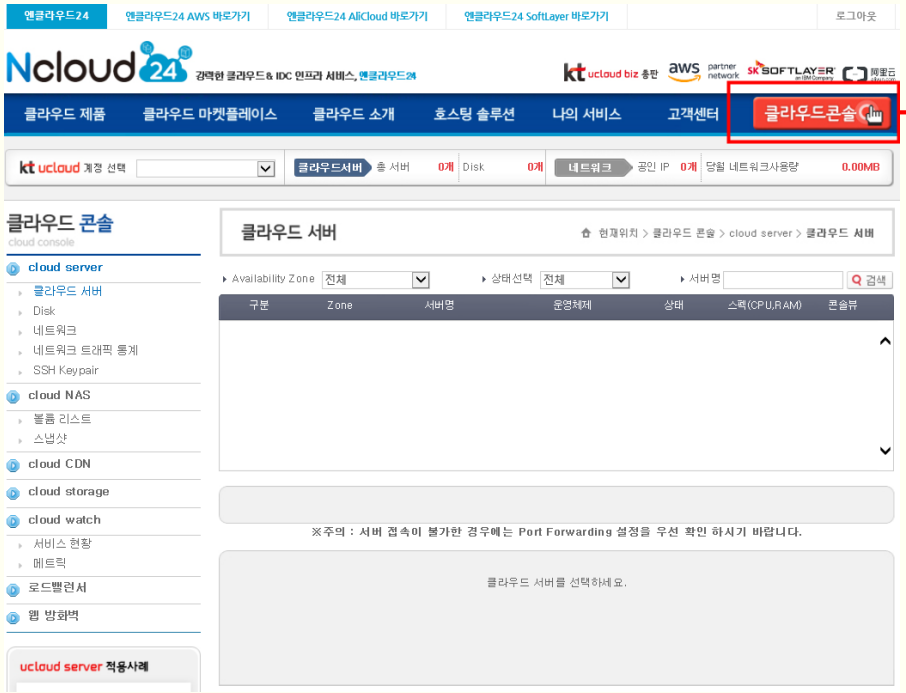
Ncloud 24
클라우드 & IDC 인프라 서비스 , 엔클라우드24

회원가입 및 사용자 매핑 진행 절차

회원가입 및 사용자 매핑 진행 절차

1 http://www.ncloud24.com 사이트에서 **회원가입** 진행 후

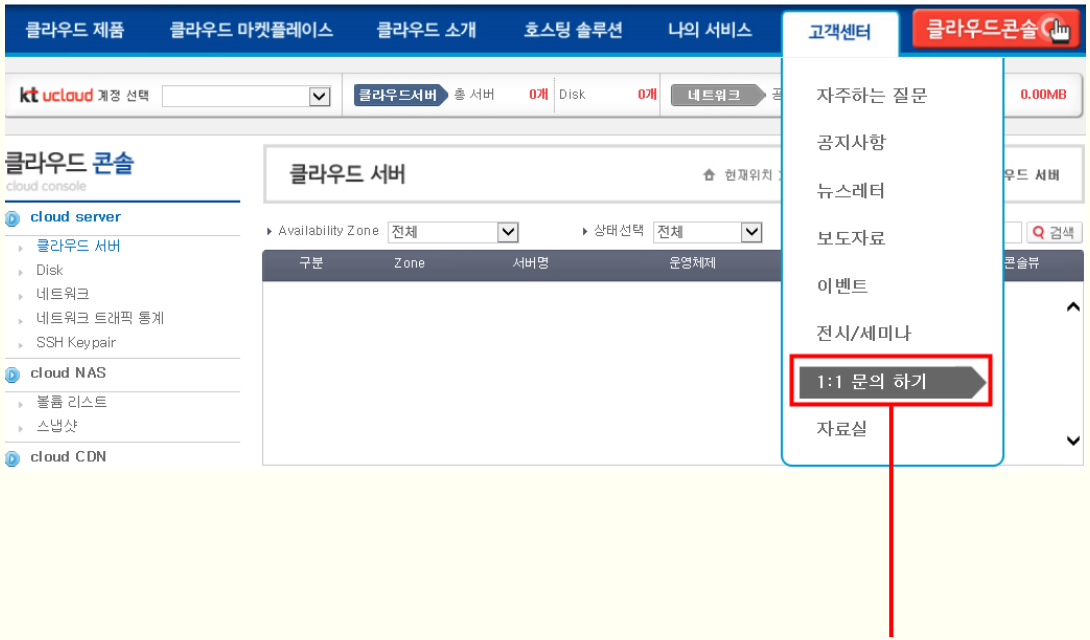


계정 로그인 후 **[클라우드콘솔]** 클릭시 초기화면

2 상단의 **[KT ucloud 계정 선택]**에 매핑된 계정이 없음

회원가입 및 사용자 매핑 진행 절차

3 엔클라우드24 계정과 KT cloud 계정과의 매핑 요청을 진행



상위 메뉴에서 **[고객센터]** > **[1:1문의하기]** 클릭

회원가입 및 사용자 매핑 진행 절차

4 계정 매핑 내용 문의

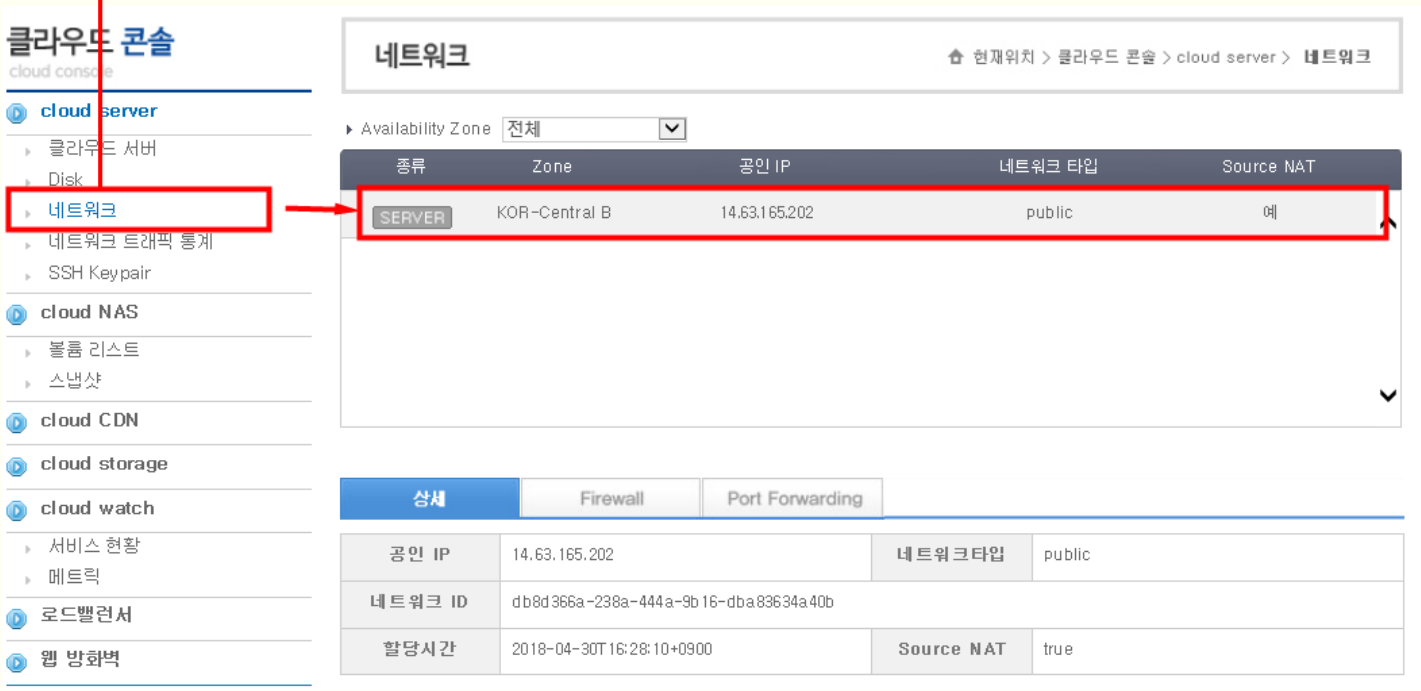
회원가입 및 사용자 매핑 진행 절차

5 문의된 사항에 대하여 완료 답변 수신 후 새로고침 및 재로그인 시 아래와 같이 요청된 계정과 생성된 서버가 확인됨.

회원가입 및 사용자 매핑 진행 절차

6 순차적인 클릭

[cloud server] -> [네트워크] -> [SERVER] 클릭

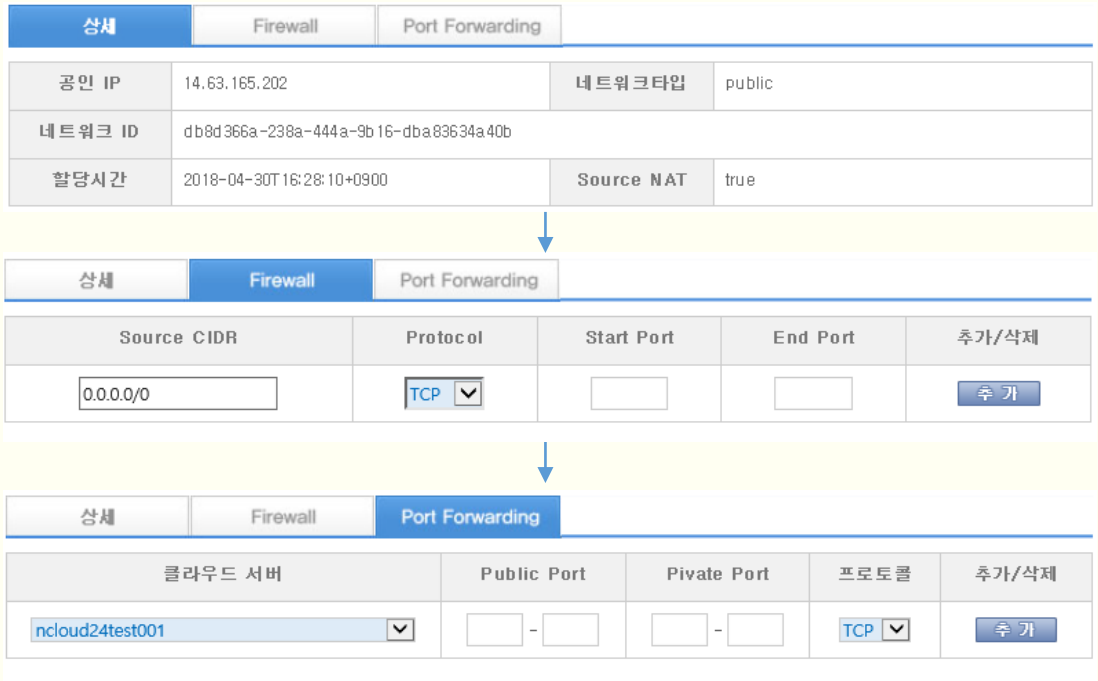


Ncloud 24
클라우드 & IDC 인프라 서비스 , 엔클라우드24

서버포트포워딩 및 방화벽 설정

포트포워딩 설정

1 상위와 같이 **[상세] / [Firewall] / [Port Forwarding]**을 클릭시 현재 상태를 확인 가능
초기화된 상태에서 설정된 **Firewall / Port Forwarding** 정책이 없음.
이에 따라 서버에 접근이 불가능한 상태임.



1. Port Forwarding 정책 설정
2. Firewall 정책 [삭제/추가]로 수정

왼쪽 이미지 순서로 서버 접근 정책 수립 후
서버 접근 가능

포트포워딩 설정

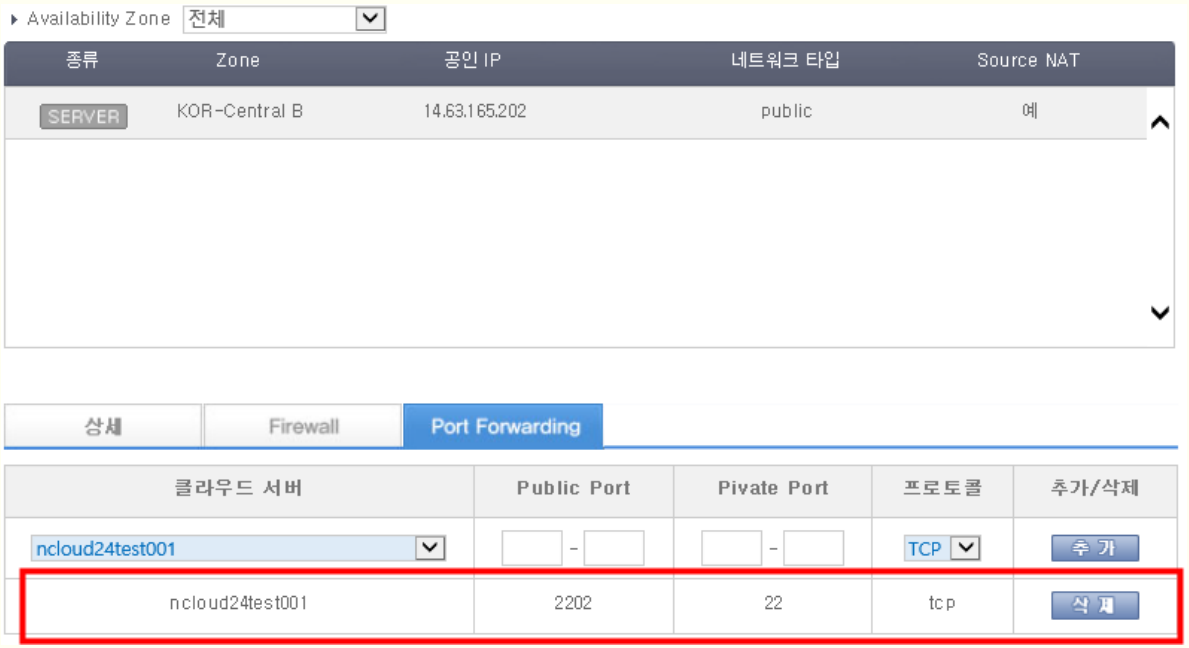
2 아래 예시와 같이 리눅스 서버 접근을 위한 포트 오픈 진행

클라우드 서버 : ncloud24test001 서버 지정
Public Port : 외부에 오픈되는 포트로 2202로 임의 지정
Private Port : 실제 서버에 운영중인 포트로 22를 지정
프로토콜 : TCP 포트 오픈이므로 TCP 지정

상기내용 지정 후 **[추가]** 버튼 클릭

포트포워딩 설정

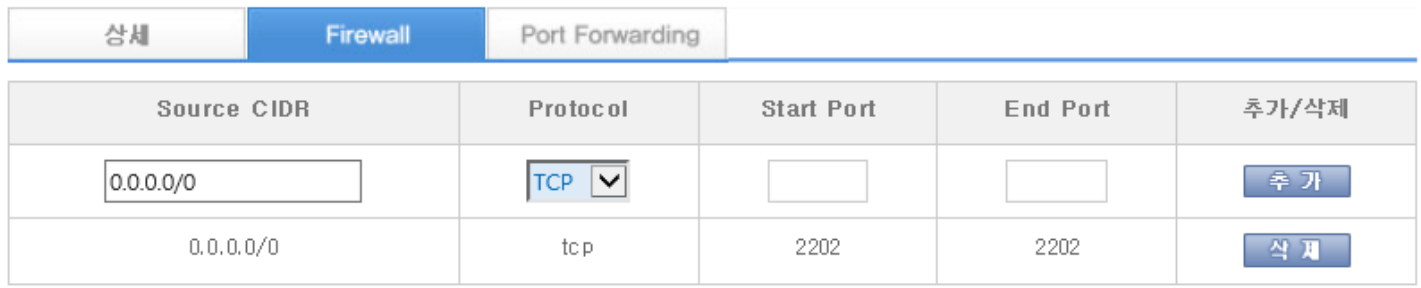
3 아래와 같이 추가된 **Port Forwarding** 리스트를 확인됨.



포트포워딩 설정

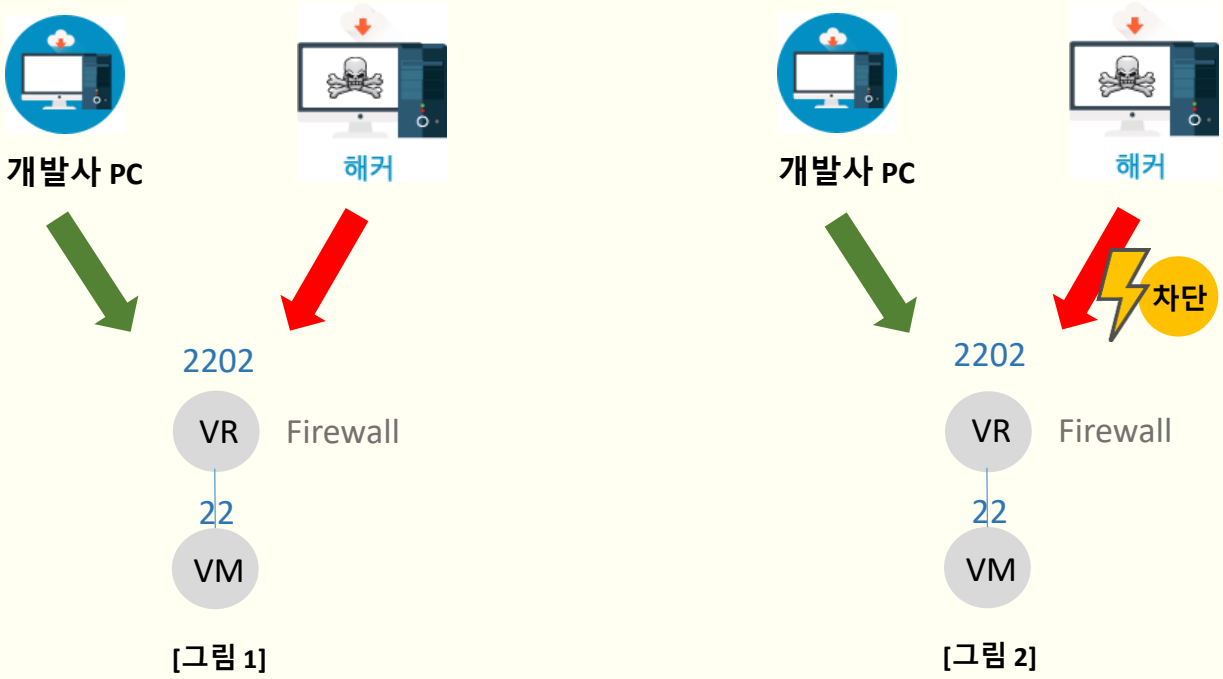
4 아래와 같이 **[Firewall]**을 클릭시 포트 포워딩 추가후에
0.0.0.0/0 라는 원격지의 모든 IP들에 대하여 2202포트 오픈 확인됨.
(포트포워딩 정책 추가시 자동으로 모든 IP에 대하여
해당 public port가 오픈되어 수정이 필요)

CIDR표기법에 대하여서는
https://blog.naver.com/ncloud24/221208338209 참고



포트포워딩 설정

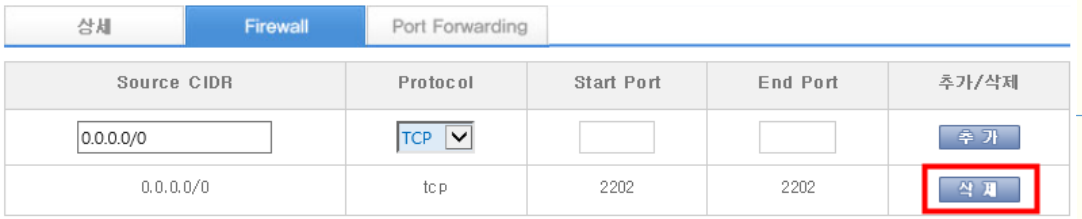
④ 상위 정책



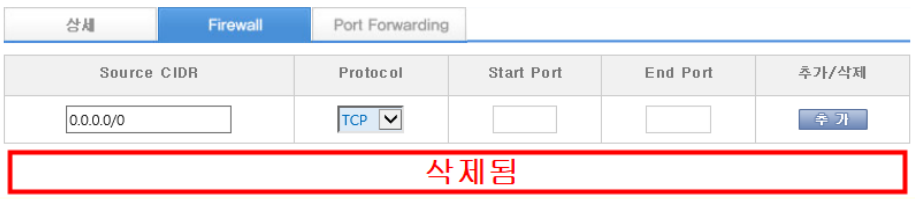
[그림 1]은 상위 정책과 같은 상태로 SSH 접속 포트에 대하여 공격 유입 가능성이 있어,
그림 2와 같이 특정 IP에 대한 접근만 허용이 필요함.

방화벽 설정

5 아래와 같이 **[Firewall]**을 클릭 상태에서 해당 정책 **[삭제]**클릭



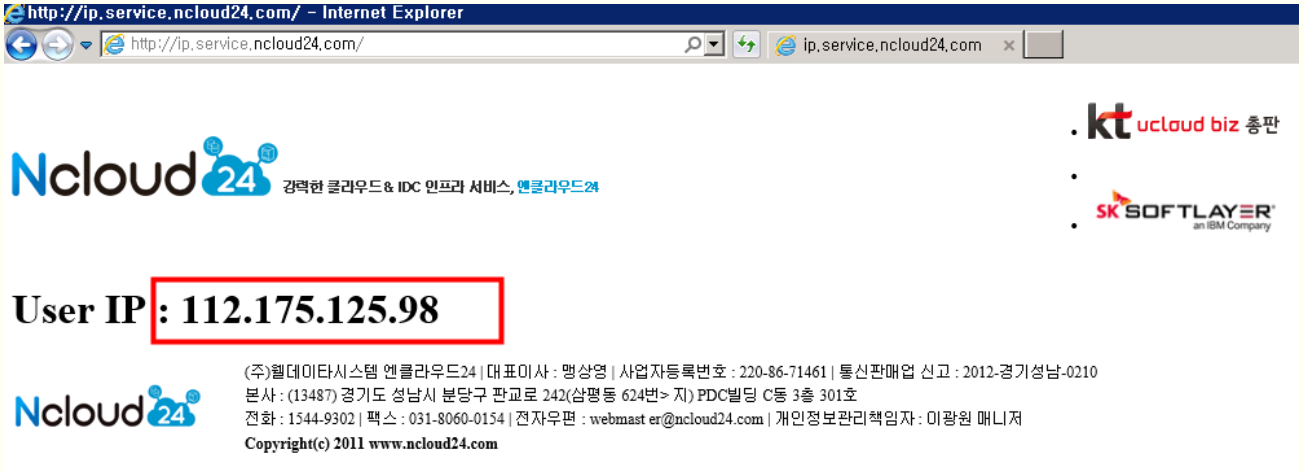
팝업되는 창에서 [예]를 클릭하여 해당 정책 삭제 진행
Firewall에서 확인시 오픈 정책없음 확인



방화벽 설정

6 내 PC(사무실,집,학교)에서만 ssh 접속에 대한 접근 허용

브라우저에서 현재 내 IP 확인
http://ip.service.ncloud24.com



- ncloud24 콘솔에서 SSH 접근 포트인 TCP 2202포트를 IP 112.175.125.98 에서만 접근 가능하도록 오픈

방화벽 설정

7 아래와 같이 추가됨을 확인

상세 | Firewall | Port Forwarding

Source CIDR	Protocol	Start Port	End Port	추가/삭제
112.175.125.98/32	TCP	2202	2202	추 가

상세 | Firewall | Port Forwarding

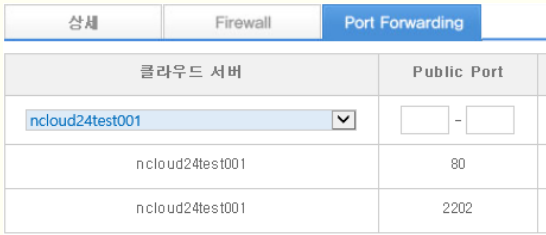
Source CIDR	Protocol	Start Port	End Port	추가/삭제
0.0.0.0/0	TCP			추 가
112.175.125.98/32	tcp	2202	2202	삭 제

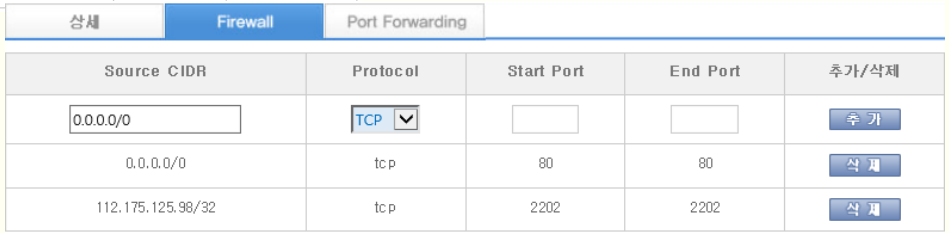
방화벽 설정

8 웹 서비스등의 특정 IP가 아닌 불특정 다수 접속을 위한 서비스 오픈

9 ncloud24 콘솔에서 웹서비스 포트인 TCP 80포트를 포트포워딩에서 추가

이후 **Firewall** 정책에서 확인





상위와 같이 웹서비스 포트인 TCP 80에 대하여 any(0.0.0.0/0)으로 자동 오픈되어 있는 부분 확인

주의사항

방화벽 설정 주의사항

1. 방화벽 오픈 초기 단계인 포트포워딩 오픈 시
   자동으로 any정책으로 오픈됨.

2. SSH, FTP, Mysql, PostgreSQL 등과 같은 관리형 포트오픈 시
   특정 IP만 접근 할 수 있도록 진행할것.

3. 서비스 포트 오픈시에도 기본적으로 제공되는 서비스상태에서
   오픈 시키지 말것.
   ex) apache 및 tomcat 웹서비스의 경우
   - 기본 페이지를 오픈 금지

4. 웹서비스 시 개발간 반드시 특정 IP만 오픈하여 서비스 확인후
   개발 완료시 오픈할 것.

5. 불필요한 포트는 오픈 시키지 말 것.

시스템 운영간 주의사항

1. 기본적으로 제공되는 계정에 대한 패스워드는 변경 권장
   패스워드 복잡도(대소문자/특수문자/숫자 조합으로 변경)

2. 개발시 서버에 업로드되는 데이터는 반드시 자체 백업을 진행.

3. 사용하지 않는 서비스는 운영하지 말것.

4. 과도한 트래픽을 유발하는 사용을 금할것.
   (과도한 트래픽 확인시 차단조치 진행)

5. 서버내 사용예정인 어플리케이션은 ncloud24 FAQ 및 블로그,
   포털의 검색을 활용하여 설치,설정,운영 할것.
   https://www.ncloud24.com/customer/bbs_faq.php
   https://blog.naver.com/ncloud24

감사합니다.