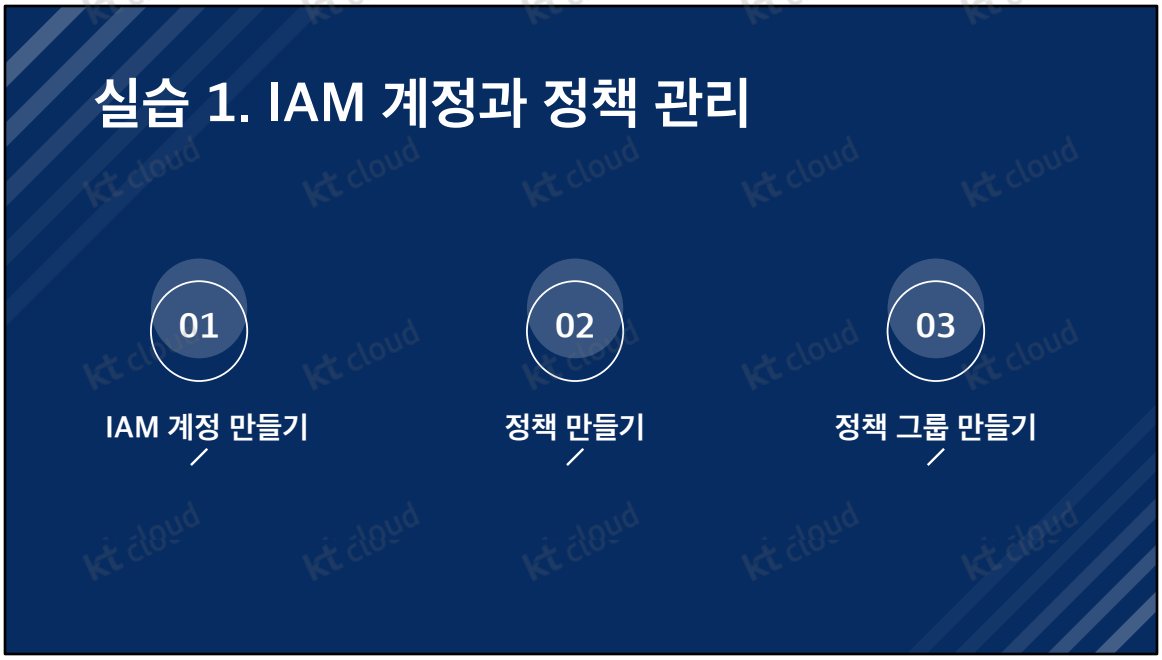
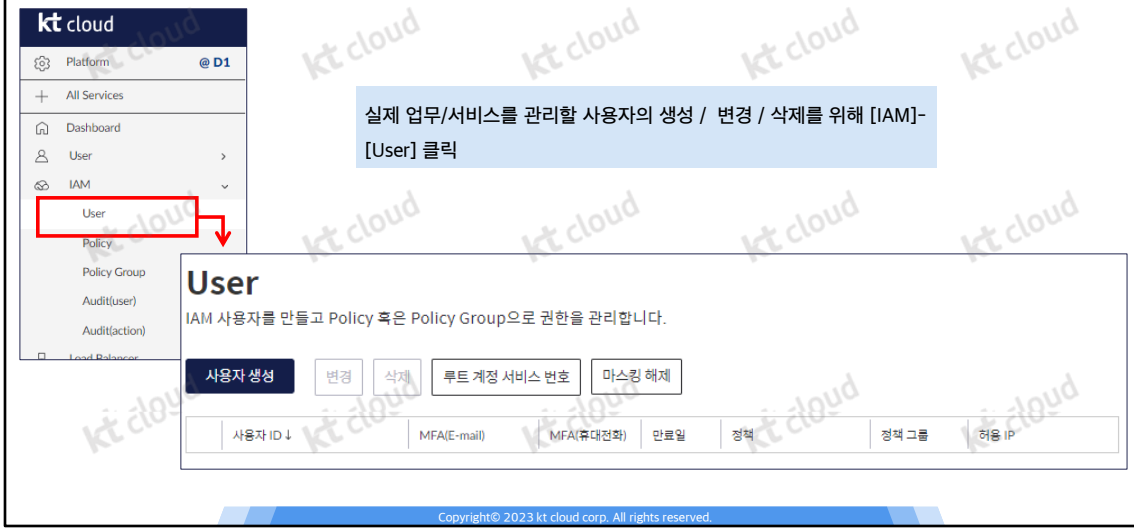


IAM 실습에서는 지금까지 사용한 루트계정으로 다음의 작업을 합니다.

- 계정 생성
- 정책 생성, 정책 그룹 생성

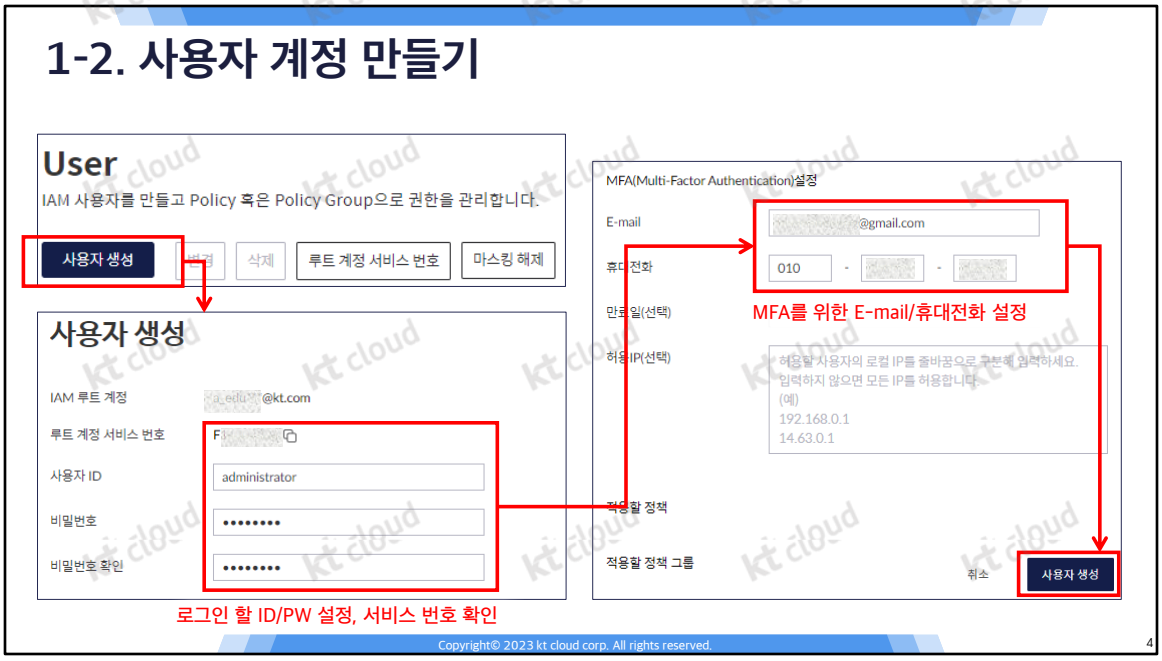
그 이후, 생성한 새로운 계정으로 다시 로그인하여 정책에 따른 권한 관리가 되는지 확인합니다.

1-1. 사용자 계정 보기



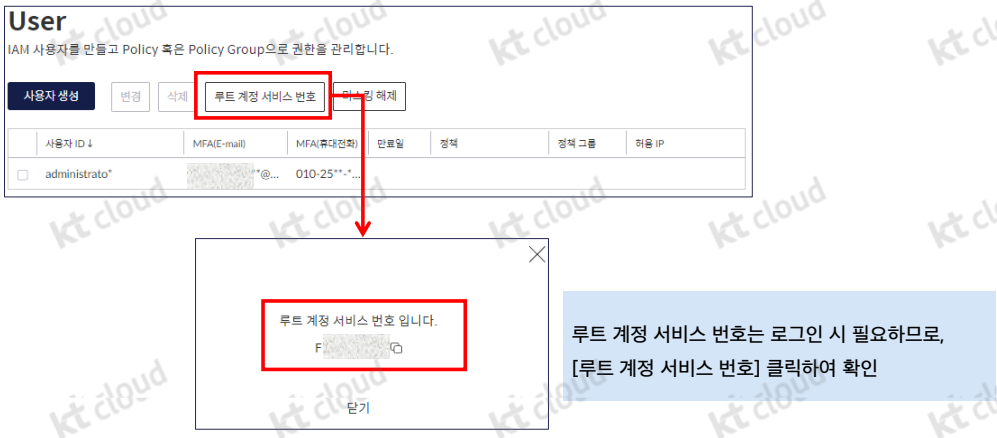
IAM(Identity and Access Management)은 하나의 계정에 청약된 서비스 및 리소스에 대한 접근 및 제어 권한을 개별 사용자 별로 부여하는 서비스입니다.
루트계정을 가진 사용자는 IAM 메뉴를 통해 업무별로 사용자 계정을 만들고 업무에 맞게 권한을 부여합니다.

1-2. 사용자 계정 만들기



[IAM]-[User] 메뉴에서 사용자 생성을 클릭하여 계정을 하나 만듭니다.
여기서는 **Administrator**를 생성합니다.

1-3. 사용자 계정 확인



루트 계정 서비스 번호는 로그인 시 필요하므로,
[루트 계정 서비스 번호] 클릭하여 확인

IAM에서 만든 계정이 로그인하기 위해서는 서비스 번호가 반드시 필요합니다. [루트 계정 서비스 번호]를 클릭하여 **서비스 번호**를 메모해 둡니다.

1-4. 정책 생성

계정만으로는 콘솔에 접근하더라도 아무런 작업을 할 수가 없습니다.
작업을 위한 최소의 권한은 계정에게 부여해야 하는데, 이때 권한들을 정책이라고 합니다.
부여할 정책들은 미리 정의를 해 둡니다.
[IAM]-[Policy]를 선택하고, [정책 생성]버튼을 클릭합니다.
정책명과 각 **서비스/서브 서비스**에 대한 **작업**, 대상 **리소스** 등을 지정하여 추가합니다.

여기서는 다음의 정책을 생성해봅니다.
(명칭은 한글과 영문이 혼용 가능합니다.)

- **Server Operation** : 서버를 운영하기 위한 권한 (서버 - 재부팅, 정지, 시작)
- **Server Admin** : 서버 관련 전체 권한 부여 (서버-전체 작업)
- **DB Admin** : DB 관리를 위한 권한과 Server 작업 권한 (서버-전체 작업, DB-전체 작업)
- **Network LB 권한** : 로드밸런서 서비스 관리 권한 (로드밸런서-전체 작업)
- **Network 웹방화벽 권한** : 웹 방화벽과 관련된 전체 권한 (웹방화벽-전체 작업)

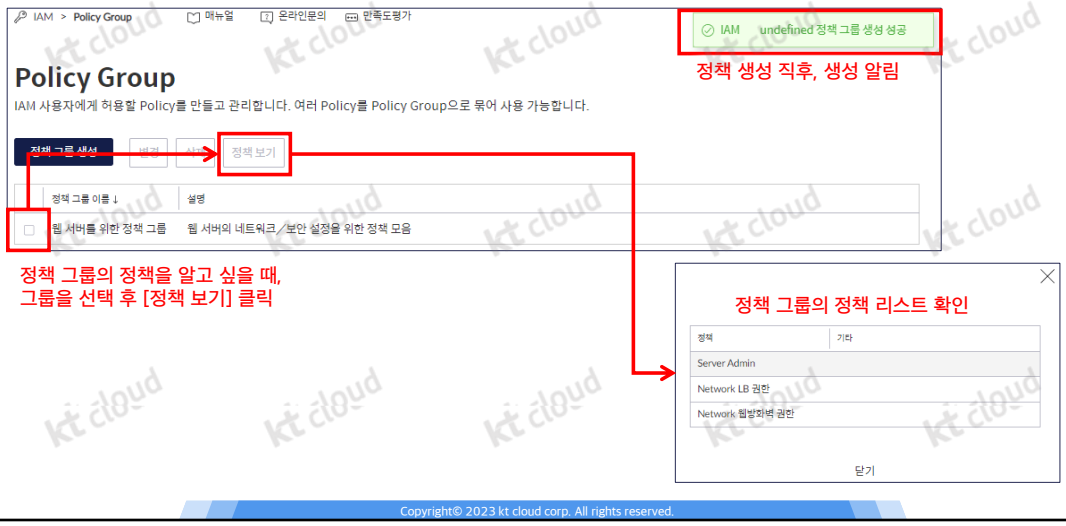
1-5. 정책 그룹 생성

여러 정책들을 묶어서 그룹으로 관리할 수 있습니다.
[IAM]-[Policy Group]에서 [정책 그룹 생성]을 클릭하면 기존에 정의된 정책들의 목록을 볼 수 있습니다.

관련 있는 정책들을 묶어서 하나의 그룹으로 관리하므로,
웹서버 관리자라는 가정하에 다음의 정책 그룹을 생성합니다.

- 정책 그룹 이름 : **웹 서버를 위한 정책 그룹**
- 적용할 정책 : **Server Admin, Network LB 권한, Network 웹방화벽 권한**

1-5. 정책 그룹 생성 후 확인



생성된 정책 그룹에 어떠한 정책들이 있는지 확인하기 위해서는
정책 그룹을 선택한 후, [정책 보기]를 클릭하면 정책 목록을 볼 수 있습니다.

웹 서버를 위한 정책 그룹을 선택하고 [정책 보기]를 클릭하여 속해 있는 정책들을 확인해 봅니다.

이제 사용자에게 정책을 매핑해 봅니다.
administrator를 선택하고 [변경]을 클릭하여 정책을 매핑하는데, 사용자 정보는 민감하므로 마스킹이 되어 있습니다. 따라서 [마스킹 해제]를 클릭하여 마스킹을 해제한 후 [변경]을 클릭합니다.

여기서는 **administrator**에게 아래 권한을 적용합니다.

- 정책 : **Server Admin, DB Admin**
- 정책 그룹 : **웹 서버를 위한 정책 그룹**

1-7. 사용자 감사

[IAM]-[Audit(User)] 메뉴는 사용자가 특정 기간동안 어떠한 작업들을 했는지 볼 수 있습니다.
콘솔에서의 작업 이력 조회 뿐 아니라, 리포팅을 위한 엑셀 다운로드 및 사용자/기간 별 조회가 가능합니다.

1-8. IAM 사용자 로그인

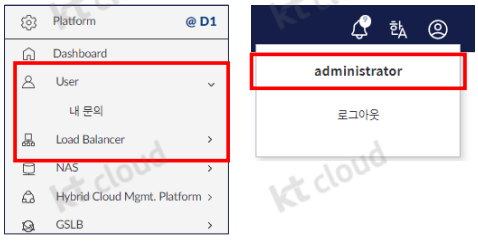
① IAM 사용자 클릭
② 사용자 정보에서 복사해 둔 서비스 번호 입력
③ 사용자 ID/비밀번호 입력

(MFA 설정 시)
① 설정한 전화번호/E-mail 중 선택, [OTP 발송] 클릭
② 받은 6자리 번호 입력 후, [인증] 클릭

이제 생성한 Administrator로 로그인해 보겠습니다.
로그인 화면에서 [IAM 사용자]탭을 클릭하고, 메모해 두었던 서비스 번호와 사용자 ID, 비밀번호를 입력합니다.
클라우드에서 사용자 정보는 민감하고 중요한 정보이므로, 가급적 로그인 시에 MFA를 통해 비밀번호 외에 추가 정보를 인증 받아 로그인 하는 것을 권장합니다.
사용자 생성시 MFA 정보를 지정했다면, 이를 통해 인증을 한번 더 하도록 합니다.

1-9. IAM 사용자 권한 확인

<일반 사용자 클라우드 콘솔>



일반 사용자의 경우,
- 관리 콘솔의 메뉴에 IAM 메뉴와 User 메뉴의 결제 정보 등이 없음
- 우측 상단에 로그인한 계정의 ID를 확인

<일반 사용자 권한 제한>

사용자에게 할당된 권한이 없는 작업을 시도하면,
안내 메시지와 함께 작업 불가

루트 계정과는 다르게 로그인했을 때 사용자 콘솔의 메뉴가 다른 것을 확인할 수 있습니다.
좌측 메뉴에서 IAM 이라는 항목이 없으며, User 항목과 그 하위 결제정보나 문의, 그룹 계정 등이 없습니다. 이러한 항목은 루트 계정만이 관리하도록 하므로 일반 IAM 사용자는 메뉴 자체가 없습니다.

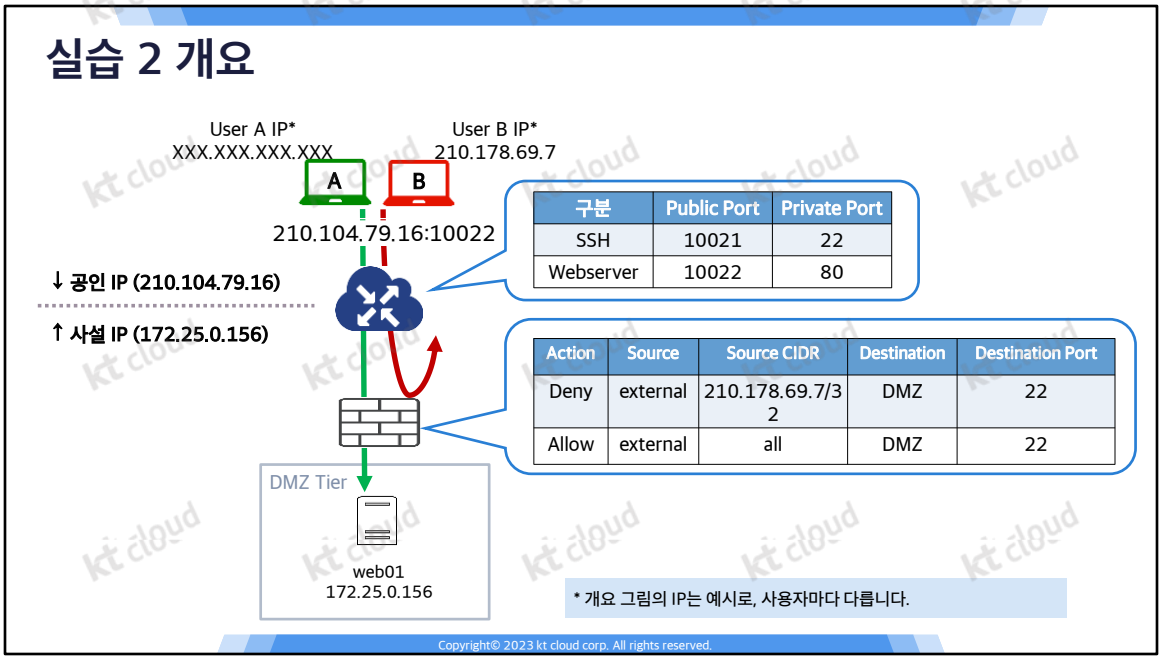
앞서, Administrator 계정에게 다음의 권한을 부여했습니다.
- 정책 : **Server Admin, DB Admin**
- 정책 그룹 : **웹 서버를 위한 정책 그룹**

그 정책과는 무관한 다른 서비스에 대한 작업에 제한이 있습니다.
이전 네트워크 실습과 같이 Tier를 생성하고자 하면
버튼은 보이지만, 실제 눌렀을 때 권한이 없다는 창이 뜨는 것을 확인합니다.

실습 2. 네트워크 보안 제어

01 접속 설정하기

02 방화벽 설정하기



실습 2에서는 네트워크 보안과 관련된 실습을 해보겠습니다.
기존의 실습에서 많이 접했던 접근 권한과 방화벽 설정에 대한 부분으로,
이미 많이 접했던 서비스입니다.
우리가 서비스를 구성하고 외부에서 접근할 수 있도록 하기 위해 필요한 것이
이 **접근 권한**과 **방화벽**입니다.
접근 권한은 외부에서 접근할 수 있도록 공인 IP의 특정 Port를 내부 서비스의 사설IP와 서비스 포트로 연결 시켜주는 역할을 합니다.
방화벽은 어떤 포트로 접근하는 요청을 허용해 줄 것인가와 관련된 제어 서비스입니다.
실습 2에서는 먼저 접근이 가능하도록 구성을 한 다음,
내 IP를 허용 거부하도록 설정하고 나서 다시 접근하여 어떻게 달라지는지 보도록 하겠습니다.

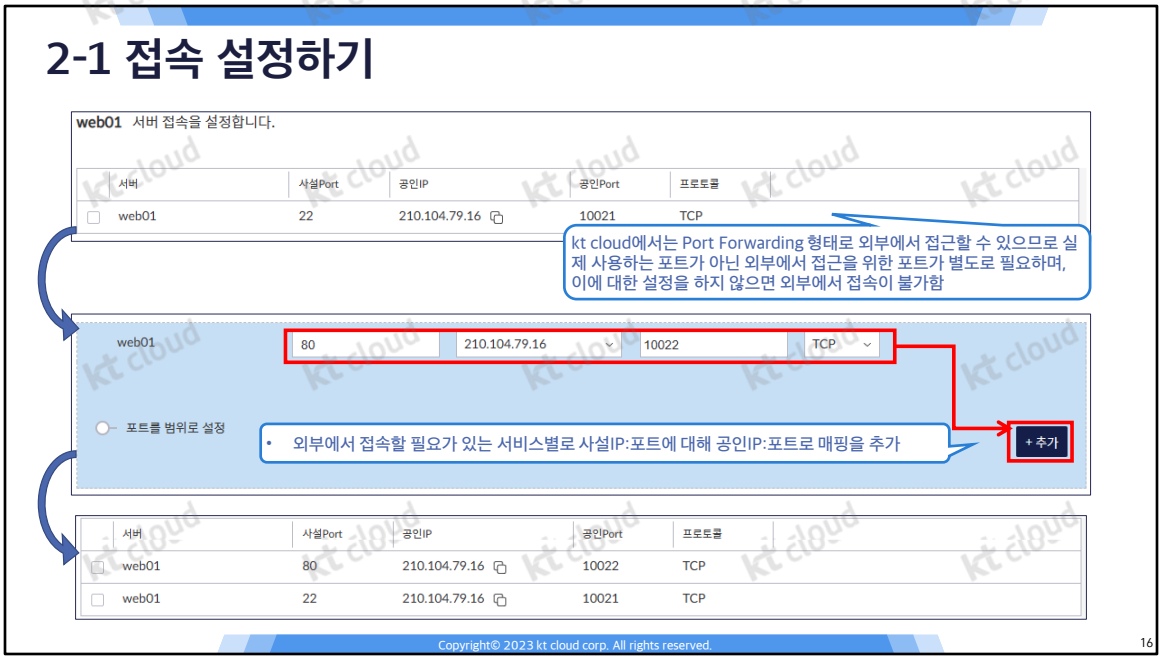
2-1 접속 설정하기

참고

접속 설정은 [Server] 메뉴와 [Networking]메뉴 둘 다에서 확인할 수 있으나,
[Server]에서는 해당 서버와 관련된 접속설정만을 보여주고 [Networking]에서는 모든 서버의 접속설정이 보여지므로
여러 서비스들을 제공하는 실 운영환경에서는 [Server]-[Server]메뉴의 접속 설정이 보다 보기 편리함

Network 실습에서 사용했던 **web01**을 이용하겠습니다.
먼저 [Server]-[Server]에서 **web01**이 있는지 확인합니다.
web01은 Network 실습에서 이미 Putty를 통해 접근하였으므로, 기본적인 접근 설정과 방화벽 설정은 되어 있는 상태입니다.

혹시 이 web01을 삭제하였거나, 설정을 마무리 못한 부분이 있다면
Network 실습내용을 확인하여 구성하도록 합니다.



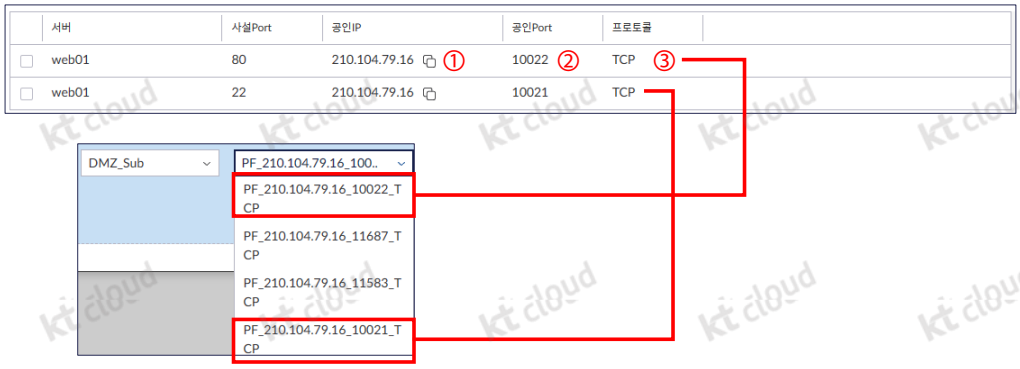
kt cloud에서는 기본적으로 공인 IP의 포트를 이용하여 여러 사설 IP의 Port로 전달하는 형태(Port Forwarding)이며 이것을 구성하는 곳이 [접속 설정] 입니다.

실제 사용하는 포트가 아닌 외부에서 접근을 위한 포트가 별도로 필요하며, 이에 대한 설정을 [접속 설정]에서 하지 않으면 외부에서 접속이 불가합니다.

이전에 22번 포트에 대해 10021번으로 접속하도록 설정을 했었습니다.
혹시 웹서비스를 하고자 한다면 웹서버가 사용하는 80포트에 대해서도 접속 설정을 추가해야 하며, 이와 같이 서비스별로 별도의 공인포트가 필요합니다.

2-2 접속 설정의 명명법

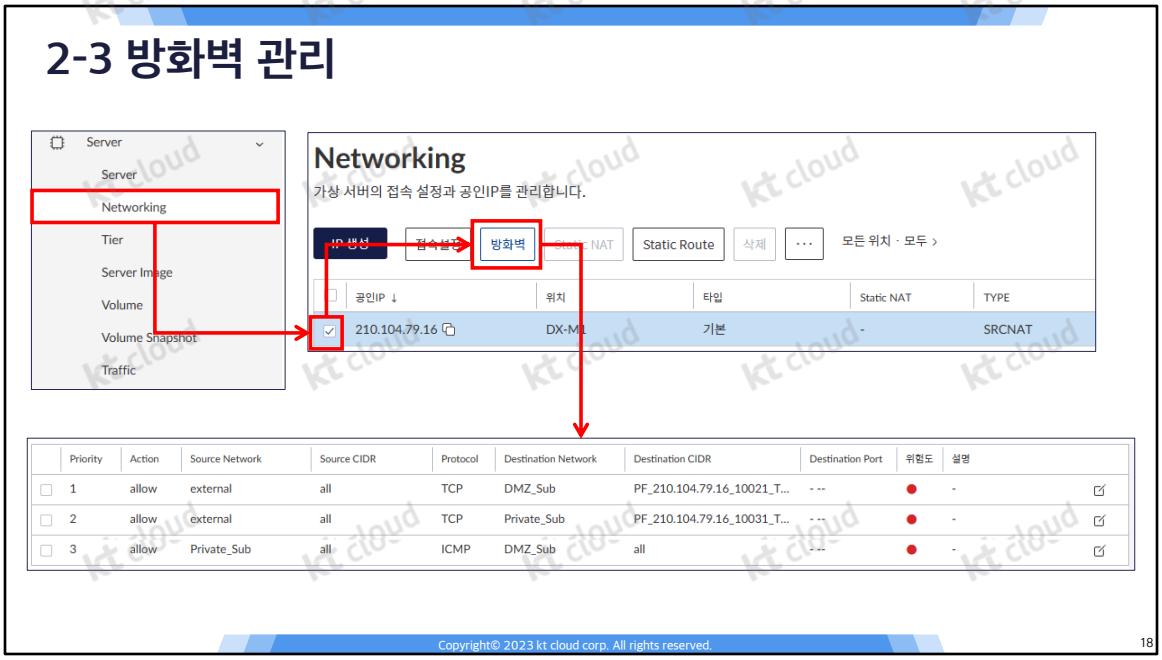
Port Forwarding의 명명: **Prefix_[공인IP]_[공인Port]_[프로토콜]**
→ PF_①_②_③ 이므로, PF_210.104.79.16_10021_TCP



[접속 설정]에서 추가한 목록은 이후에 방화벽 설정 등에서 drop-down 형태로 보여집니다.
명칭은 우리가 지정하지 않고 자동으로 다음과 같이 정해집니다.

PF_공인IP_공인Port_프로토콜

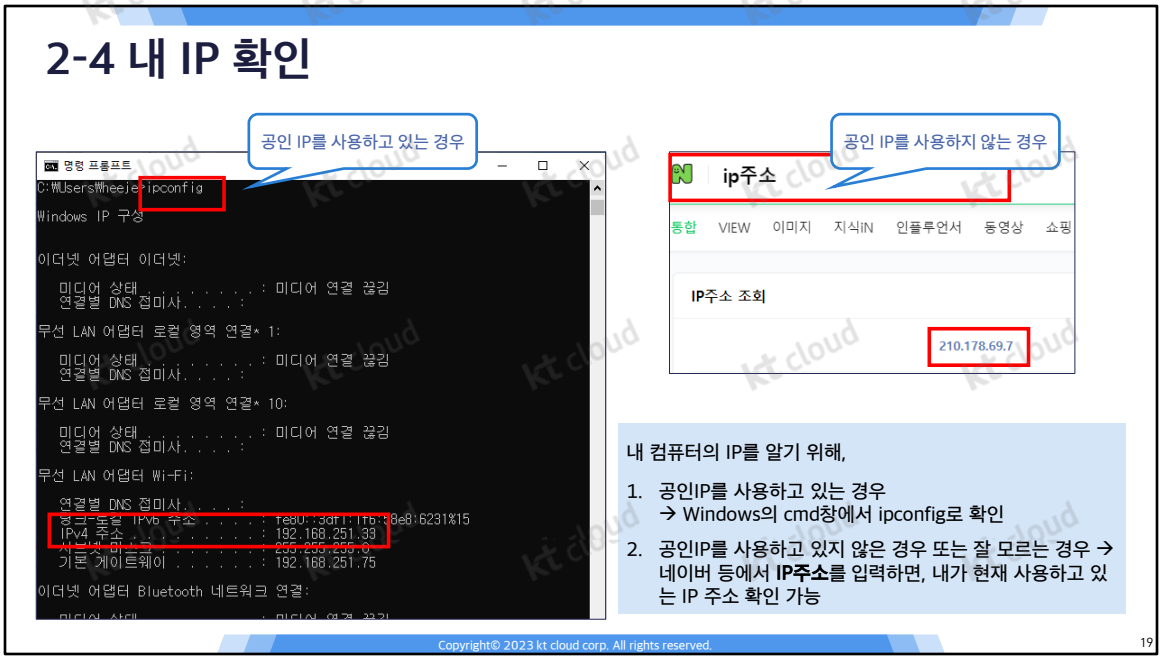
Drop-down 목록에서 접속 설정을 볼 때 이 규칙을 유념해서 각각의 접속 설정이 실제 어떤 것을 지칭하는지 보도록 합니다.



[Server]-[Networking]에서 방화벽 설정을 합니다.
[Networking]은 공인 IP를 기준으로 관리가 되므로, 먼저 내가 접근(사용)할 공인 IP를 선택하고 [방화벽]을 클릭합니다.

Network 실습을 모두 마무리 했다면 하단과 같이 세 개의 방화벽 설정이 있습니다.
이 세 개의 방화벽 설정은 모두 Allow 정책으로, 외부에서 22번 포트로의 접근은 모두 허용하고 있습니다.

여기서는 이제 22번 포트에 대해 내 IP가 접근하는 것을 막아보도록 할 것입니다.



접근을 막기 위해 먼저 내 IP를 확인하겠습니다.

사용하고 있는 IP가 공인 IP를 사용하고 있다면, Windows에서는 cmd창에서 **ipconfig**를 이용해서 확인할 수 있습니다.

그러나, 대부분 공인 IP의 제한으로 인해 사설 IP를 할당 받아 사용하는 경우가 많고, 공유기를 이용하여 인터넷을 사용하거나, Mobile의 핫스팟 등으로 연결하고 있는 경우가 많은데 ipconfig를 이용한 확인은 외부에서 인식하는 공인 IP가 아닌 사설 IP를 보여줄 수 있으므로 다른 방법을 이용해야 합니다.

간단하게는 Naver나 Daum 등에서 '**IP 주소**' 또는 '**내 IP**'등을 입력하면 확인이 가능합니다.

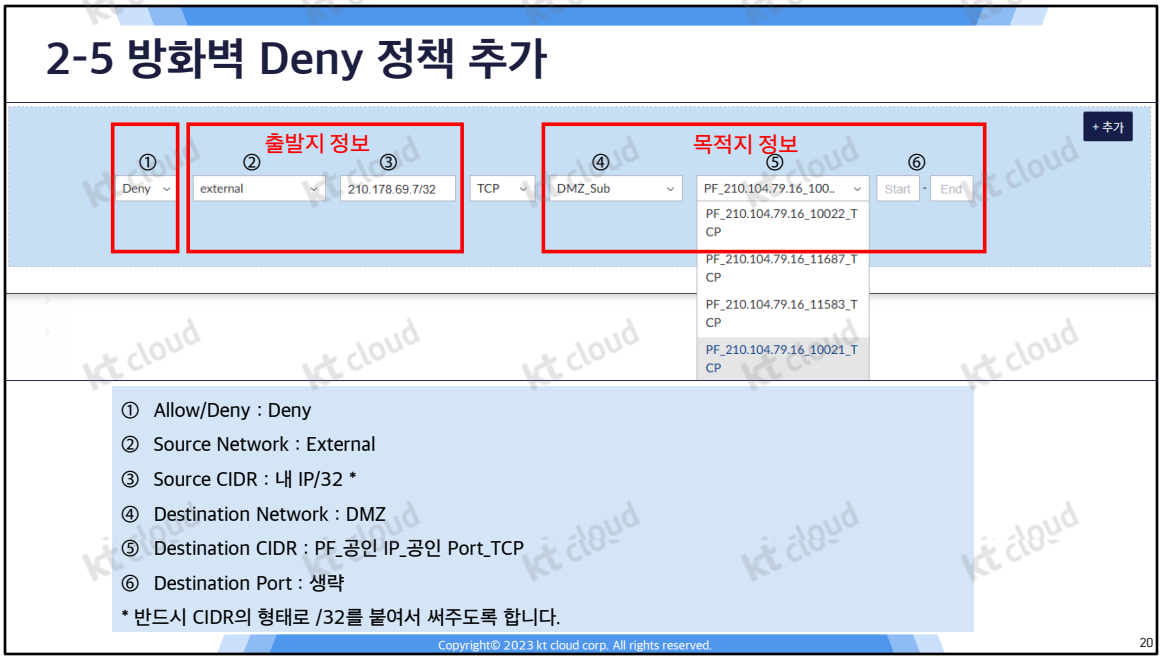
그 외에 다음 사이트에서 확인할 수 있습니다.

- www.whatismyip.com
- www.findip.kr

참고로 linux의 경우는 다음의 curl 명령으로 알 수 있습니다.

- curl ident.me
- curl ifconfig.me

- curl icanhazip.com



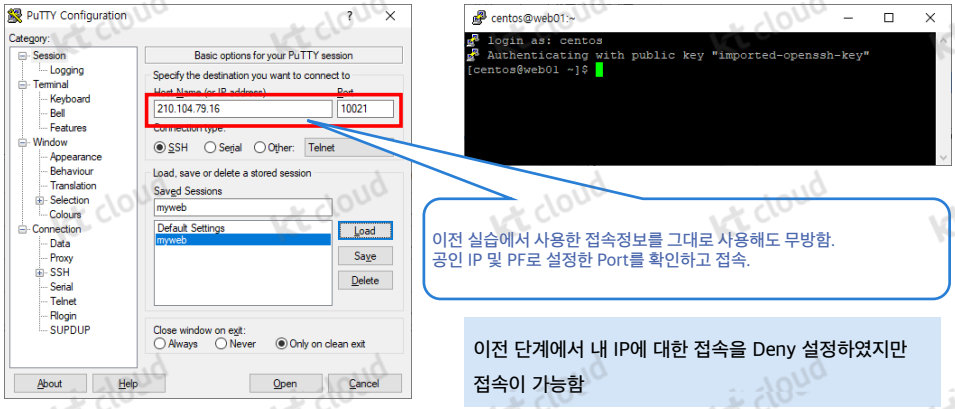
내 IP를 확인했으면 이제 방화벽에 Deny 정책을 추가해봅니다.
다음의 순으로 입력합니다.

① Allow/Deny 구분 : 기본은 All Deny
② Source Network : 외부에서 접근하므로 External
③ Source CIDR : 이전 단계에서 확인한 내 IP. 하나의 IP만을 지정하더라도 반드시 /32까지 입력
④ Destination Network : web01이 있는 DMZ
⑤ Destination CIDR : web01의 22번 포트의 PF 이름
⑥ Destination Port : 범위로 입력하며, 단일 Port는 같은 숫자 입력. PF의 경우 생략가능

2-5 방화벽 Deny 정책 추가

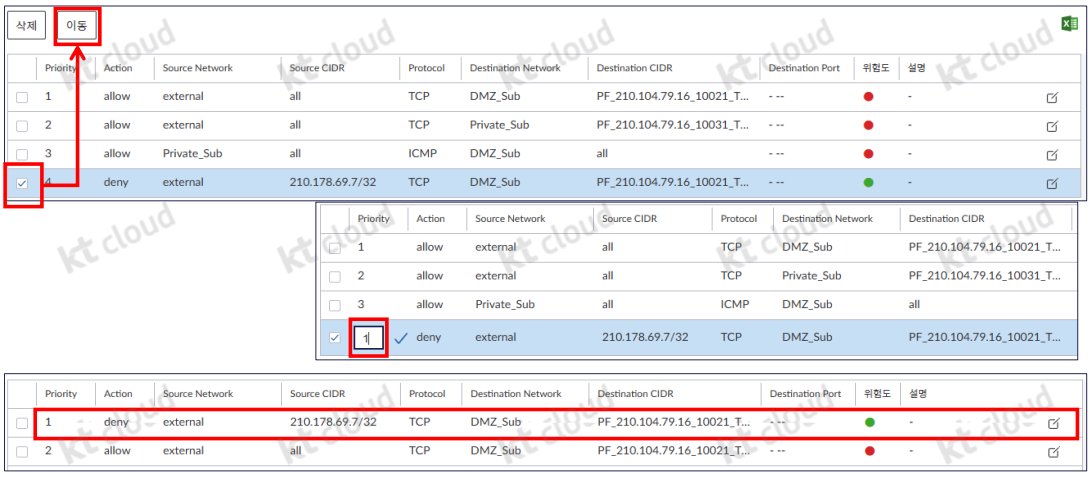
정책이 추가되면 우측 상단에 연두색 알림이 뜨고 방화벽 목록에 추가된 정책을 볼 수 있습니다.
이 때 Source CIDR 값이 명시되어 위험도가 초록색입니다.

2-6 접속 테스트



Putty를 이용하여 web01에 접속해 봅시다.
이전 실습에서 사용한 Session을 그대로 사용합니다.
방화벽에서 Deny 설정을 하였지만 접속이 가능한 것을 볼 수 있습니다.

2-7 방화벽 정책의 우선순위 변경

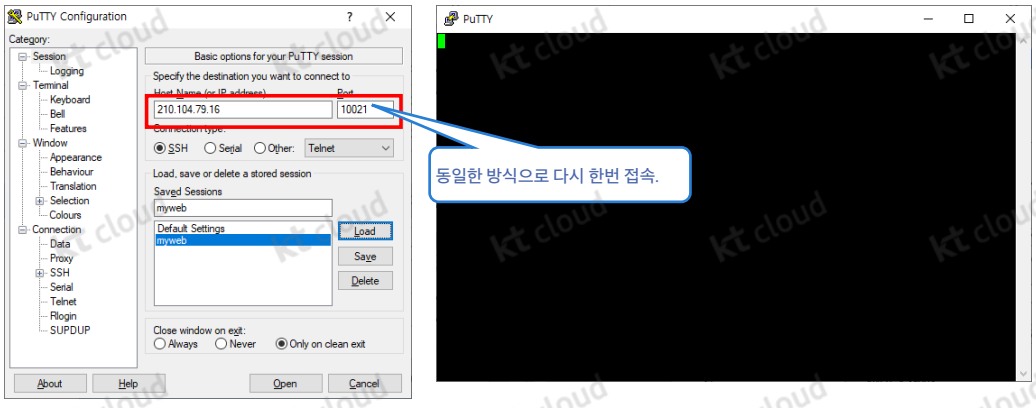


23

이유는 방화벽에서는 우선순위에 따른 순번이 있기 때문입니다.
현재 추가한 Deny 정책은 순번이 1번보다 아래에 있으므로, 1번 정책(10021번으로의 모든 IP에서의 접근을 허용)이 먼저 적용이 됩니다.
추가한 Deny 정책을 우선 적용시키기 위해 [이동]버튼을 눌러서 순번을 변경합니다.
[이동]버튼을 클릭하면 해당 정책의 우선 순위를 입력할 수 있고, 그 옆 파란색 체크를 클릭하면 반영이 됩니다.
지정한 순번으로 정책이 이동하면 그 하위 순번의 정책들은 하나씩 순번이 뒤로 밀려나게 됩니다.

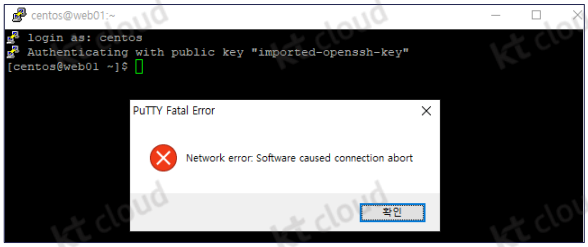
우리는 추가한 Deny정책의 순번을 **1**로 바꾸었으므로 이전에 1번 순위에 있던 정책이 2번으로 바뀐 것을 볼 수 있습니다.

2-8 접속 테스트



이제 다시 2-6과 동일하게 접속을 시도합니다.
같은 설정으로 접속하지만, 접속이 안되는 것을 확인합니다.

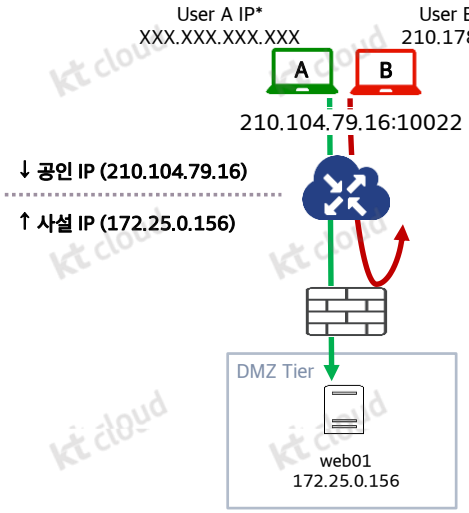
2-8 접속 테스트



만약 접속중인 화면이 있다면, 방화벽 정책이 변경됨과 동시에 더 이상 응답이 없으며 잠시 뒤 Error 창이 뜨는 것을 확인할 수 있음

이전에 접속되어 있던 창이 있다면, 이 화면도 더 이상 응답이 없고 에러창이 뜨는 것을 볼 수 있습니다.
방화벽 설정은 수정한 즉각 반영되며 새로운 접속 외에 기존의 접속 또한 반영한 정책대로 실행되는 것을 확인합니다.

Security 실습 2 요약



요약

네트워크 상의 제어는 크게 접속 설정과 방화벽 설정으로 구분됩니다.

접속 설정

- 공인 IP를 kt cloud 내의 서비스의 사설IP 및 포트로 매핑하는 작업으로, 이러한 접속 설정을 통해서 외부에서 호출이 가능합니다.

방화벽

- 접속 설정을 하더라도 실제 접근에 대한 제어는 다시 한번 방화벽을 거치게 되며, 기본적으로는 Deny 로 간주되므로 Allow 정책을 추가해야만 접근이 가능합니다.
- 접근하는 IP에 따라 제어를 하게 되므로 동일한 서비스에 대해 특정 IP대역의 접근을 막거나, 특정 IP만을 허용할 수 있습니다.
- 여러 정책이 중복하여 적용이 되지만 각 정책의 우선 순위가 있으므로 우선 순위대로 반영됩니다.