사용하기 전에

Q. 네이버 클라우드 플랫폼의 Secure Zone Firewall 서비스는 무엇인가요?

- Secure Zone 내 생성한 인스턴스로의 접근에 방화벽 정책을 설정해 접근을 제어할 수 있는 기능을 제공합니다.
  Q. Secure Zone Firewall 는 어떻게 이용하나요?

- Secure Zone 이용약관 동의
- Secure Zone Fiewall 이용 신청
- Cloud Log Analytics 이용 신청 및 로그 저장소 연동
- Secure Zone VM 생성
- Secure Zone Policy 생성/Address Group 생성
- Secure Zone Firewall Network Usage 조회
- Secure Zone Firewall Log 조회
  Q. Secure Zone Firewall 서비스를 사용하지 않으면 Secure Zone VM 에 접근할 수 없나요?

- Secure Zone 내부 간을 제외한 외부 통신은 모두 차단되어 있습니다.
- 일반 Zone 또는 SSL VPN 과 Secure Zone 간에 Secure Zone Firewall 에 Policy 를 생성하여 통신 허용 정책을 생성해야 Secure Zone VM 에 접근이 가능합니다.
  Q. Secure Zone VM 에 접근 정책을 설정할 수 있는 Zone 은 어디인가요?

- SSL VPN 으로 인입되는 트래픽과 Secure zone 을 제외한 Ncloud 의 모든 Zone 간의 사설 접근입니다.
  Q. Policy 가 뭔가요?

- 정의된 Source IP 와 Destination IP 간에 특정 프로토콜 및 포트에 대한 통신을 허용하거나 차단하는 보안 정책입니다.
  Q. Address Group 이 뭔가요?

- 고객이 소유한 VM 을 원하는 그룹으로 묶어서 정책에서 사용할 수 있도록 하는 오브젝트입니다.
  Q. Log 는 뭔가요?

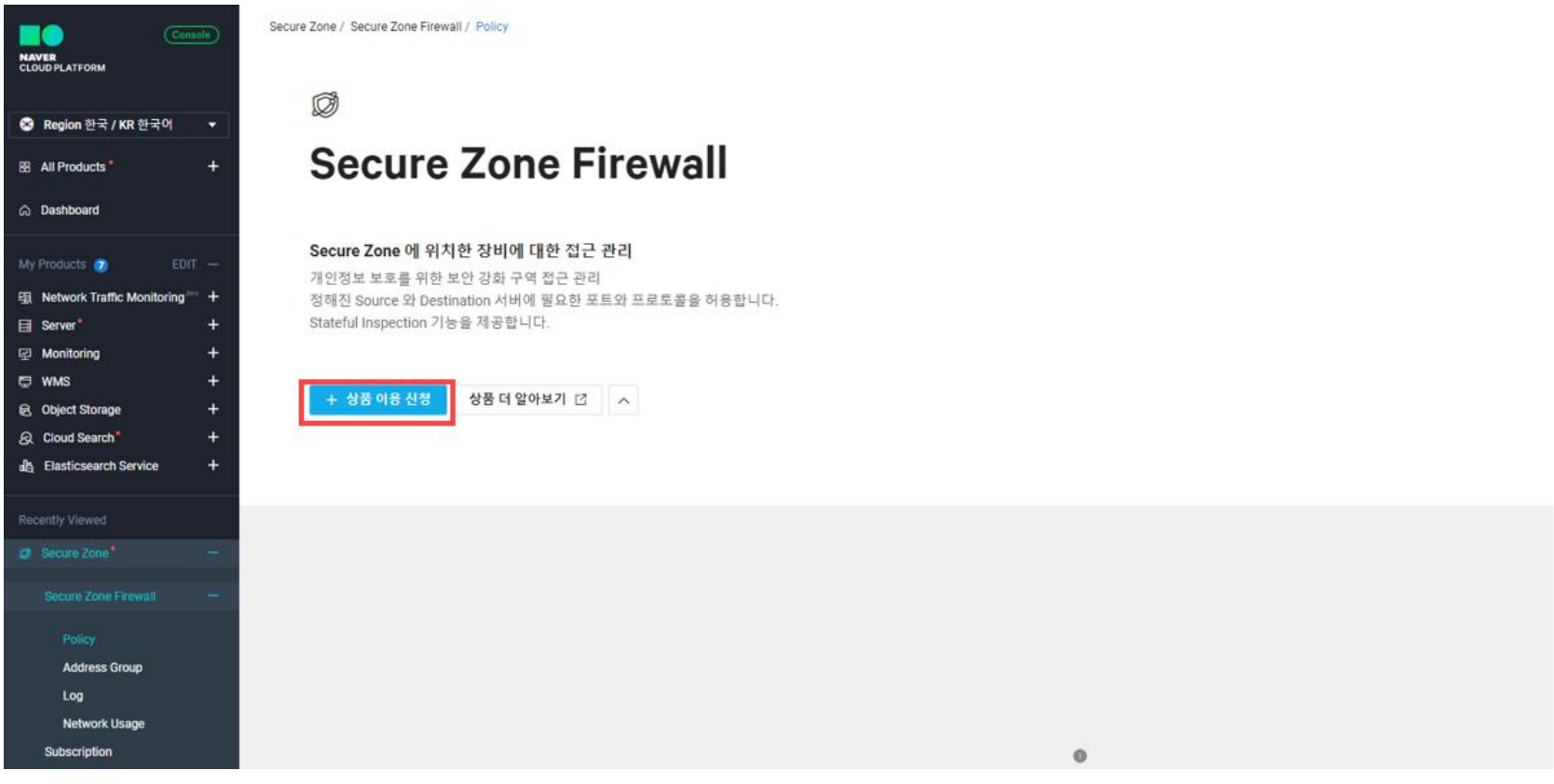
- Secure Zone Firewall 방화벽 정책에 따라 Secure Zone 의 접속 시도가 기록된 Traffic Log 입니다. Cloud Log Analytics 상품에서도 검색/조회가 가능합니다.
  Q. Excel 파일로 다운로드할 수 있나요?

- 검색 결과를 Excel 파일로 다운로드할 수 있습니다.
- 단, 전체 데이터가 아니라 검색 결과 화면에 보이는 내용만 다운로드할 수 있습니다.

Secure Zone Firewall 서비스 사용하기

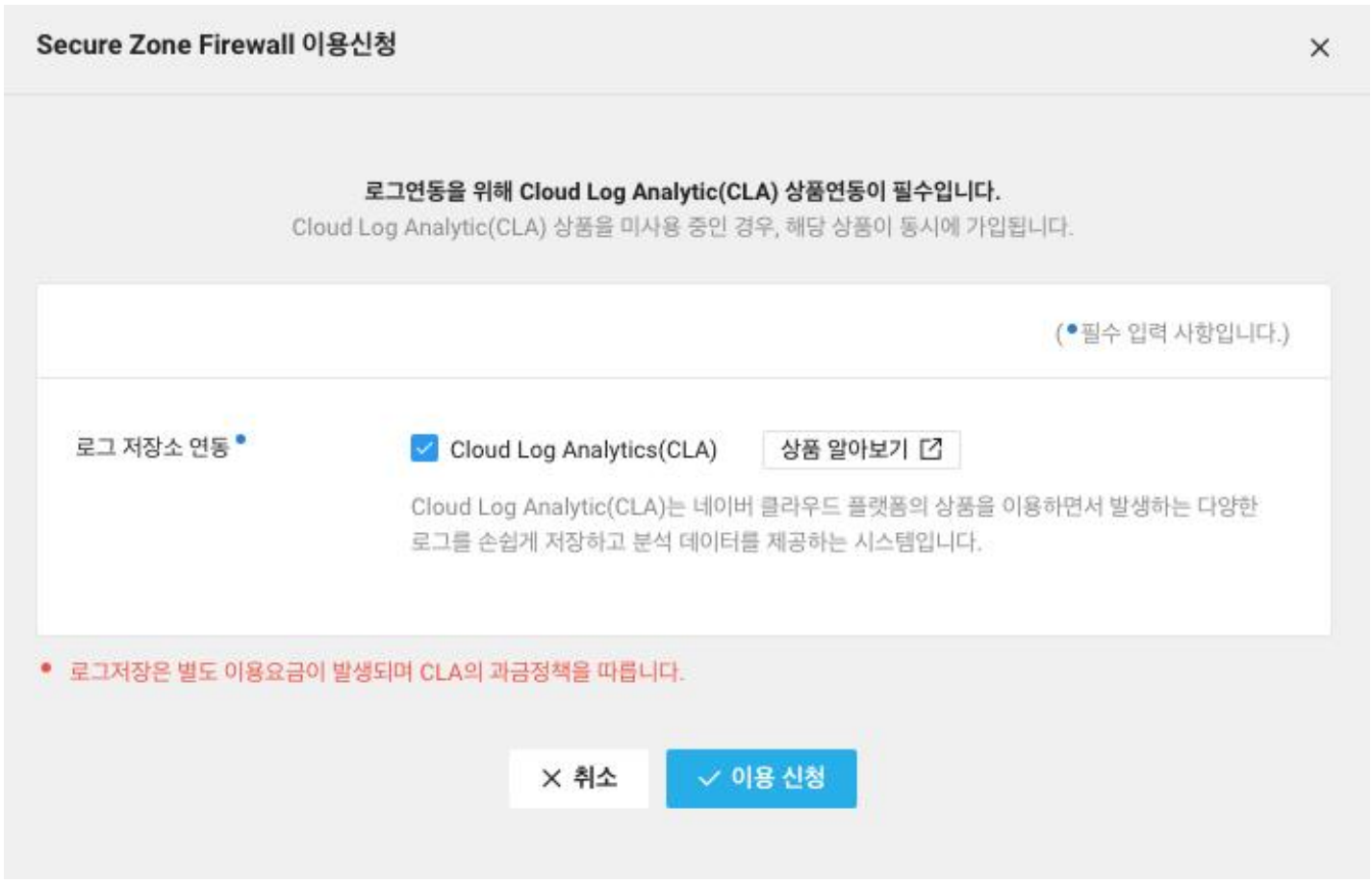
Secure Zone Firewall 서비스 이용 신청

① 콘솔에 접속 후, **Security > Secure Zone > Secure Zone Firewall** 을 클릭합니다.



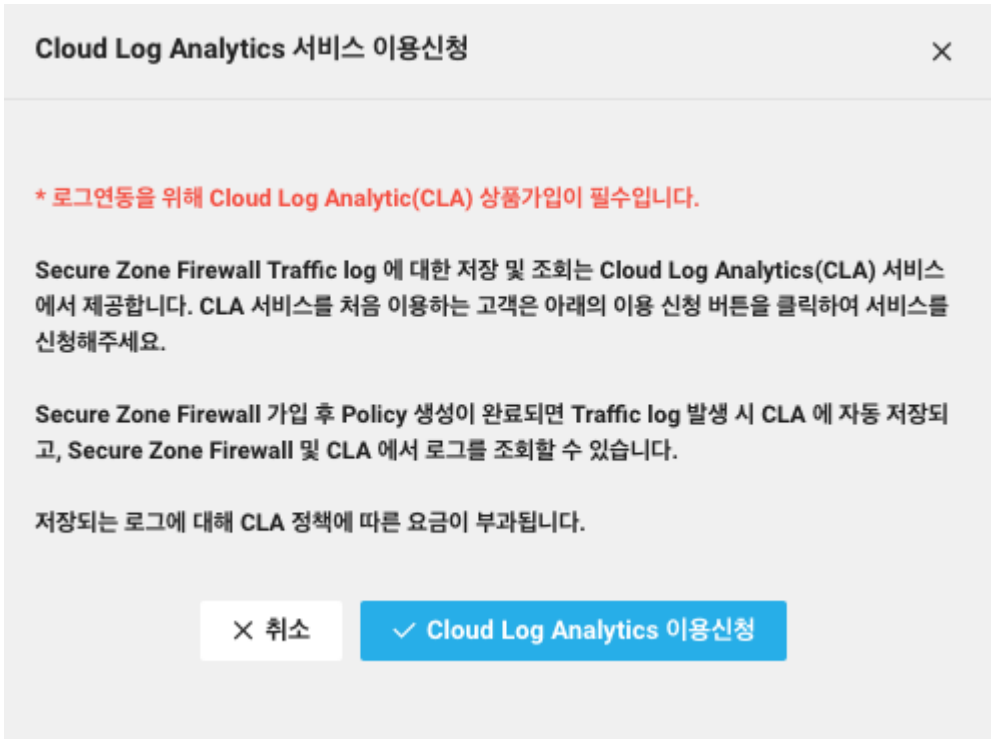
② **Secure Zone Firewall** 하위 메뉴 중 **Policy** 를 클릭합니다.

③ **+ 이용신청** 버튼을 클릭합니다.

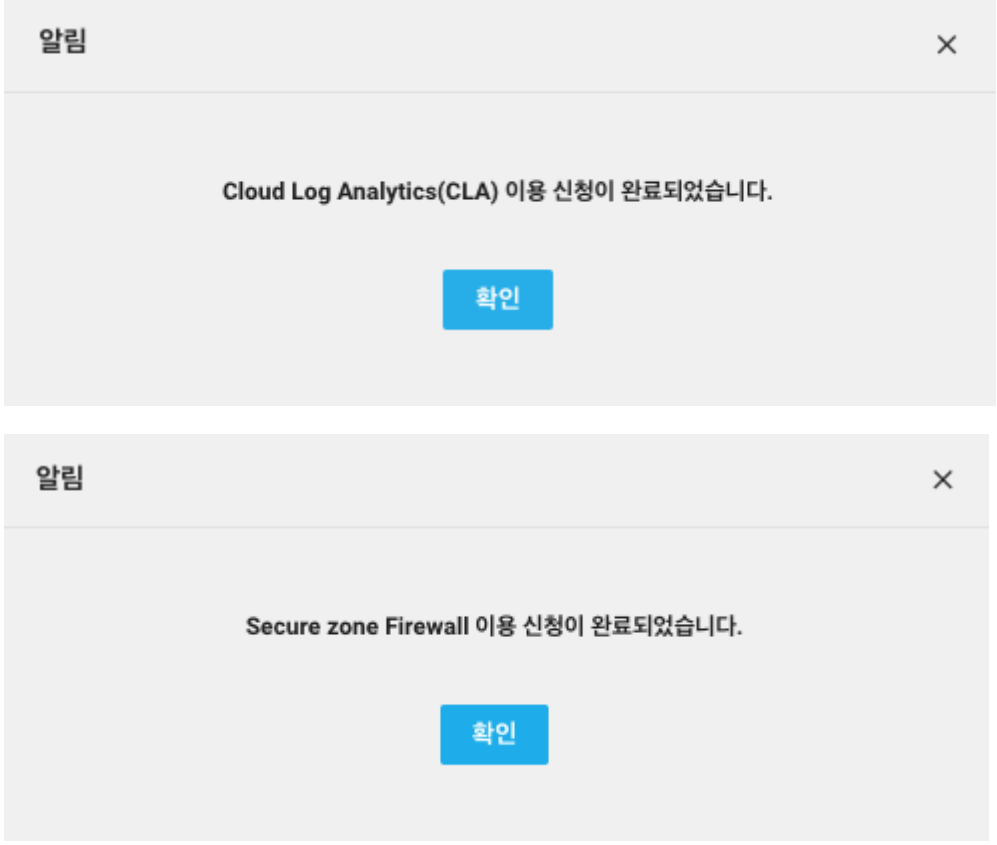


④ **로그 저장소 연동**에서 **Cloud Log Analytics(CLA)**를 선택합니다.(필수)

- 기존 Cloud Log Analytics 가입자에게는 이 팝업 창이 노출되지 않습니다.



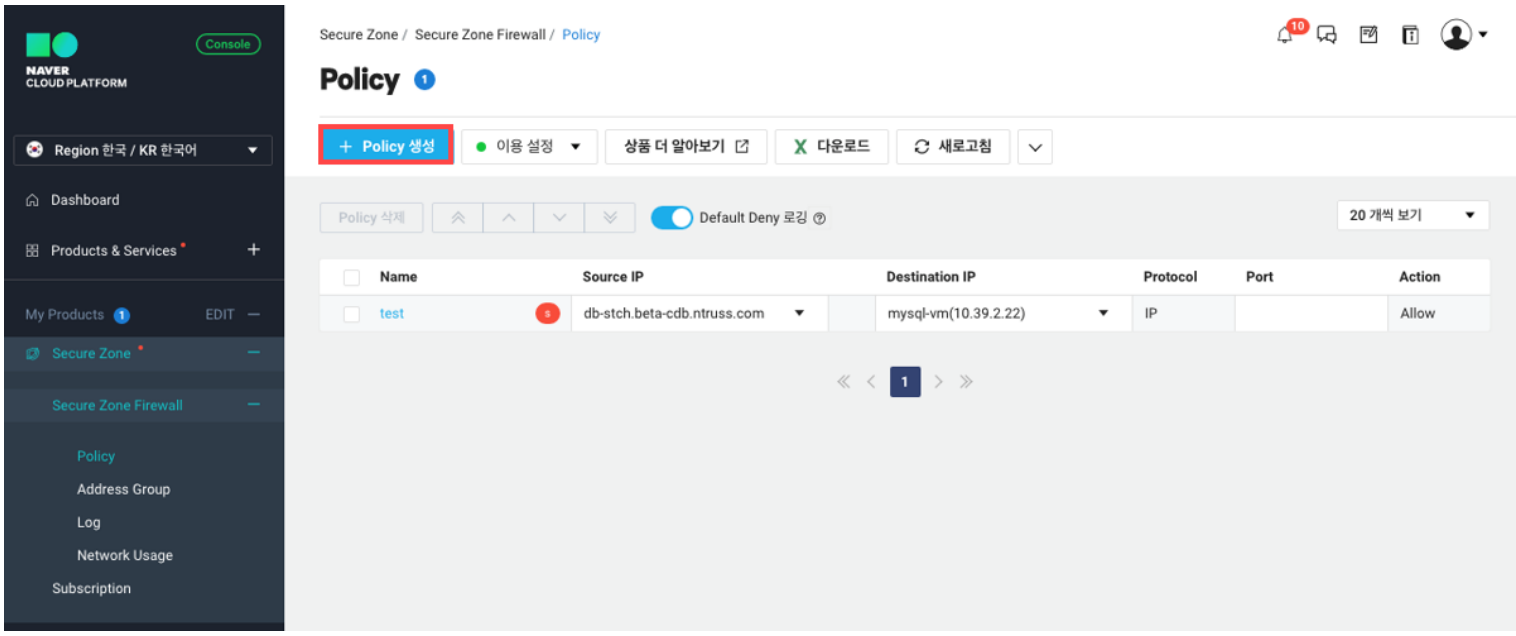
⑤ **Cloud Log Analytics 이용신청** 버튼을 클릭하여 Cloud Log Analytics 서비스에 가입합니다.



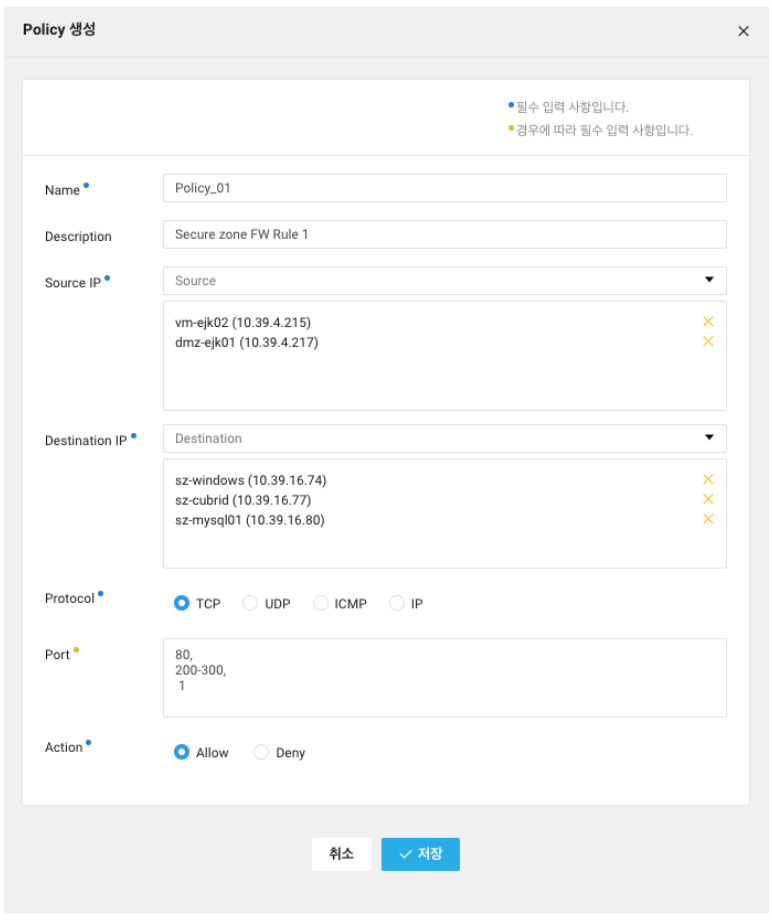
- 미가입 상태일 때 **Policy**, **Address Group**, **Network Usage** 메뉴 선택 시 Secure Zone Firewall 이용 신청 페이지로 이동합니다.

Policy 설정

Policy 생성



① **Security > Secure Zone > Secure Zone Firewall > Policy** 에서 **+ Policy 생성** 버튼을 클릭합니다.

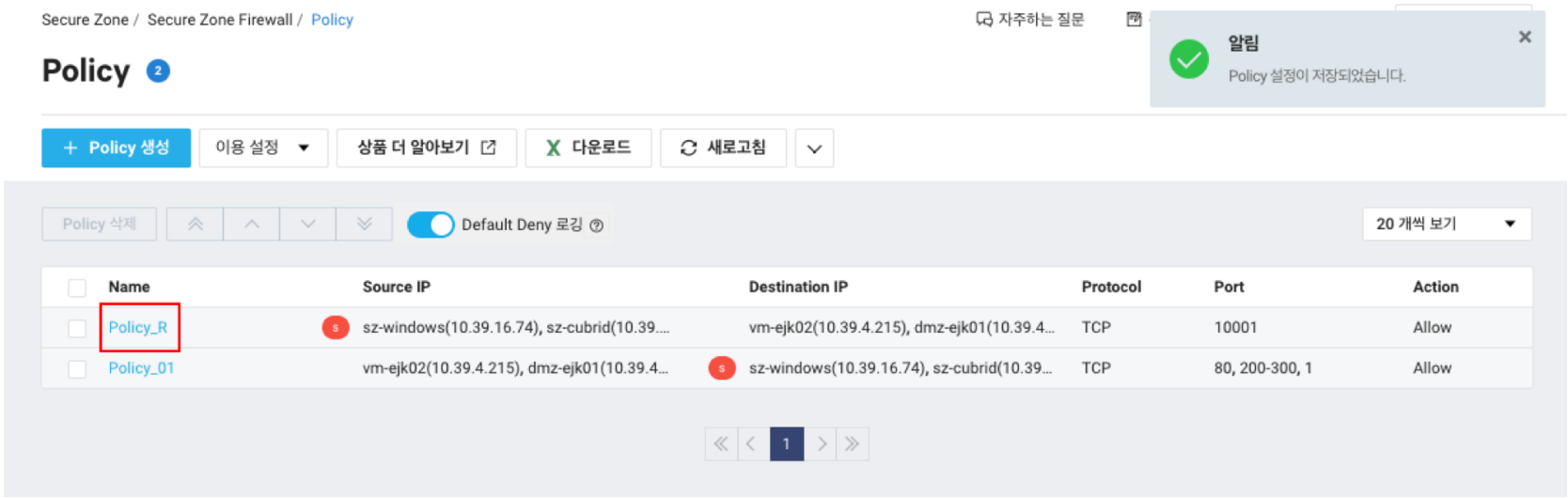


- Name: Policy 이름
- Description: Policy 설명
- Source IP: 고객 소유의 VM / 사설 LB / SSL VPN
- Destination IP: 고객 소유의 VM
- Protocol: TCP / UDP / ICMP
- Port: destination port (0 ~ 65,535)
- Action: Allow / Deny

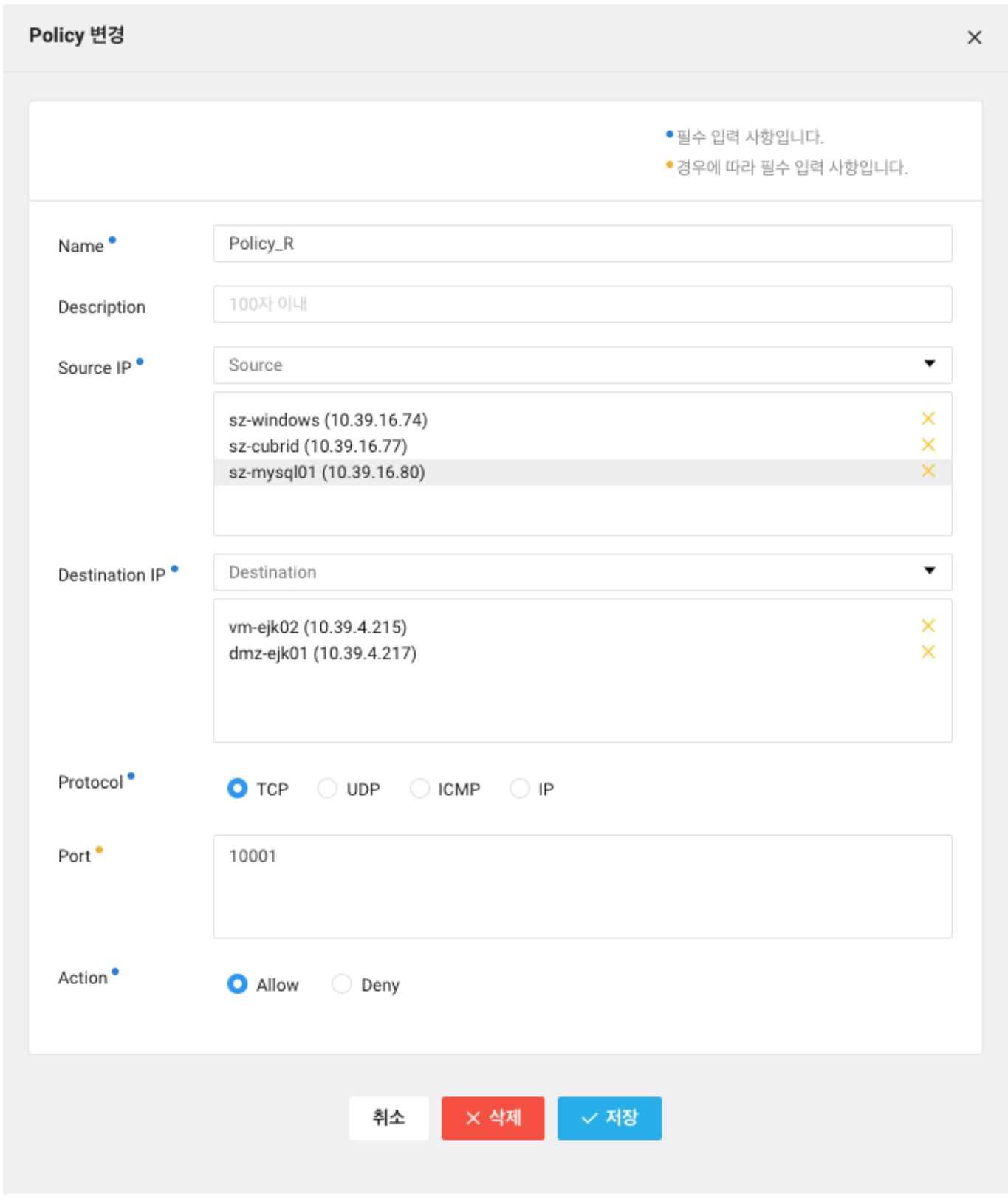
Source IP 와 Destination IP 중 하나는 Secure Zone 필수입니다.

② 필수 값을 입력한 후 **[저장]** 버튼을 클릭하여 Policy 를 생성합니다.

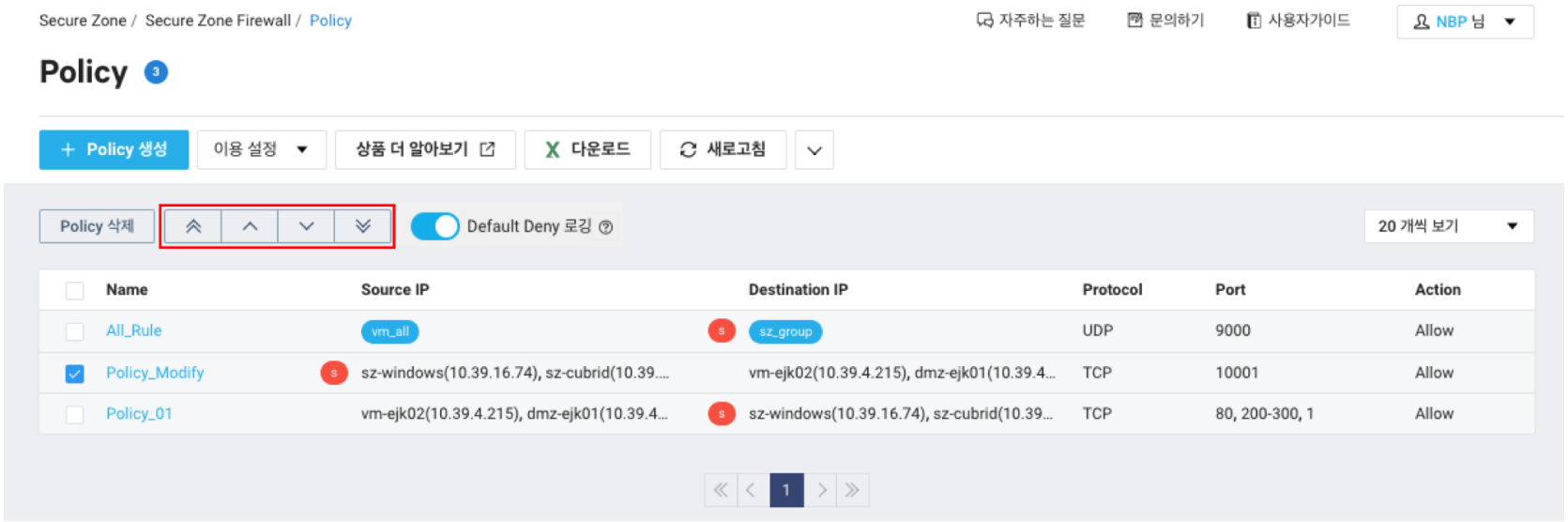
Policy 변경



① **Security > Secure Zone > Secure Zone Firewall > Policy** 에서 변경하고자 하는 Policy 의 Name 을 클릭합니다.

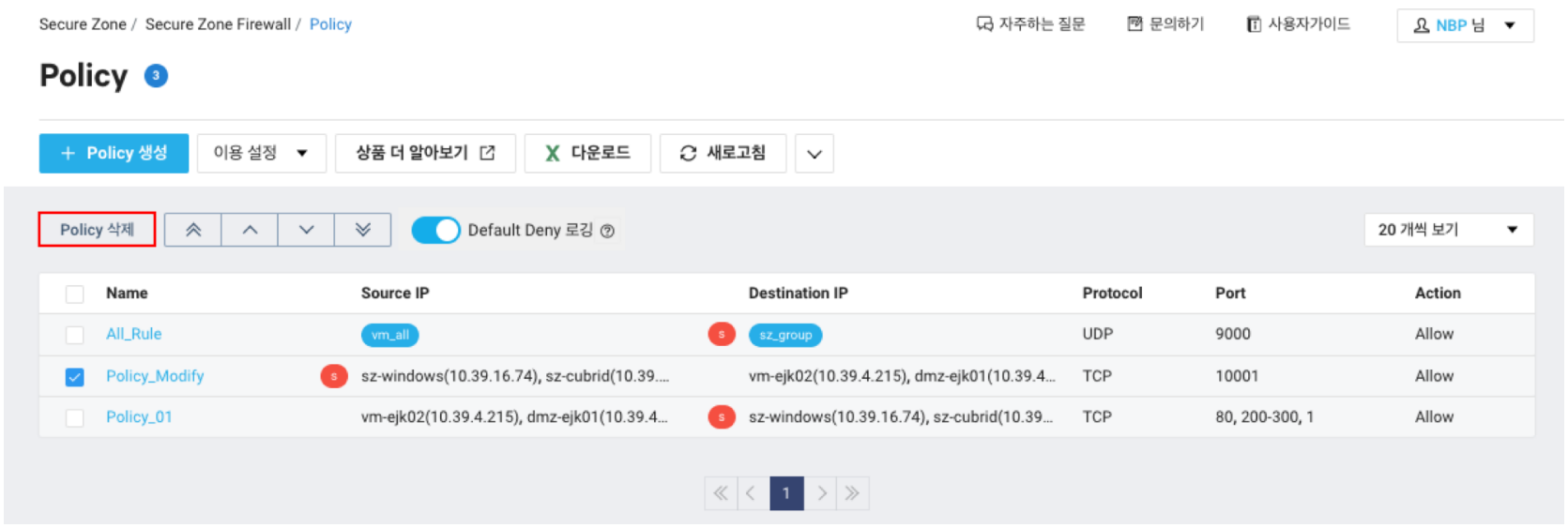


② 변경하고자 하는 값을 넣어 수정 후 **저장**을 클릭하여 Policy 를 변경합니다.

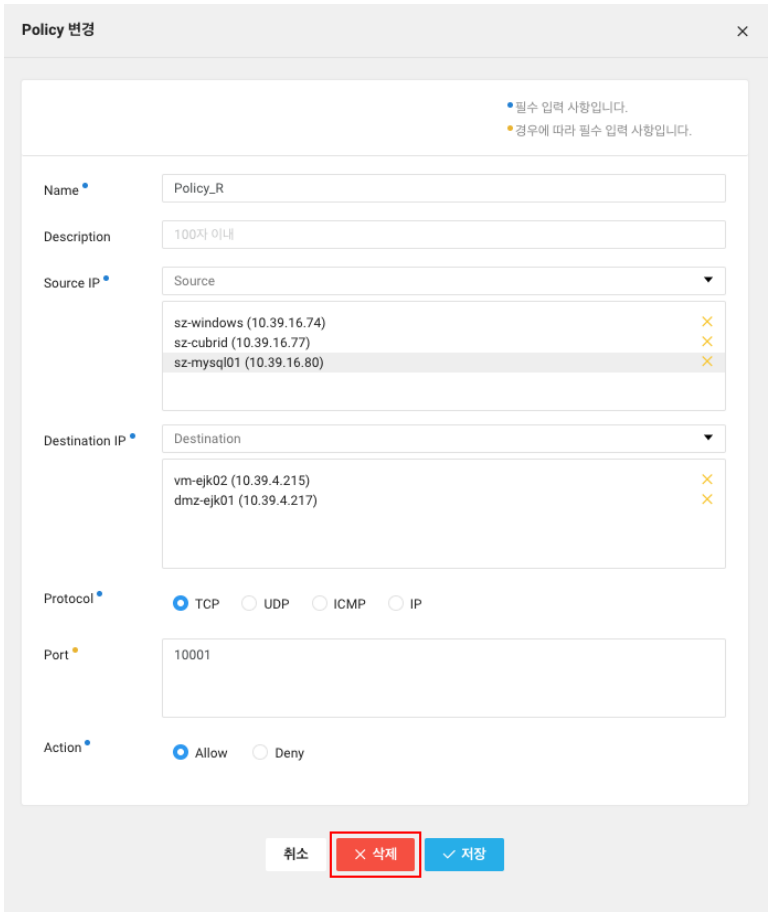


③ Policy 우선순위를 수정하기 위해 Policy 하나를 선택하여 순서변경 버튼으로 우선순위를 조정합니다.

Policy 삭제



① **Security > Secure Zone > Secure Zone Firewall > Policy** 에서 삭제하고자 하는 Policy 의 콤보박스를 다중 선택 후 **Policy 삭제** 버튼을 클릭하여 삭제합니다.



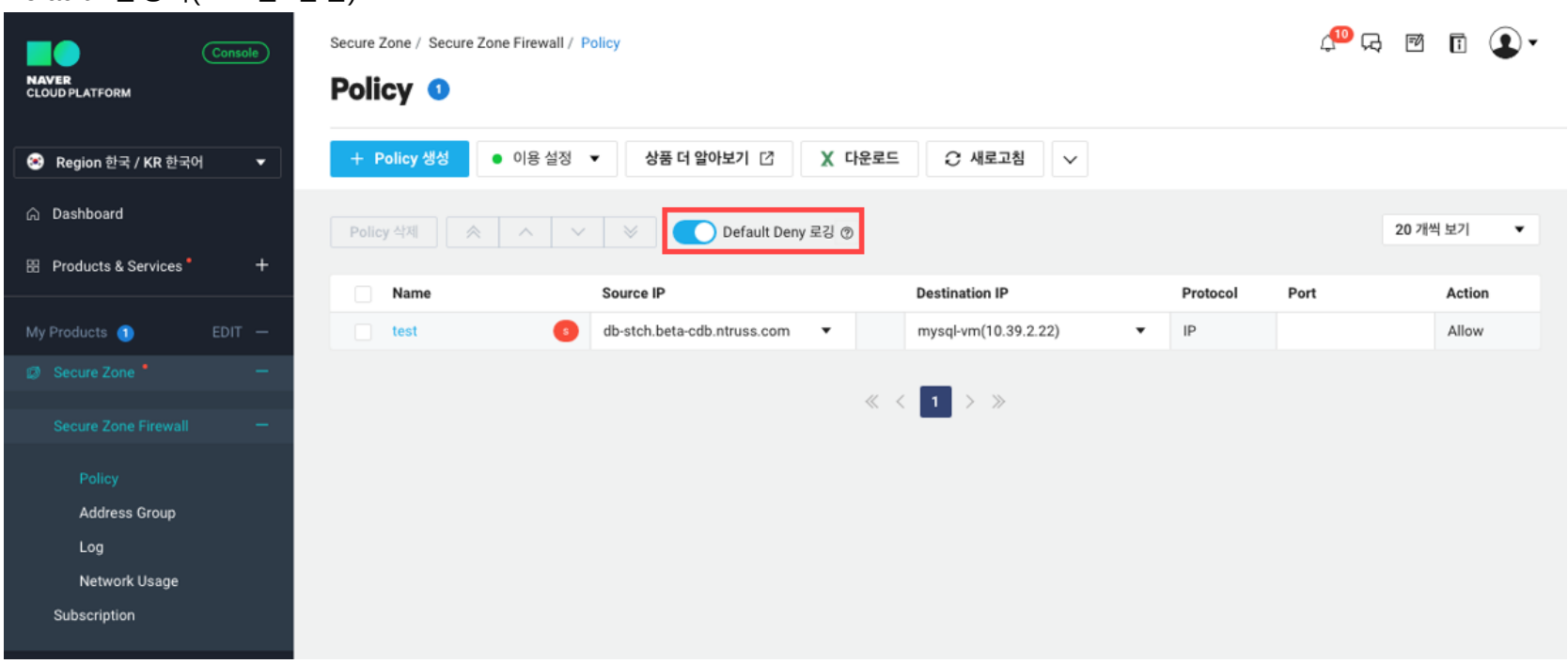
② **Security > Secure Zone > Secure Zone Firewall > Policy** 에서 삭제하고자 하는 Policy 의 Name 을 클릭한 후 **[삭제]** 버튼을 클릭합니다.

Default Deny 정책 로그 활성화/비활성화

기본적으로 방화벽에 정책 설정을 하지 않으면 All Deny 입니다. 아무 정책이 없어서 트래픽이 차단되는 경우 Default 정책에 의해 차단되고 로그가 남는데, 허용되지 않은 접속 시도가 많은 경우 Log Size 가 많이 증가하여 Cloud Log Analytics 저장소 용량을 많이 차지할 수 있습니다.

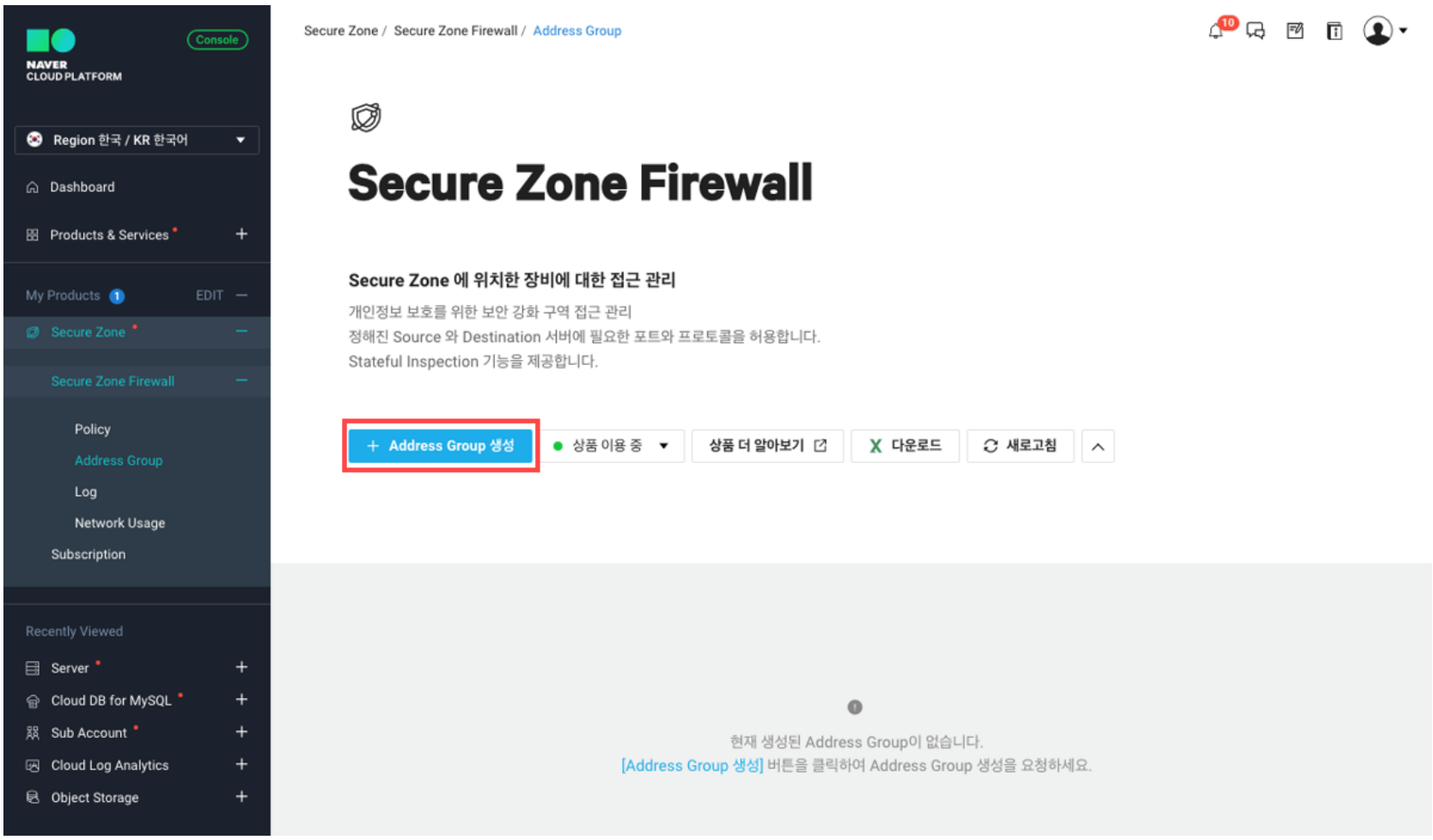
① **Default Deny 로깅**을 활성화/비활성화하여 Default Deny 정책에 해당하는 로그를 남기거나 남지 않도록 설정할 수 있습니다.

- Default: 활성화(로그를 남김)

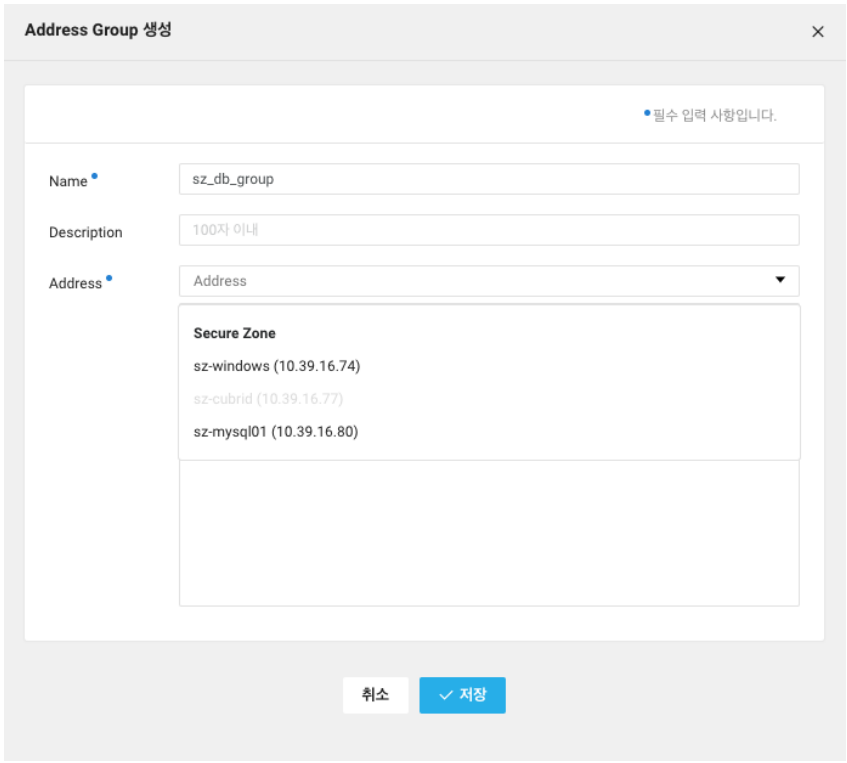


Address Group 설정

Address Group 생성

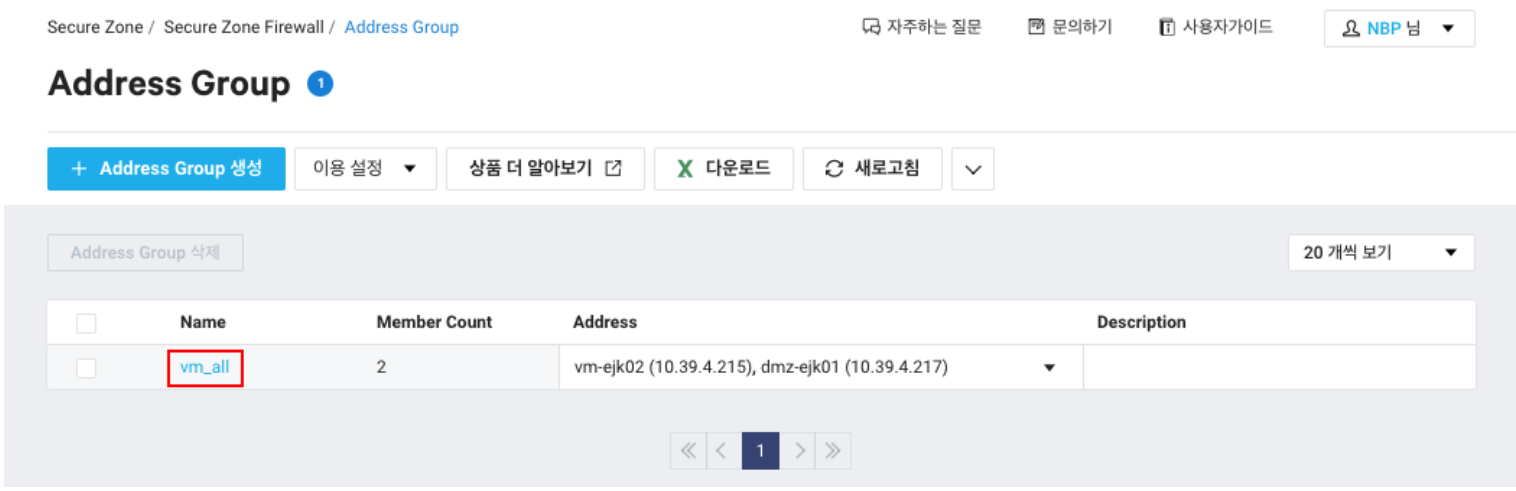


① **Security > Secure Zone > Secure Zone Firewall > Address Group** 에서 **+ Address Group 생성** 버튼을 클릭합니다.

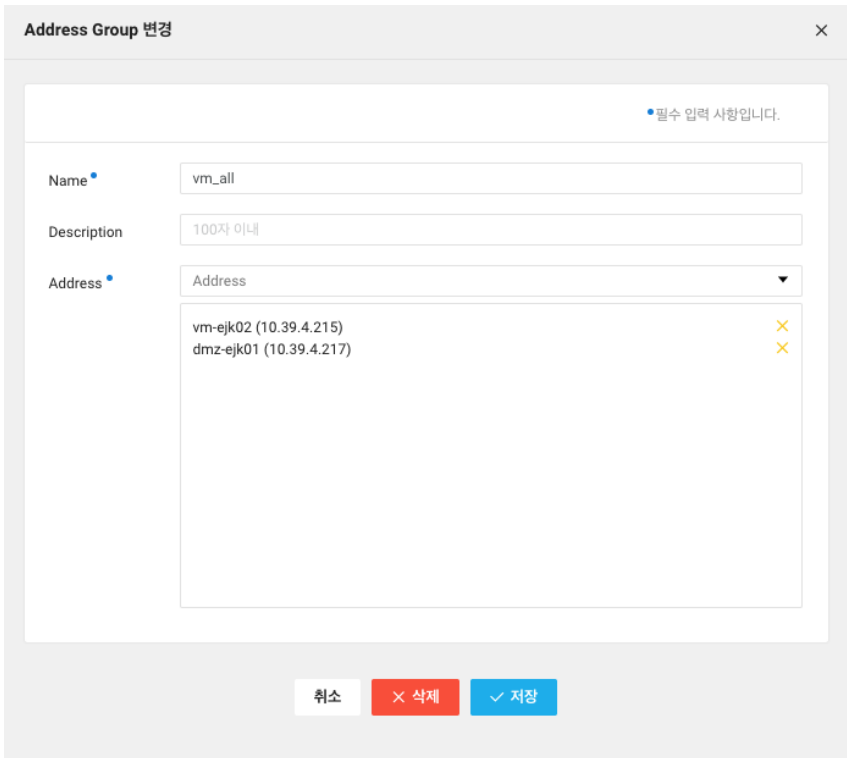


② Address 를 다중 선택하고 **[저장]** 버튼을 클릭하여 Address Group 을 생성합니다.

Address Group 변경

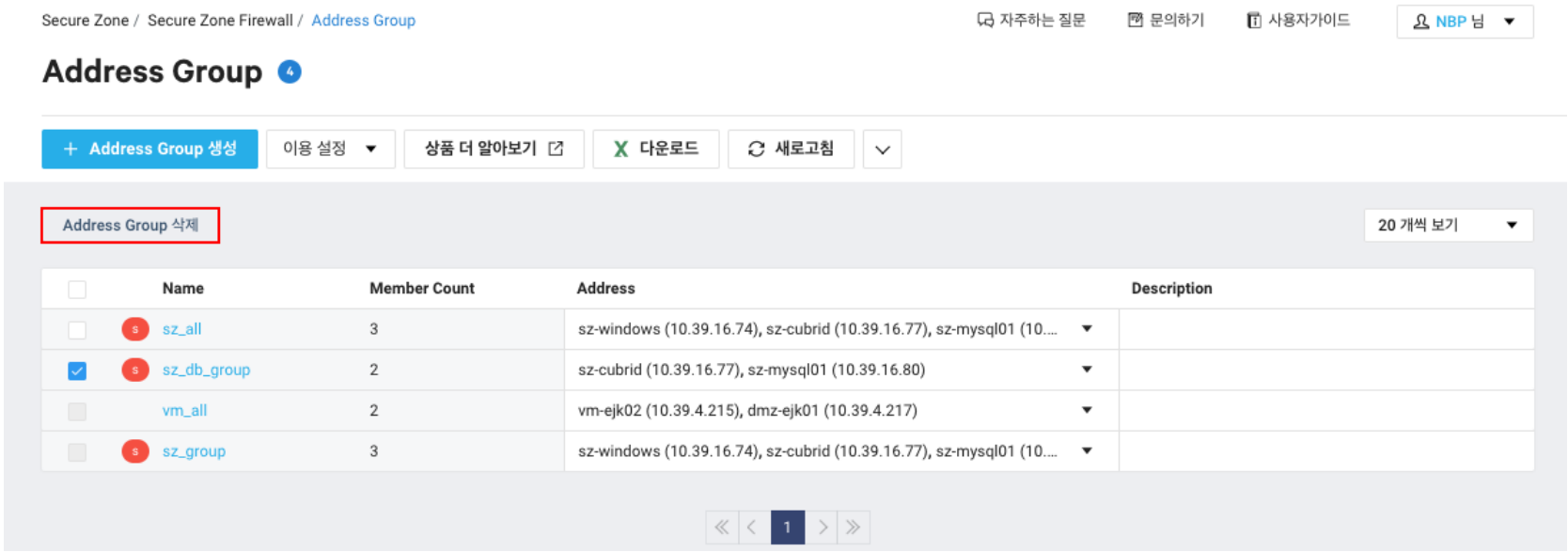


① **Security > Secure Zone > Secure Zone Firewall > Address Group** 에서 변경하고자 하는 Address Group 의 Name 을 클릭합니다.

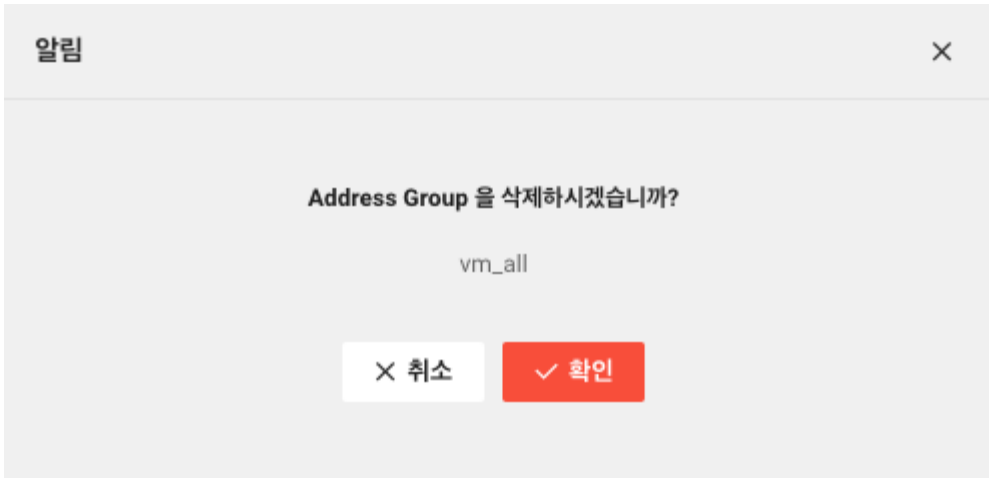


② 변경하고자 하는 값을 넣어 수정 후 **[저장]** 버튼을 클릭하여 Address Group 을 변경합니다.

Address Group 삭제

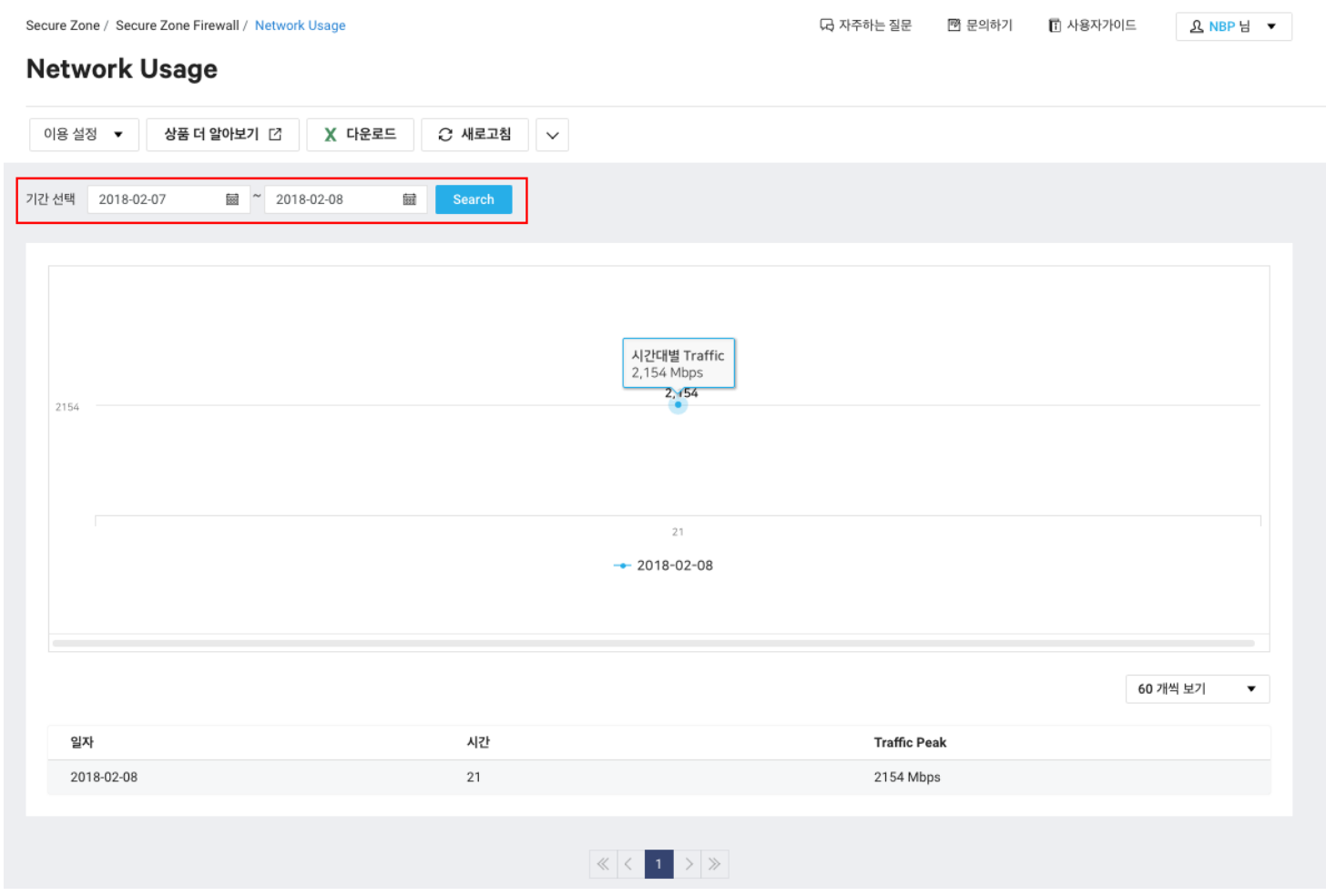


① **Security > Secure Zone > Secure Zone Firewall > Address Group** 에서 삭제하고자 하는 Address Group 을 다중 선택한 수 **Address Group 삭제**버튼을 클릭합니다.



② 삭제 대상 Address Group 체크한 후 **확인** 버튼을 클릭하여 삭제합니다.

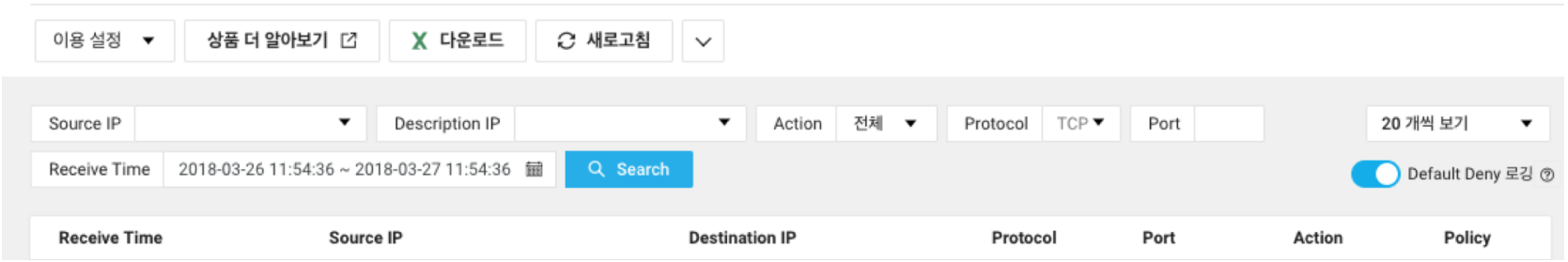
Network Usage 조회



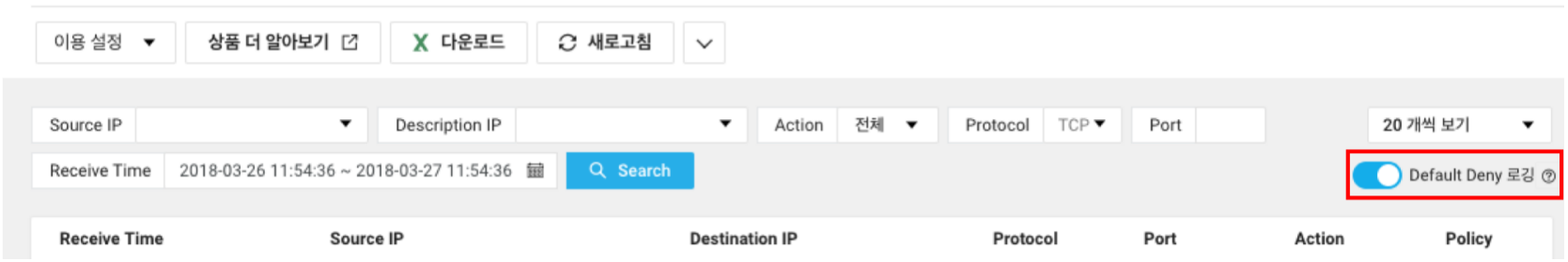
① **Security > Secure Zone > Secure Zone Firewall > Network Usage** 에서 시간대별 peak 트래픽 사용량을 조회합니다.

- 원하는 기간을 선택하여 조회할 수 있습니다.(최대 기간 설정: 1 개월)

Log 조회



- Receive Time: 날짜 범위로 검색 가능(보관 주기 및 사이즈는 Cloud Log Analytics 상품 정책에 따름)
- Source IP: 고객 소유의 VM / 사설 LB / SSL VPN
- Destination IP: 고객 소유의 VM
- Protocol: TCP / UDP / ICMP
- Port: destination port 검색 (0 ~ 65,535)
- Action
  - accept: for the end of non-TCP traffic // non-TCP 의 경우(icmp, udp.... tcp 를 제외한) 통과를 의미,
  - deny: for traffic blocked by a firewall policy // 정책에 의한 Block
  - close: for the end of TCP session closed with a FIN/FIN-ACK/RST // Allow 를 의미하며, FIN or RST 에 의한 정상 종료
  - timeout: for the end of a TCP session which is closed because it was idle. // Allow 는 되었지만 timeout 값에 의해 결국은 Block 된 경우, TCP SYN 은 보냈지만 remote 에서 응답이 없는 경우에도 남음
  - ip-conn: for IP connection failed for the session (host is not reachable) // Allow 는 되었지만 fortigate 가 어떤 reply packet 을 받지 못해 종료된 경우. ICMP request 는 있으나 reply 는 없음, UDP request 있으나 reply 없을 때
- Policy: 해당 Log 가 히트된 Policy 명
- Default Deny 정책 로그 활성화/비활성화



Secure Zone VM 장비 IP를 ACG에 등록

- Secure zone 과 일반 zone 의 접근 제어를 Secure Zone Firewall 정책으로 통제하기 위해서는 각각의 VM 및 SSL VPN 을 동일한 ACG 설정 및 아래와 같은 규칙을 등록해야 합니다.(필수)

프로토콜	접근 소스	허용 포트(서비스)	메모
TCP	acggroup2(405)	1-65535	
UDP	acggroup2(405)	1-65535	
ICMP	acggroup2(405)		

Secure Zone Firewall 권한 Sub Account 적용

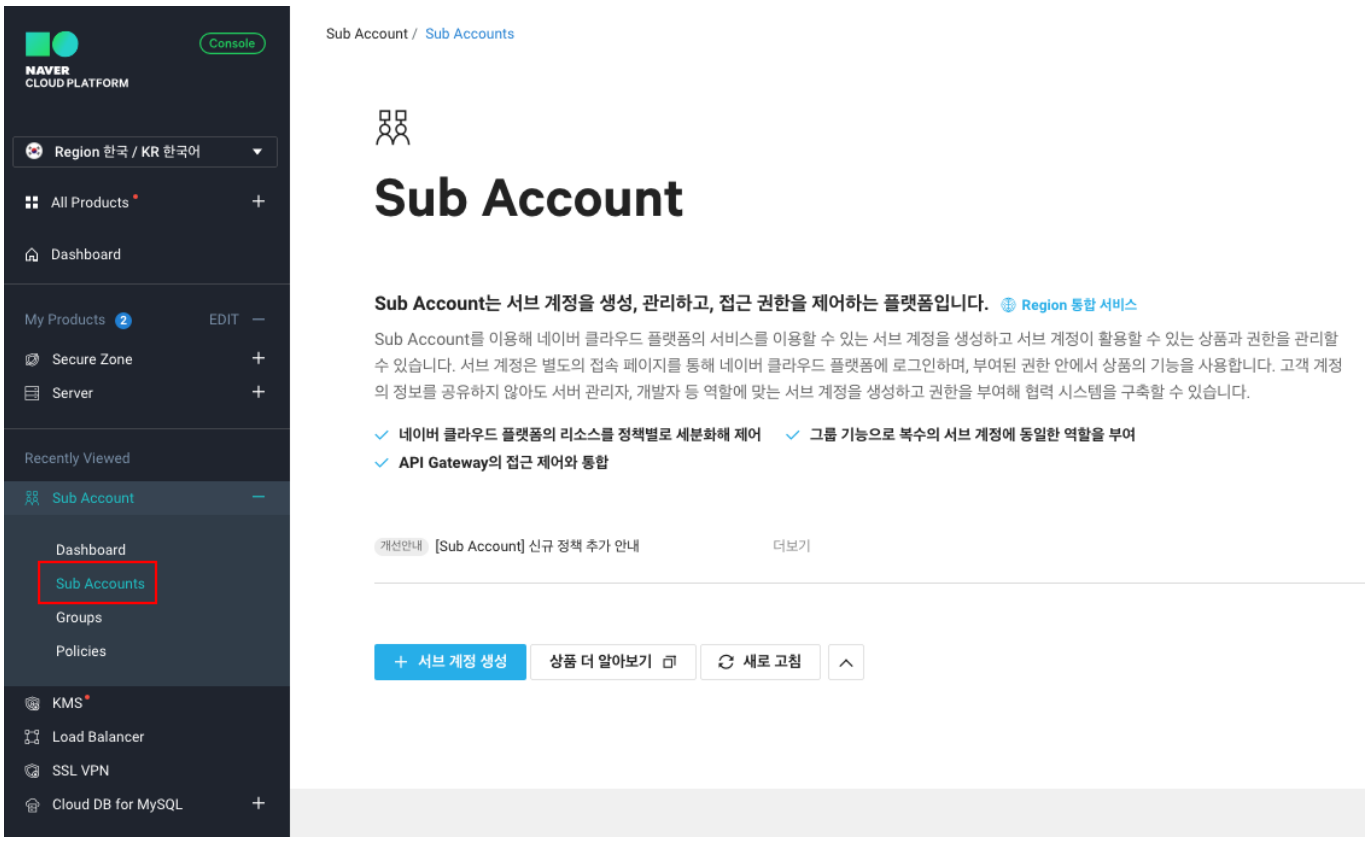
Sub Account 권한 상세

관리자와 사용자 권한으로 분류되고 다음과 같은 권한이 부여됩니다.

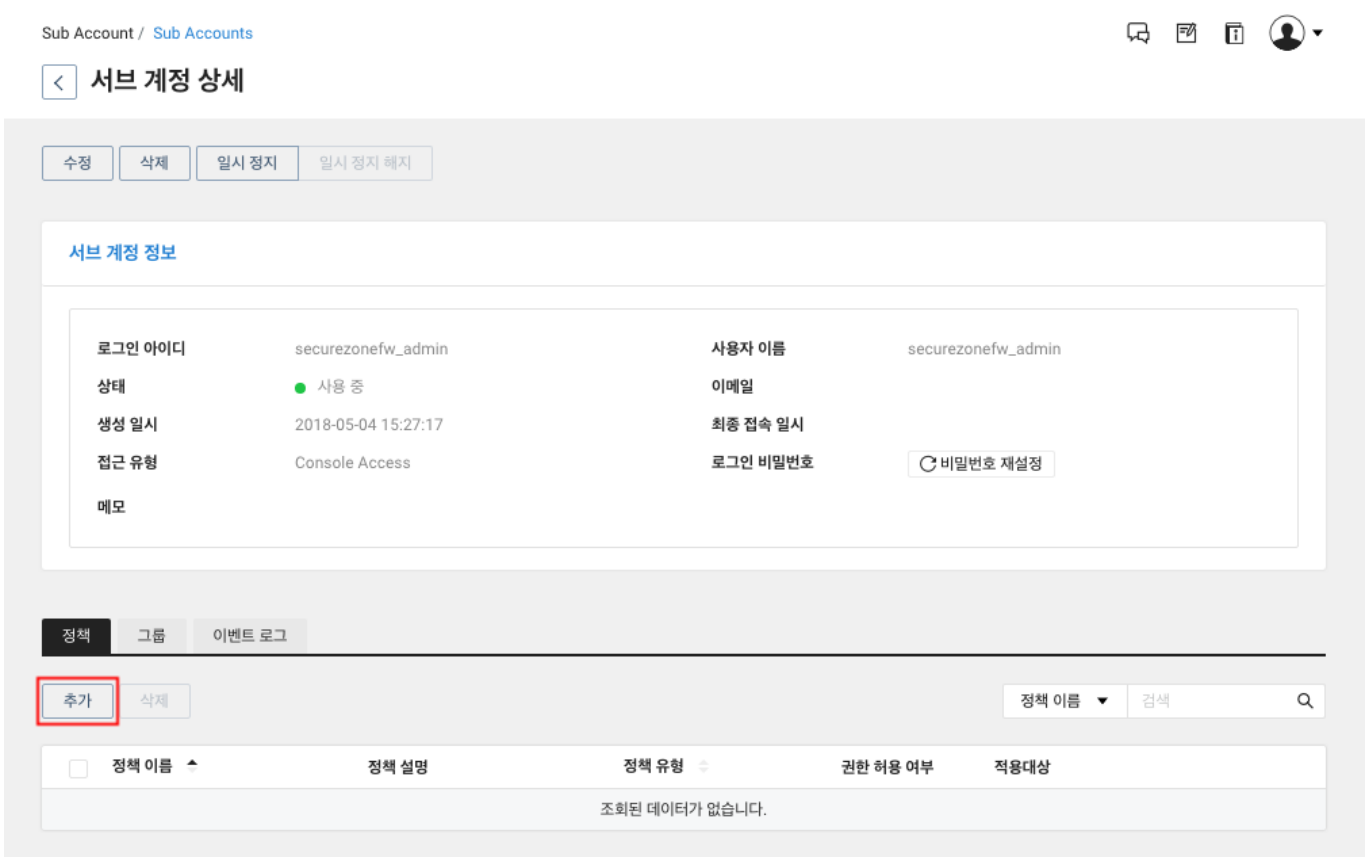
- NCP_SECURE_ZONE_FIREWALL_MANAGER
  - Secure Zone Firewall 상품 내 오브젝트 조회 및 Policy, Address Group 생성/삭제/변경 권한을 가집니다.
- NCP_SECURE_ZONE_FIREWALL_VIEWER
  - Secure Zone Firewall 상품 내 오브젝트 조회 권한을 가집니다.

Secure Zone Firewall 관리자 권한 부여하기

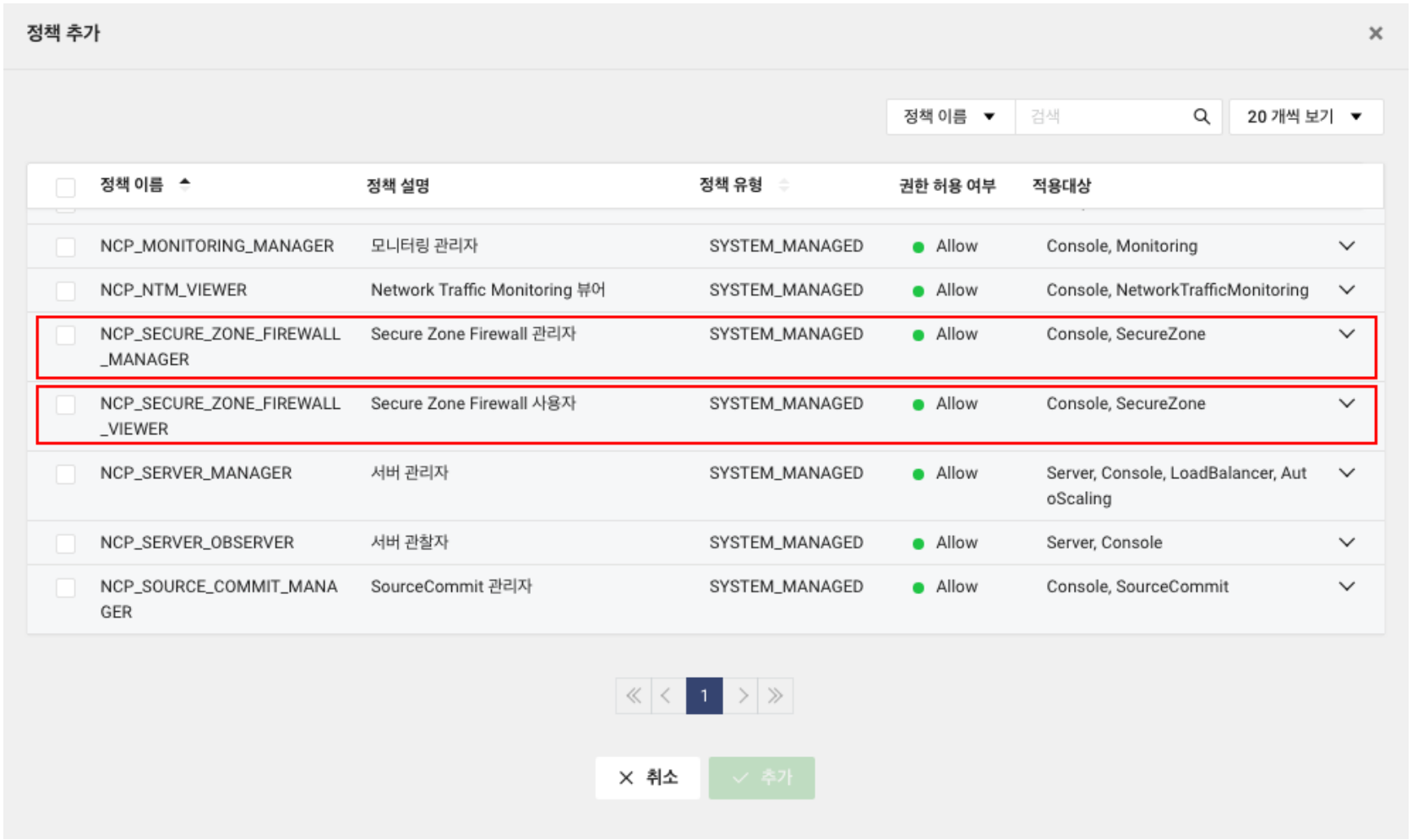
① 특정 사용자에게 Secure Zone Firewall 권한을 부여하기 위해서는 먼저 Sub Accounts 서비스를 선택합니다.



② Secure Zone Firewall 권한을 부여하고자 하는 서브 계정을 선택합니다.



③ 서브 계정 상세 화면에서 정책의 **추가** 버튼을 클릭합니다.

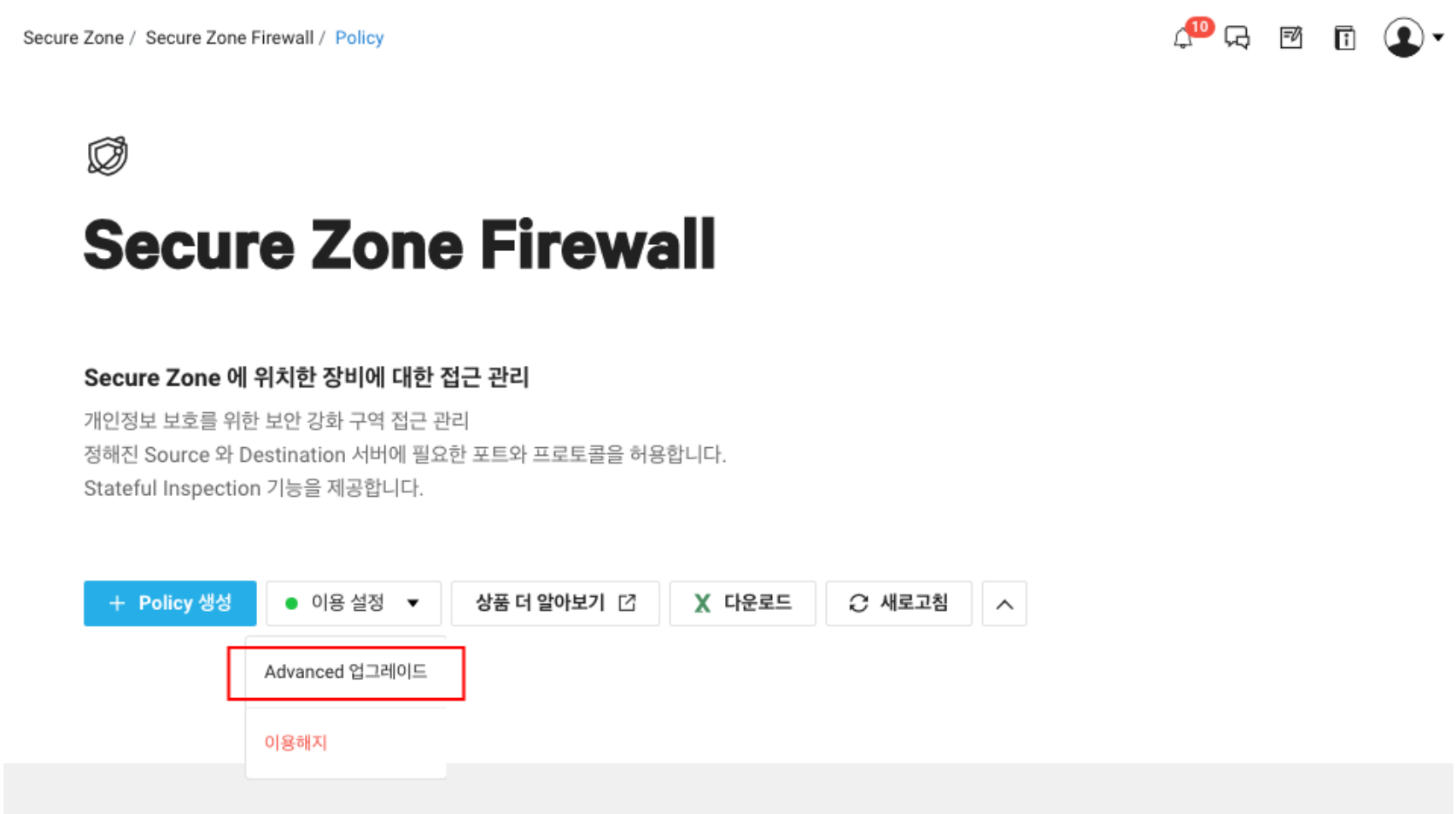


④ 선택된 서브 계정의 정책에서 NCP_SECURE_ZONE_FIREWALL_MANAGER 정책 또는 NCP_SECURE_ZONE_FIREWALL_VIEWER 중 부여하고자 하는 정책을 선택하여 해당 권한을 추가합니다.

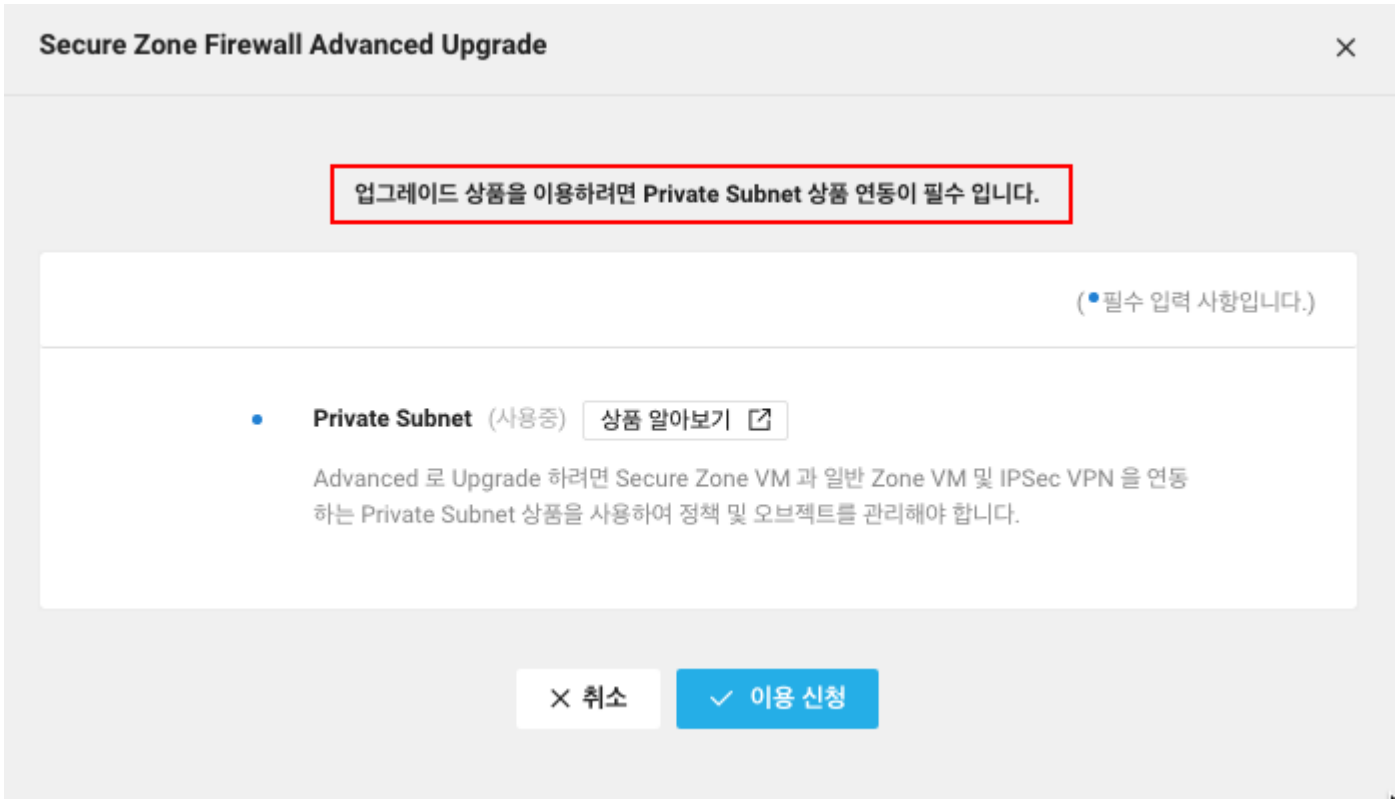
Secure Zone Firewall Advanced 업그레이드하기

Secure Zone Firewall Advanced 업그레이드 신청

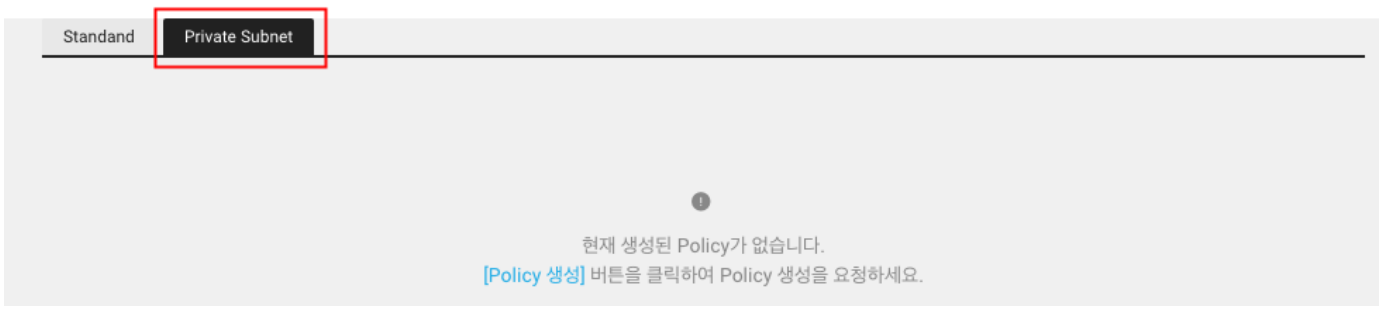
① **Security > Secure Zone > Secure Zone Firewall** 가입된 상태에서 "이용 설정"을 클릭합니다.



② **Advanced 업그레이드** 버튼을 클릭합니다.



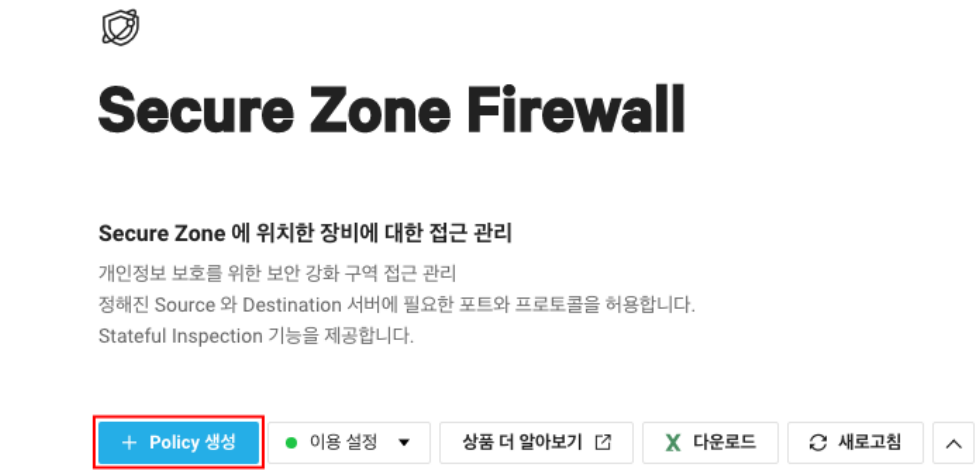
- **Advanced 업그레이드 상품을 이용하려면 Private Subnet 상품 가입이 필수 입니다.**
  ③ Advanced 로 업그레이드가 완료되면 Private Subnet 탭이 생깁니다.

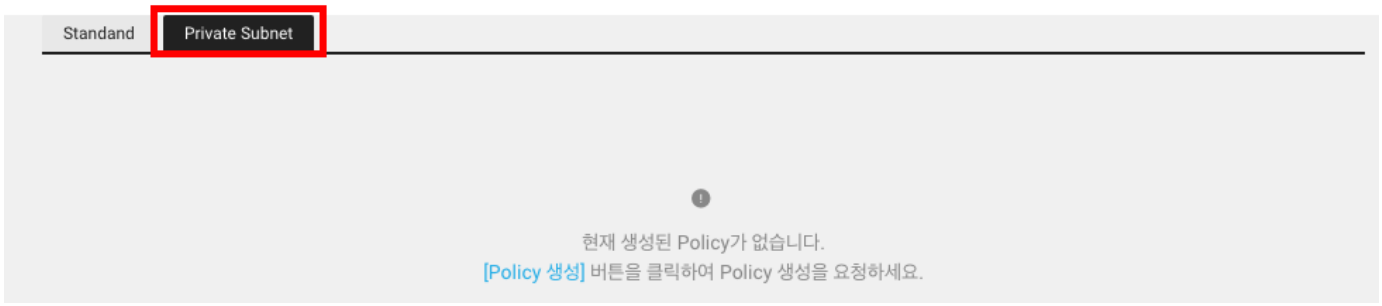


- Policy / Address Grou / Log 메뉴에서 Private Subnet 탭 선택 후 Advanced 기능을 이용합니다.

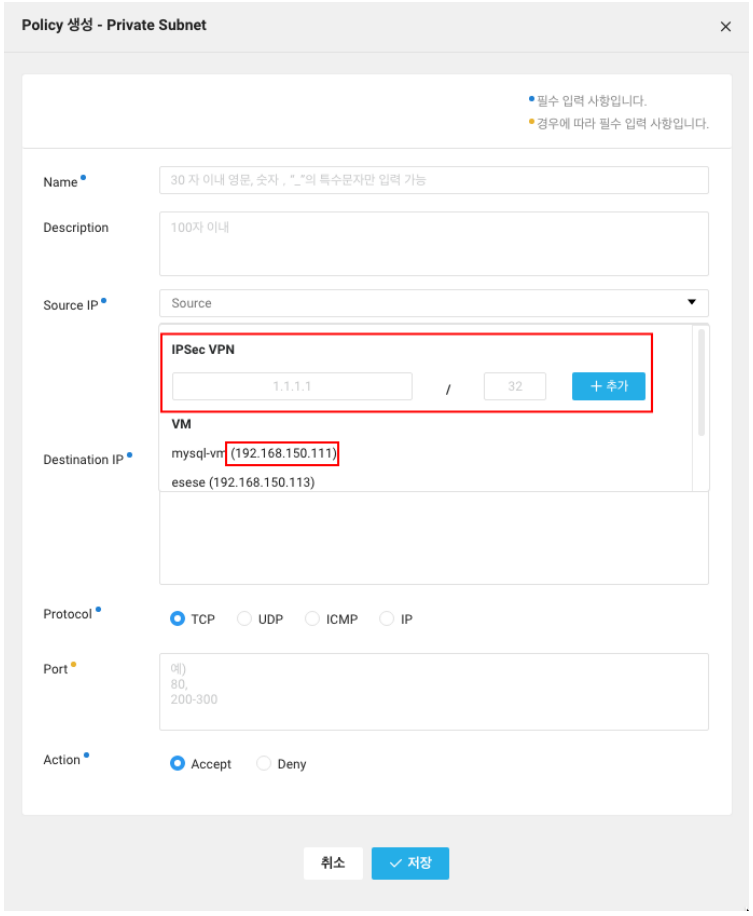
Policy 설정 - Advanced

Policy 생성





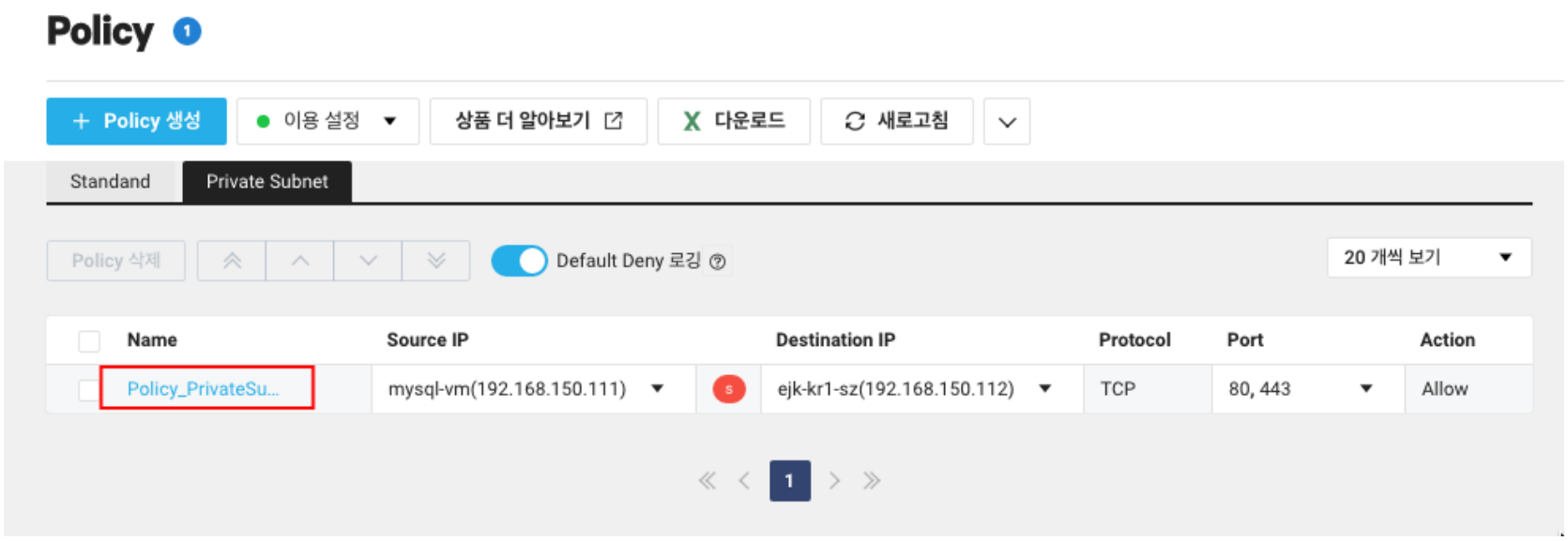
① **Security > Secure Zone > Secure Zone Firewall > Policy > Private Subnet** 에서 **+ Policy 생성** 버튼을 클릭합니다.



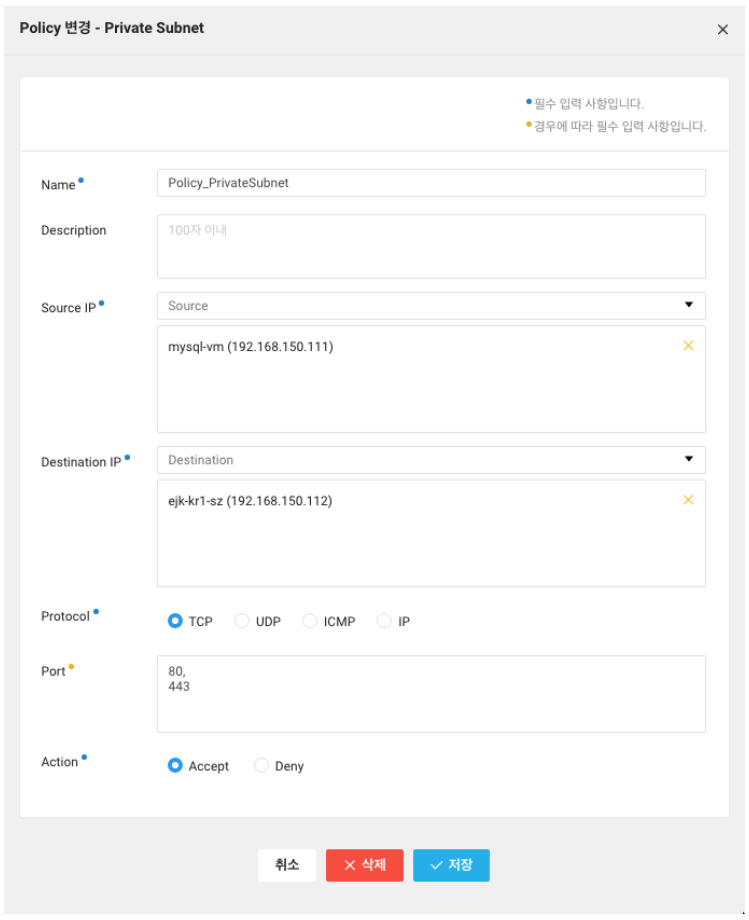
- Name: Policy 이름
- Description: Policy 설명
- Source IP: IPSec VPN (고객 직접 입력) / Private Subnet Network Interface 할당된 고객 소유 VM
- Destination IP: Private Subnet Network Interface 할당된 고객 소유 VM
- Protocol: TCP / UDP / ICMP
- Port: destination port (0 ~ 65,535)
- Action: Allow / Deny
  Source IP 와 Destination IP 중 하나는 Secure Zone 필수입니다.

② 필수 값을 입력한 후 **[저장]** 버튼을 클릭하여 Policy 를 생성합니다.

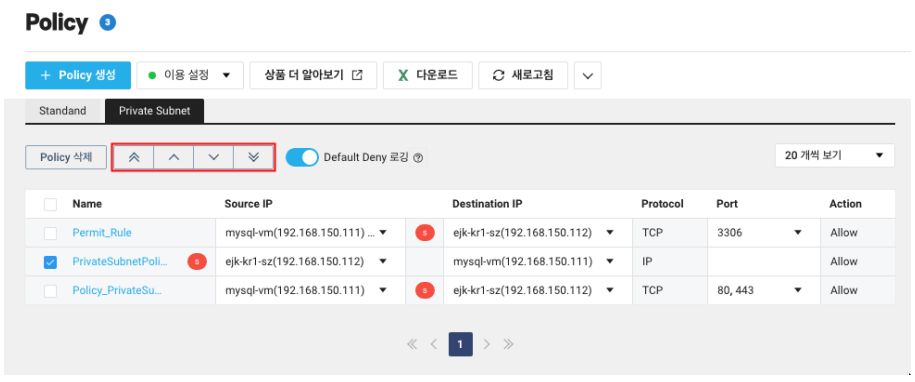
Policy 변경



① **Security > Secure Zone > Secure Zone Firewall > Policy > Private Subnet** 에서 변경하고자 하는 Policy 의 Name 을 클릭합니다.

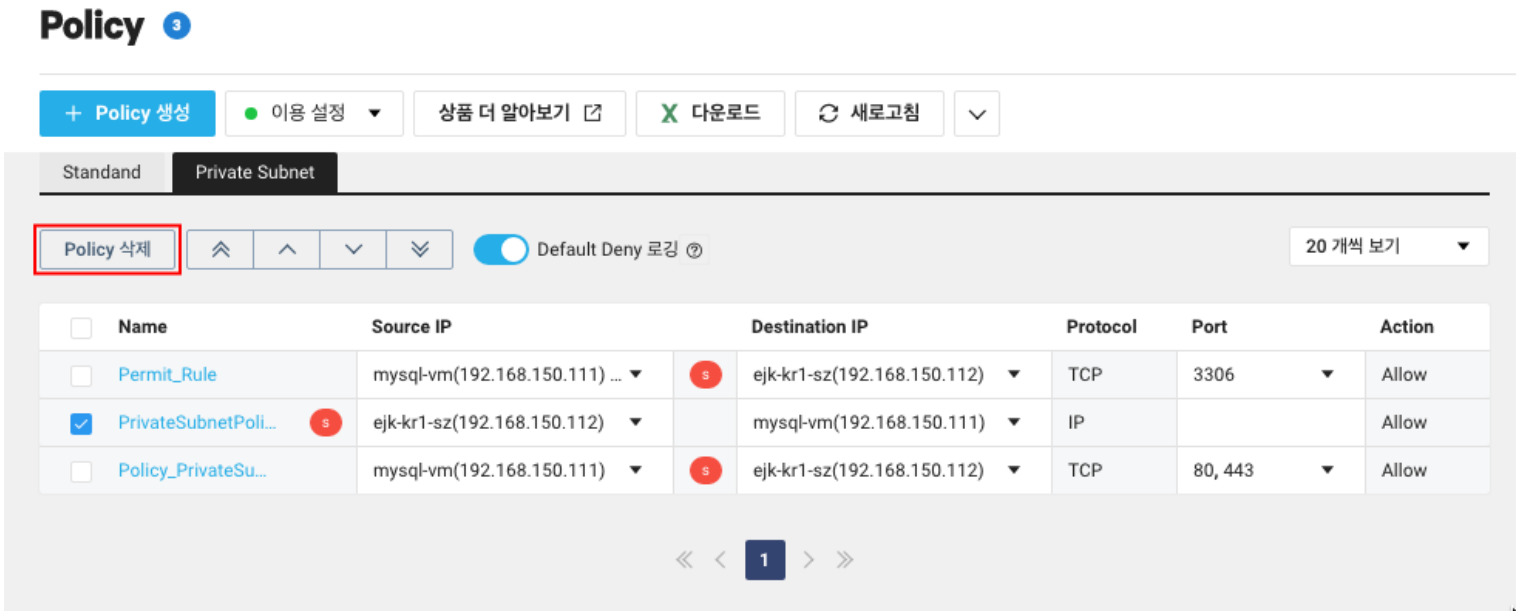


② 변경하고자 하는 값을 넣어 수정 후 **저장**을 클릭하여 Policy 를 변경합니다.

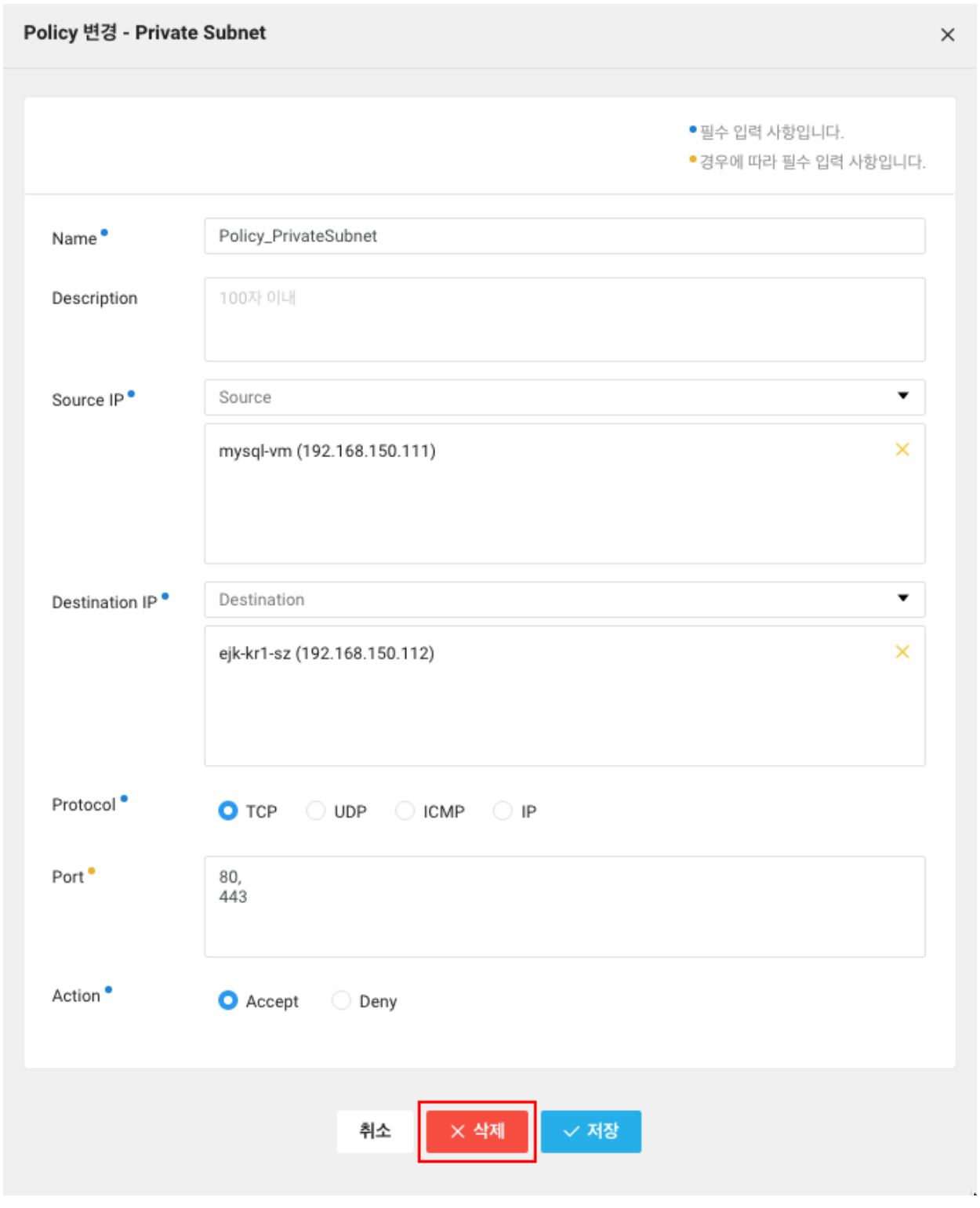


③ Policy 우선순위를 수정하기 위해 Policy 하나를 선택하여 순서변경 버튼으로 우선순위를 조정합니다.

Policy 삭제



① **Security > Secure Zone > Secure Zone Firewall > Policy > Private Subnet** 에서 삭제하고자 하는 Policy 의 콤보박스를 다중 선택 후 **Policy 삭제** 버튼을 클릭하여 삭제합니다.



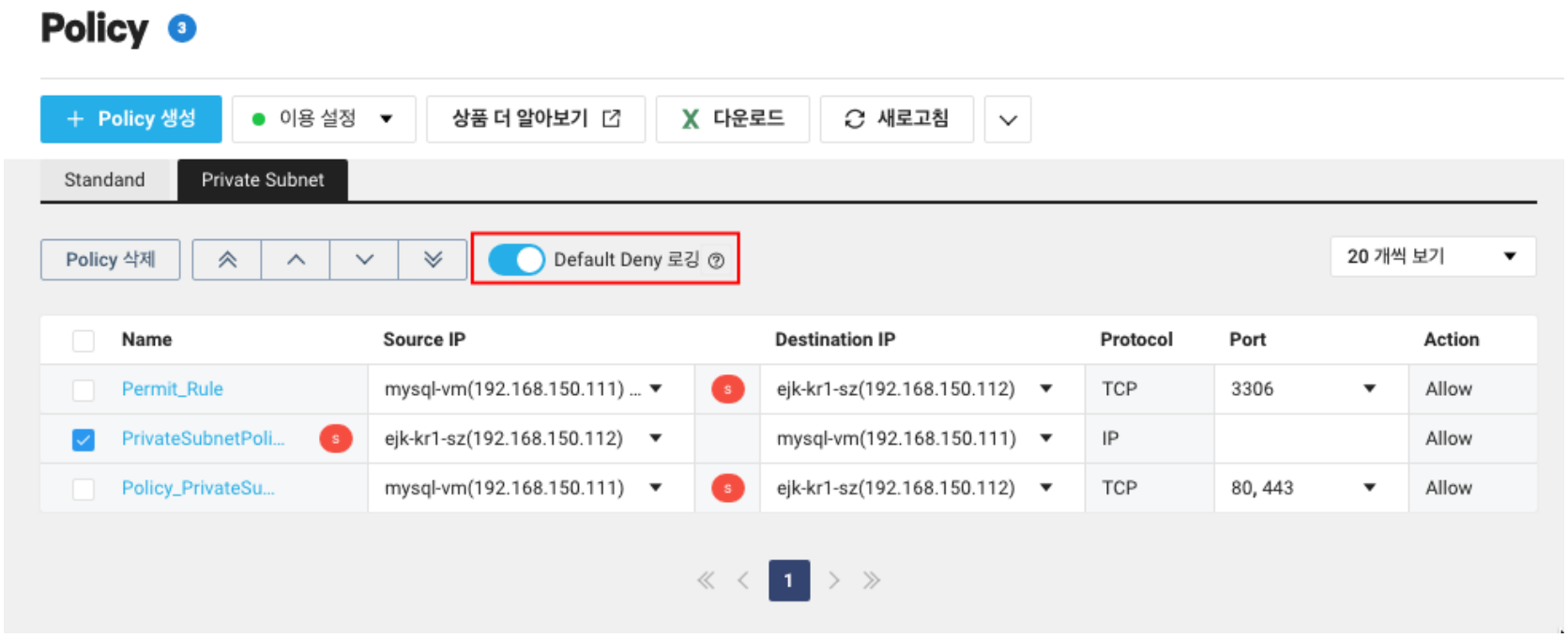
② **Security > Secure Zone > Secure Zone Firewall > Policy > Private Subnet** 에서 삭제하고자 하는 Policy 의 Name 을 클릭한 후 **[삭제]** 버튼을 클릭합니다.

Default Deny 정책 로그 활성화/비활성화

기본적으로 방화벽에 정책 설정을 하지 않으면 All Deny 입니다. 아무 정책이 없어서 트래픽이 차단되는 경우 Default 정책에 의해 차단되고 로그가 남는데, 허용되지 않은 접속 시도가 많은 경우 Log Size 가 많이 증가하여 Cloud Log Analytics 저장소 용량을 많이 차지할 수 있습니다.

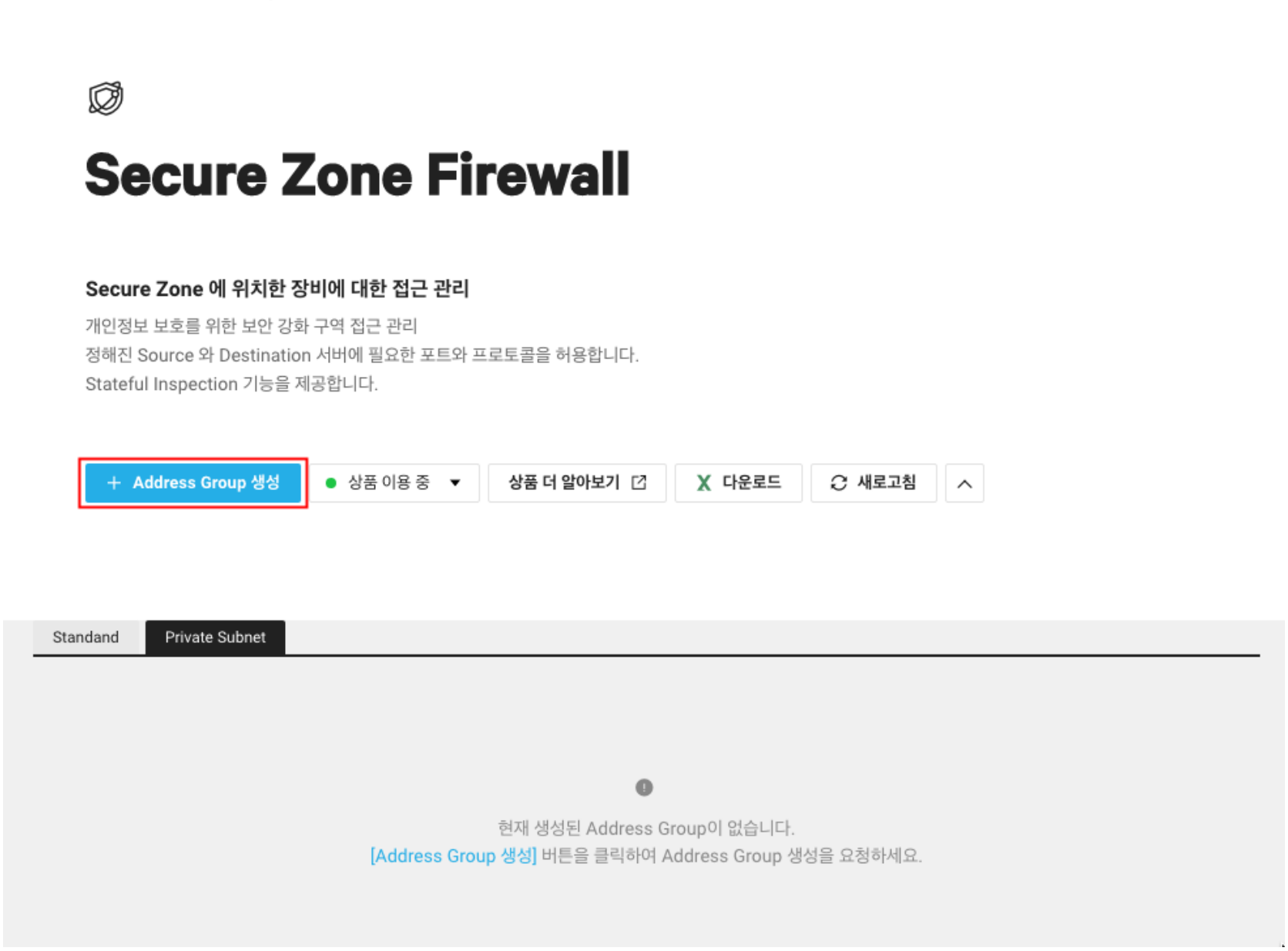
① **Default Deny 로깅**을 활성화/비활성화하여 Default Deny 정책에 해당하는 로그를 남기거나 남지 않도록 설정할 수 있습니다.

- Default: 활성화(로그를 남김)

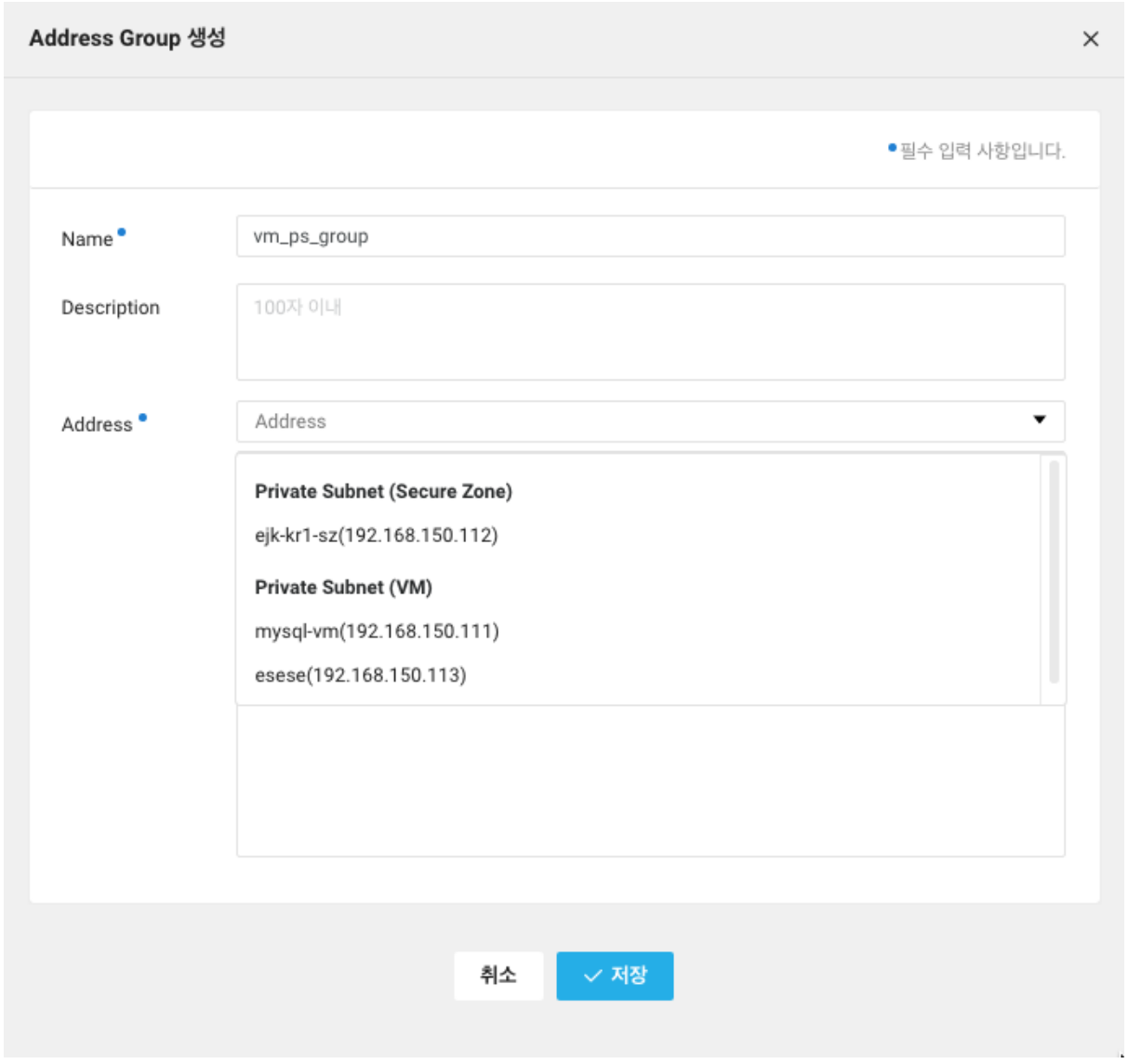


Address Group 설정 - Advanced

Address Group 생성

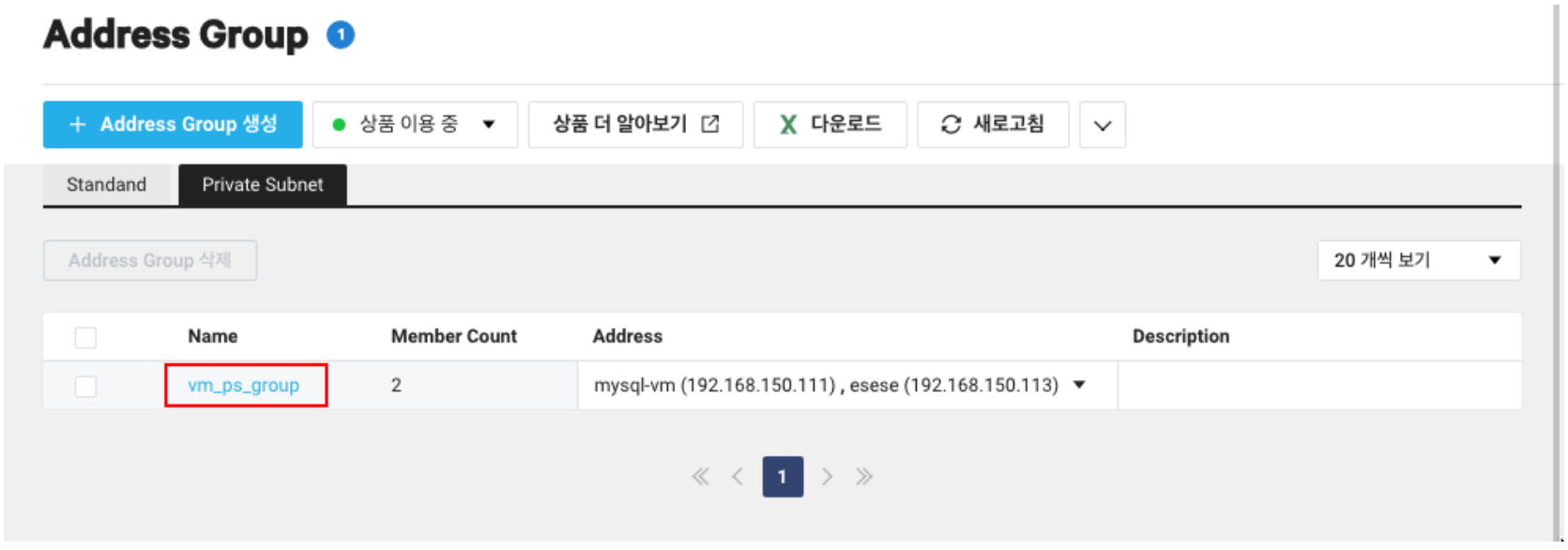


① **Security > Secure Zone > Secure Zone Firewall > Address Group > Private Subnet** 에서 **+ Address Group 생성** 버튼을 클릭합니다.

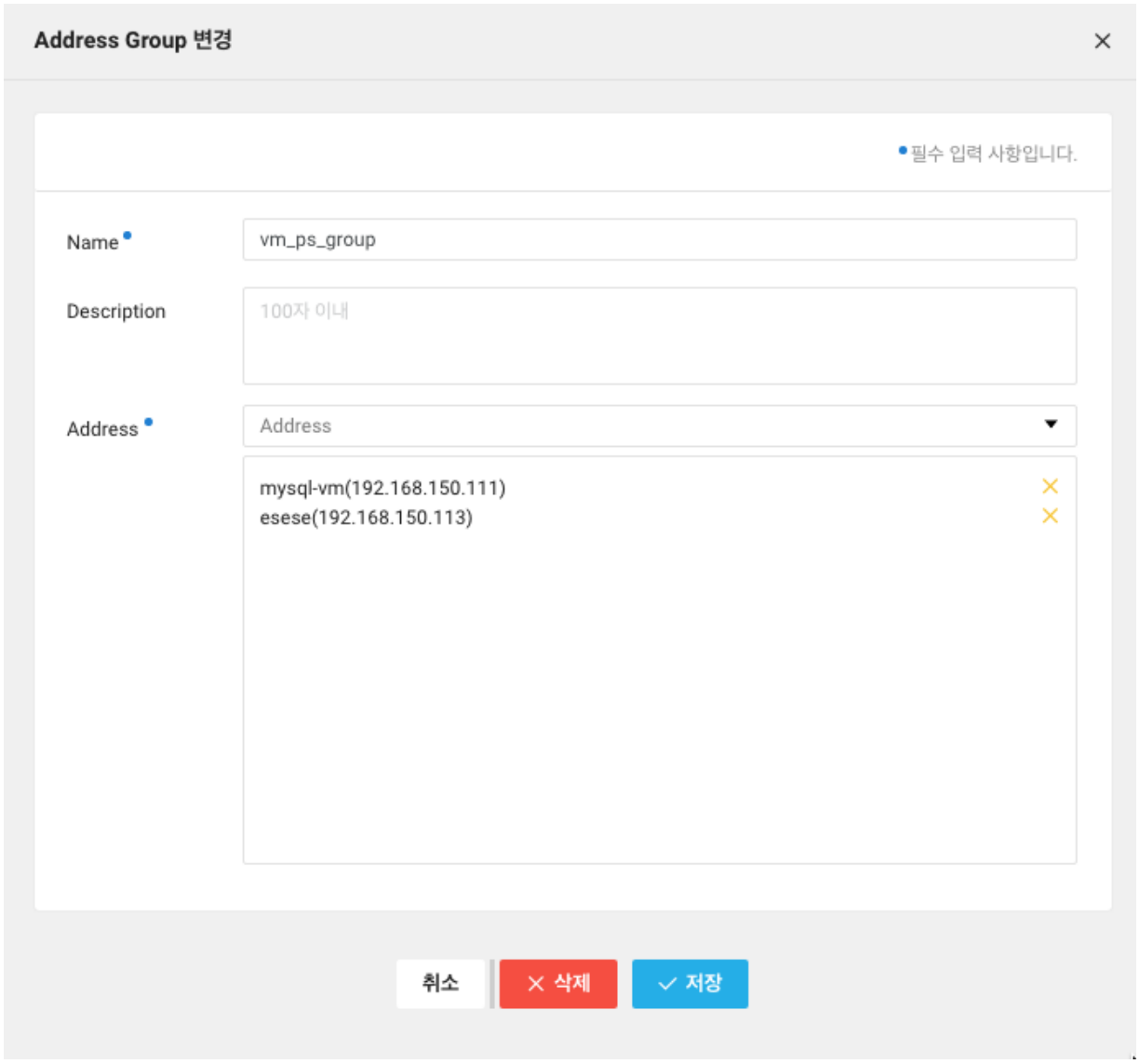


② Address 를 다중 선택하고 **[저장]** 버튼을 클릭하여 Address Group 을 생성합니다.

Address Group 변경

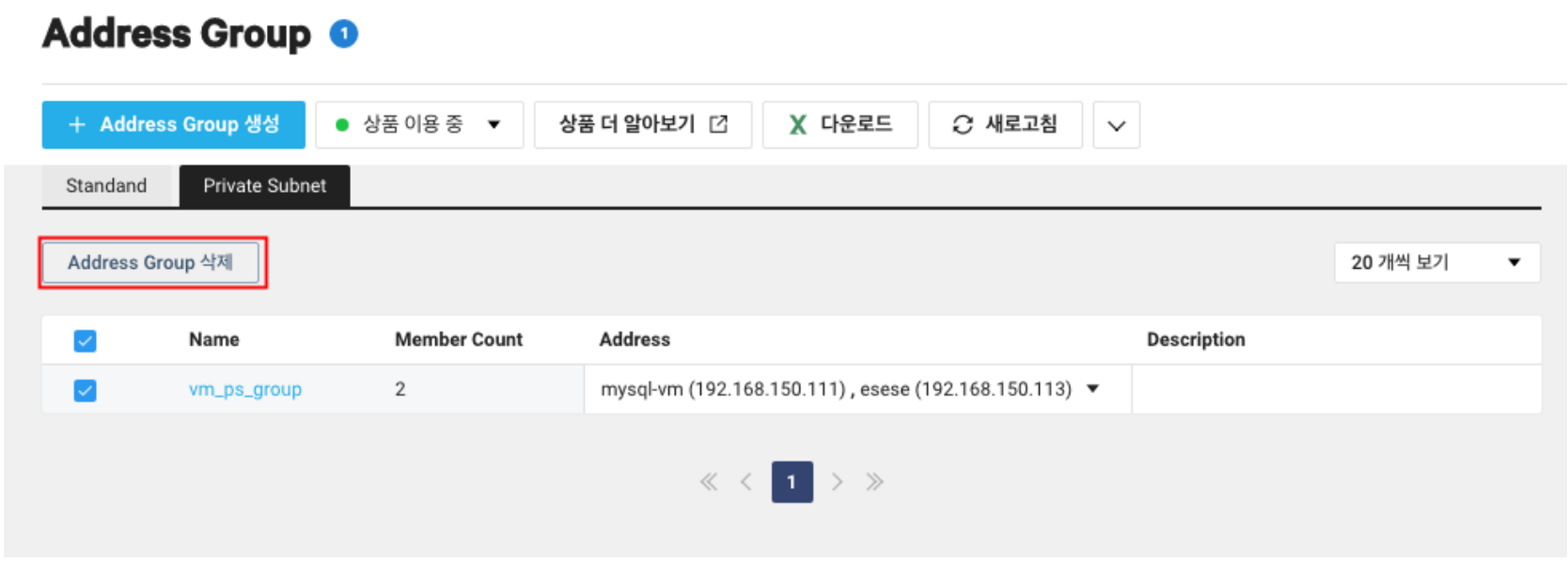


① **Security > Secure Zone > Secure Zone Firewall > Address Group > Private Subnet** 에서 변경하고자 하는 Address Group 의 Name 을 클릭합니다.

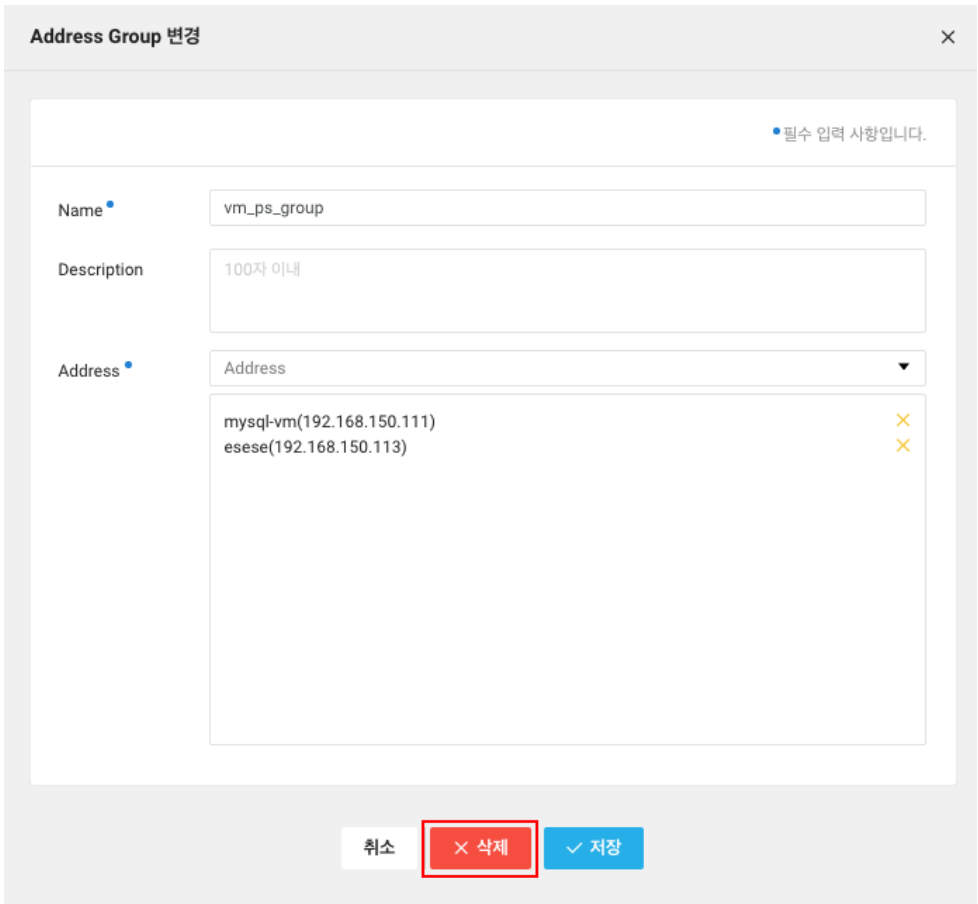


② 변경하고자 하는 값을 넣어 수정 후 **[저장]** 버튼을 클릭하여 Address Group 을 변경합니다.

Address Group 삭제

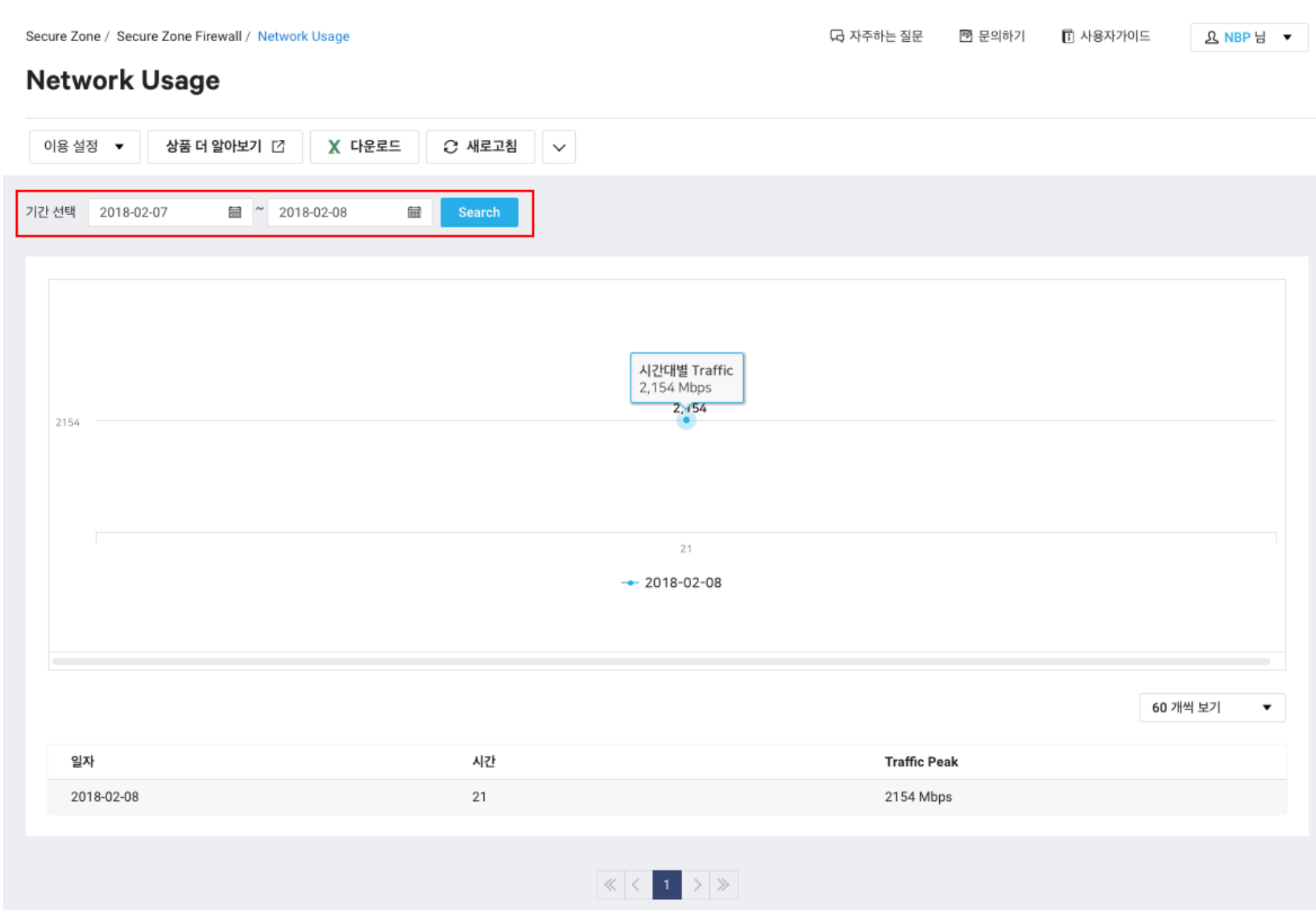


① **Security > Secure Zone > Secure Zone Firewall > Address Group > Private Subnet** 에서 삭제하고자 하는 Address Group 을 다중 선택한 수 **Address Group 삭제**버튼을 클릭합니다.



② **Security > Secure Zone > Secure Zone Firewall > Address Group > Private Subnet** 에서 삭제하고자 하는 Address Group 의 Name 을 클릭한 후 **[삭제]** 버튼을 클릭합니다.

Network Usage 조회

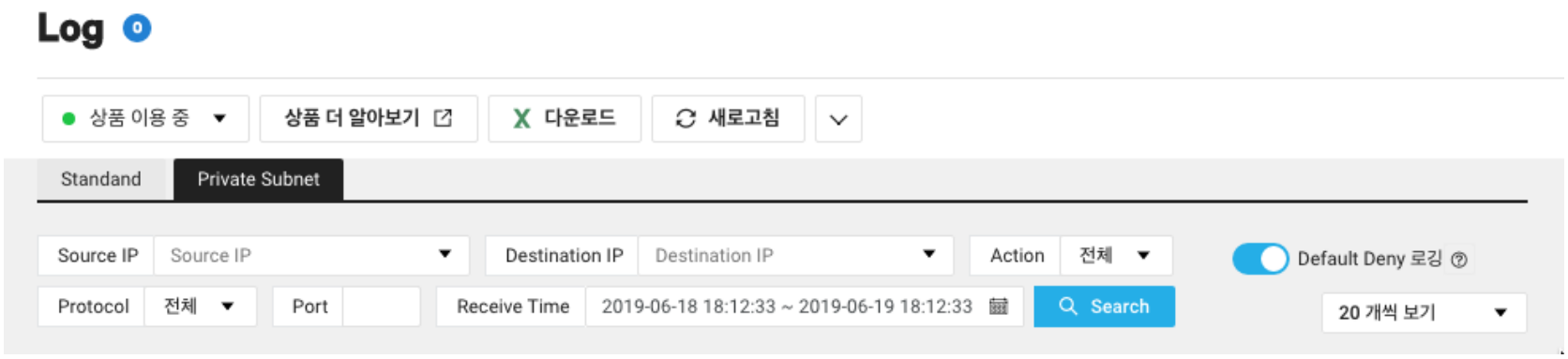


① **Security > Secure Zone > Secure Zone Firewall > Network Usage** 에서 시간대별 peak 트래픽 사용량을 조회합니다.

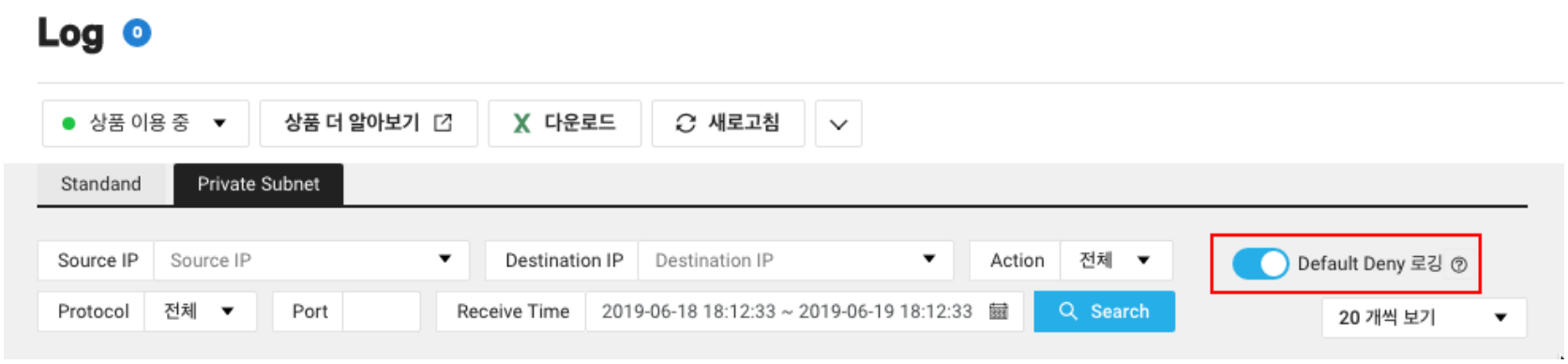
- 원하는 기간을 선택하여 조회할 수 있습니다.(최대 기간 설정: 1 개월)

Log 조회

Secure Zone > Secure Zone Firewall > Log > Private Subnet 탭에서 Private Subnet Traffic Log 확인



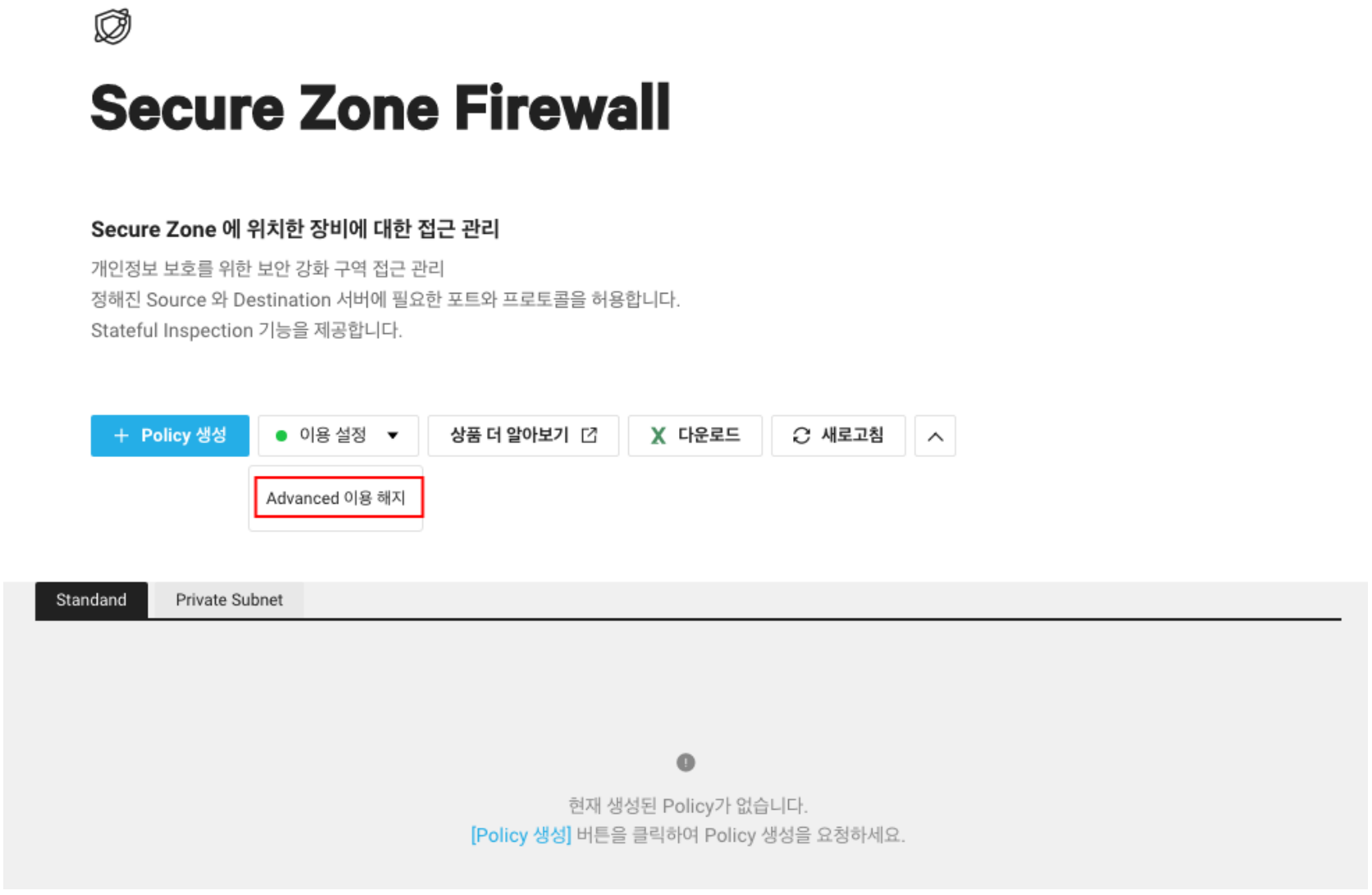
- Receive Time: 날짜 범위로 검색 가능(보관 주기 및 사이즈는 Cloud Log Analytics 상품 정책에 따름)
- Source IP: 고객 소유의 VM / 사설 LB / SSL VPN
- Destination IP: 고객 소유의 VM
- Protocol: TCP / UDP / ICMP
- Port: destination port 검색 (0 ~ 65,535)
- Action
  - accept: for the end of non-TCP traffic // non-TCP 의 경우(icmp, udp.... tcp 를 제외한) 통과를 의미,
  - deny: for traffic blocked by a firewall policy // 정책에 의한 Block
  - close: for the end of TCP session closed with a FIN/FIN-ACK/RST // Allow 를 의미하며, FIN or RST 에 의한 정상 종료
  - timeout: for the end of a TCP session which is closed because it was idle. // Allow 는 되었지만 timeout 값에 의해 결국은 Block 된 경우, TCP SYN 은 보냈지만 remote 에서 응답이 없는 경우에도 남음
  - ip-conn: for IP connection failed for the session (host is not reachable) // Allow 는 되었지만 fortigate 가 어떤 reply packet 을 받지 못해 종료된 경우. ICMP request 는 있으나 reply 는 없음, UDP request 있으나 reply 없을 때
- Policy: 해당 Log 가 히트된 Policy 명
- Default Deny 정책 로그 활성화/비활성화



Secure Zone Firewall 이용 해지

Secure Zone Firewall Advanced 해지

① **Security > Secure Zone > Secure Zone Firewall > Advanced** 가입된 상태에서 "Advanced 이용해지"를 클릭합니다.



- Advanced 상품이 해지되고 Standard 상품 가입은 유지됩니다.
  ② **Security > Secure Zone > Secure Zone Firewall** Advanced 상품이 가입되지 않은 상태에서 "이용해지"를 클릭합니다.