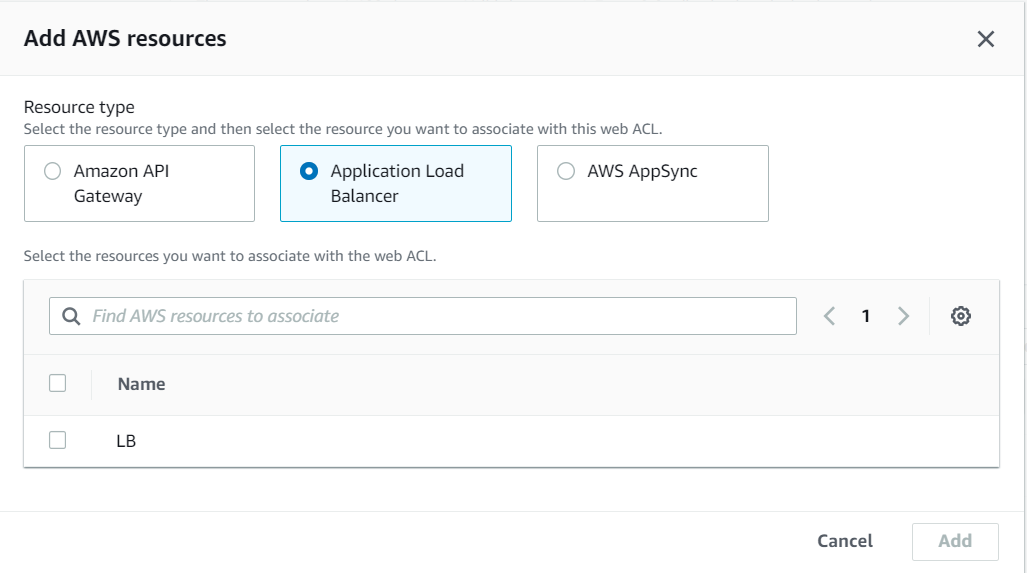
화면에는 이미 WAF가 생성되어 있는데 이 WAF를 생성하는 방법은 우선 Create web ACL 버튼을 클릭한다.



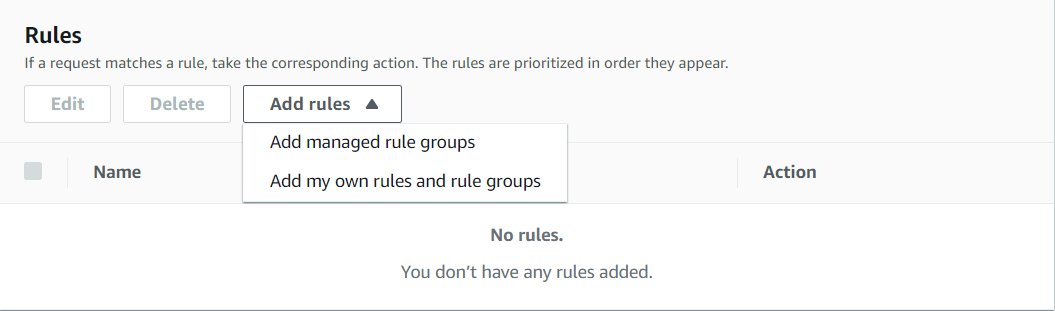
Web ACL의 세부 설정을 하는 화면이다. WAF 이름과 클라우드워치 메트릭 이름을 입력하고 리소스 타입을 리전 리소스로 바꾼 후 자신이 작업할 리전을 선택한다.



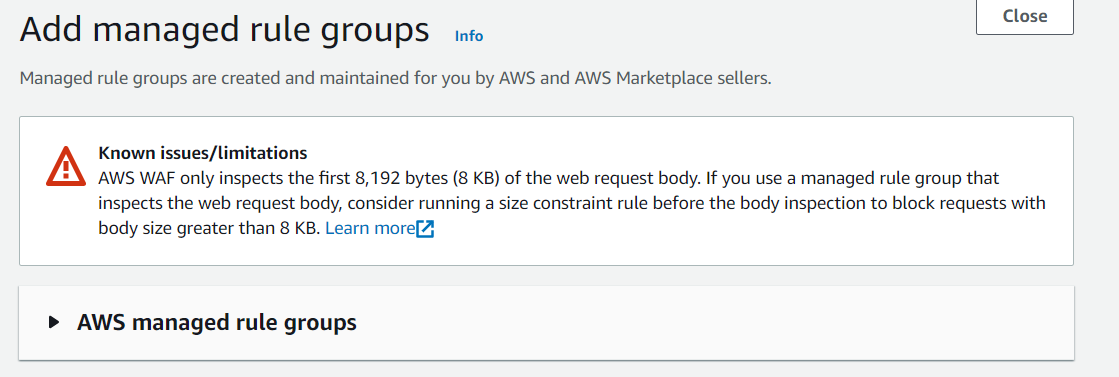
내가 가지고 있는 AWS 리소스와 연결할 수 있는 창이다. 오른쪽 위 Add AWS resources를 누르면

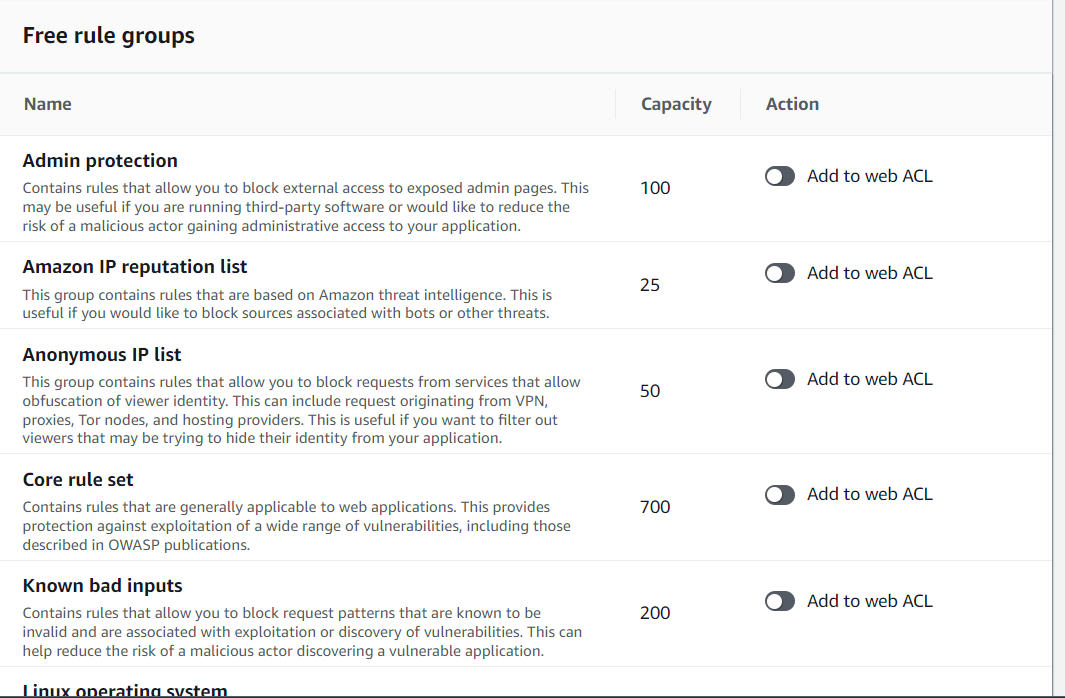


리소스를 선택하는 창이 뜬다. 만들어진 ALB를 연결하고 다음으로 넘어간다.

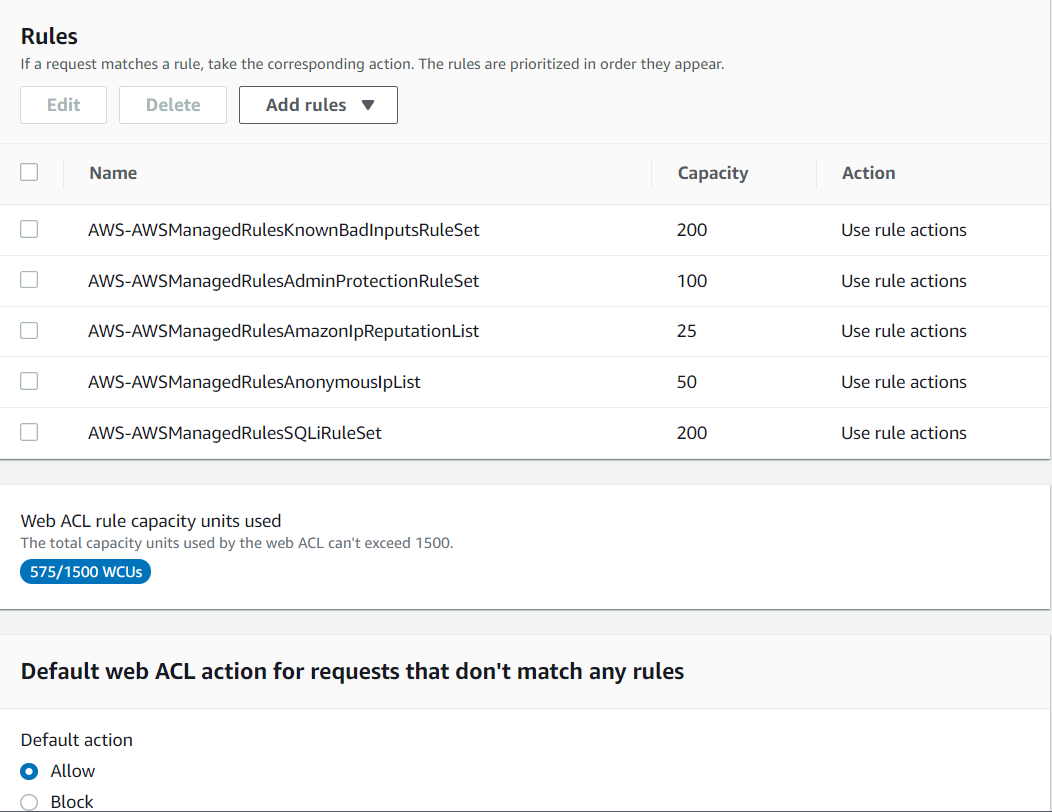


규칙을 추가하는 화면이다. 만들어 둔 규칙을 선택해도 되고 AWS에서 기본적으로 제공하는 규칙을 선택할 수 있다.

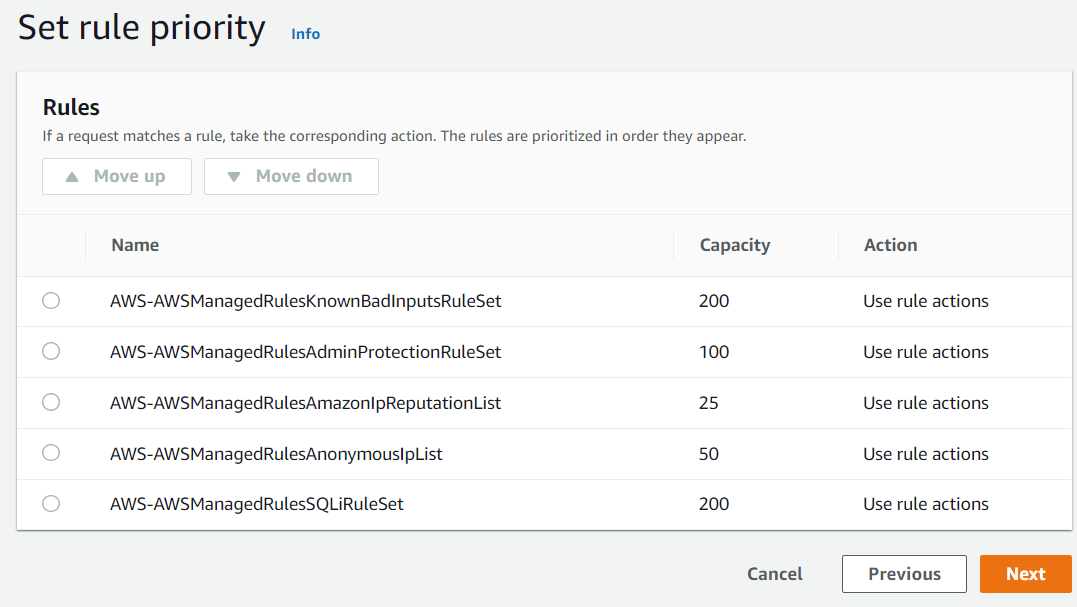




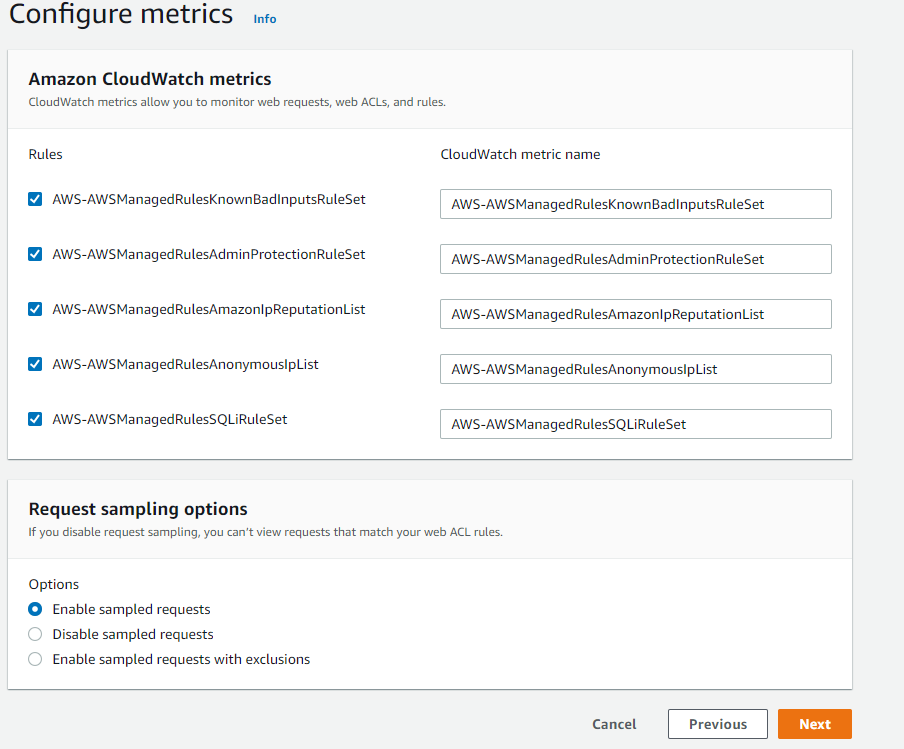
AWS에서 무료로 제공하는 규칙 그룹들이다. 규칙 양 제한에 걸리지 않게 추가할 것들을 추가하면 된다.



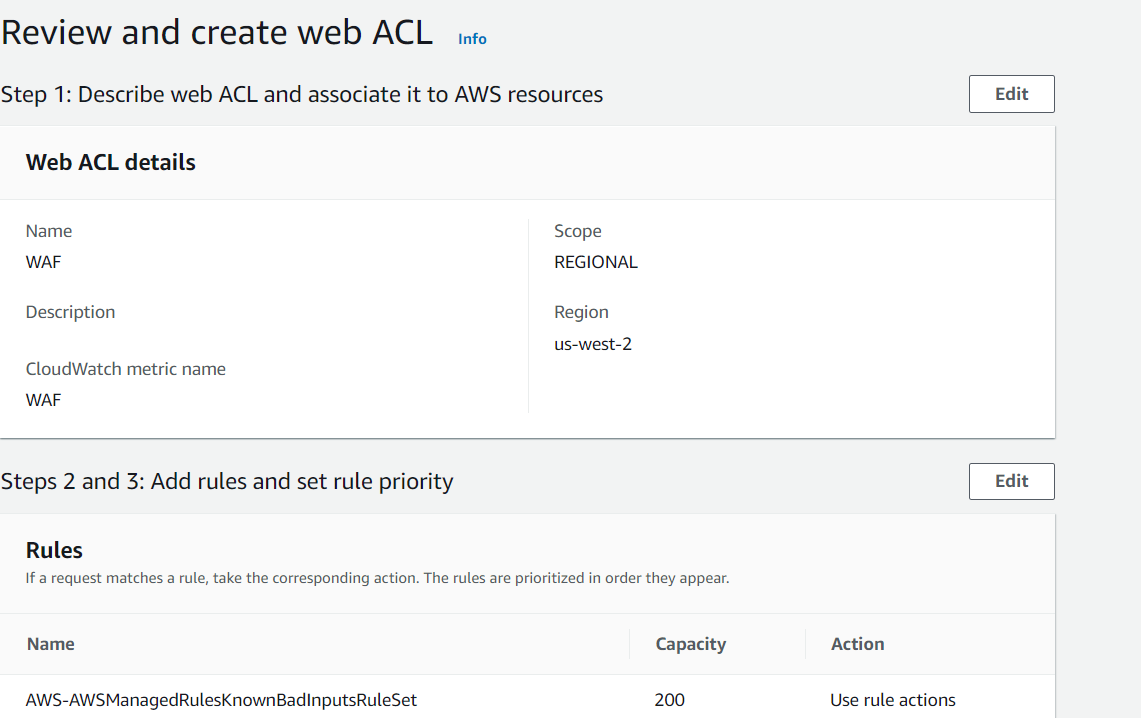
규칙을 확인하는 화면이다. 아래 체크는 허용으로 두고 다음으로 넘어간다.



규칙의 우선순위를 정하는 화면이다. 우선순위를 둘 규칙에 체크하면 된다.

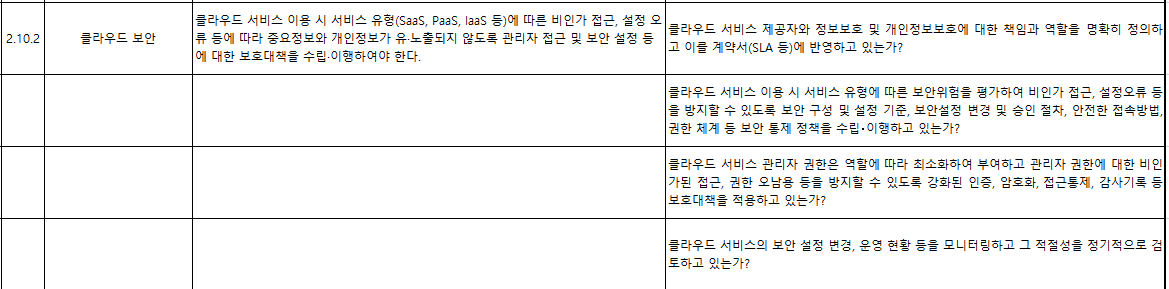


샘플 요청 화면이다. 샘플 요청은 하기 싫으면 Disable을 해도 된다.



검토 화면이다. 설정 사항들을 검토하고 만들기 버튼을 누르면 아까의 화면처럼 WAF가 생성된다.

# +ISMS-P 충족여부



ISMS-P의 2. 보호대책 요구사항에서 10-2번이 클라우드 보안 관련 조항이다.

세부 조항 중 첫번째인 클라우드 서비스 제공자와 정보보호 및 개인정보보호에 대한 책임과 역할을 명확히 정의하고 이를 계약서(SLA 등)에 반영하고 있는가? 항목을 보면 AWS는 별도의 계약서를 제공하지 않기 때문에 요건에 충족이 되지 않는다고 볼 수 있다.

또한, 세부 조항 중 세번째인 클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고 관리자 권한에 대한 비인가된 접근, 권한 오남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근통제, 감사기록 등 보호대책을 적용하고 있는가? 항목을 보면 관리자 권한 최소화를 명시하고 있는데 AWS는 관리자(매니저)권한이 최소화 되어있지 않으므로 요건이 충족되지 않는다고 볼 수 있다.