ABLESTACK

ABLESTACK Link를 통한 마이크로 세그먼테이션 보안 관리

ABLESTACK®

ABLESTACK Link를 통한 마이크로 세그먼테이션 보안 관리

제로 트러스트 보안은 암묵적 신뢰가 항상 취약하다는 관점에 따라 만들어진 개념으로, '보안'은 절대 신뢰하지 말고, 항상 확인하라'는 전략으로 설계되어야 한다는 주장을 담고 있습니다. 클라우드 및 가상화를 통해 만들어진 인프라는 기존의 데이터 보안 경계를 빠르게 허물고 있습니다. 기존에는 물리적으로 관리 가능한 보안 인프라가 기업의 데이터센터를 둘러싸고 있었지만, 가상화 및 클라우드가 발전함에 따라 이러한 경계가 복잡해지고, 넓어져서 보안 관리에 새로운 도전을 주고 있습니다.

제로 트러스트 보안 모델은 다양한 방식으로 구현되는데, 가상화 인프라 및 네트워크 수준에서는 일반적으로 마이크로 세그먼테이션을 사용합니다. 마이크로 세그먼테이션은 조직의 데이터센터 또는 클라우드(가상화) 환경에서 워크로드, 즉 가상머신 및 컨테이너 간의 네트워크 액세스를 제어하고 제한하는데 도움이 되는 보안 접근 방식입니다.

ABLESTACK는 Link 구성요소를 통해 Mold에서 중앙 집중화된 보안 정책을 관리하고, 이를 가상머신 네트워크 패브릭에 적용함으로써 인프라 관리자 또는 보안 관리자가 효과적으로 세부적인 가상머신 트래픽을 통제하고 관리할 수 있는 방법을 제공합니다. 마이크로 세그먼테이션 기능을 사용하는 절차는 다음과 같습니다.

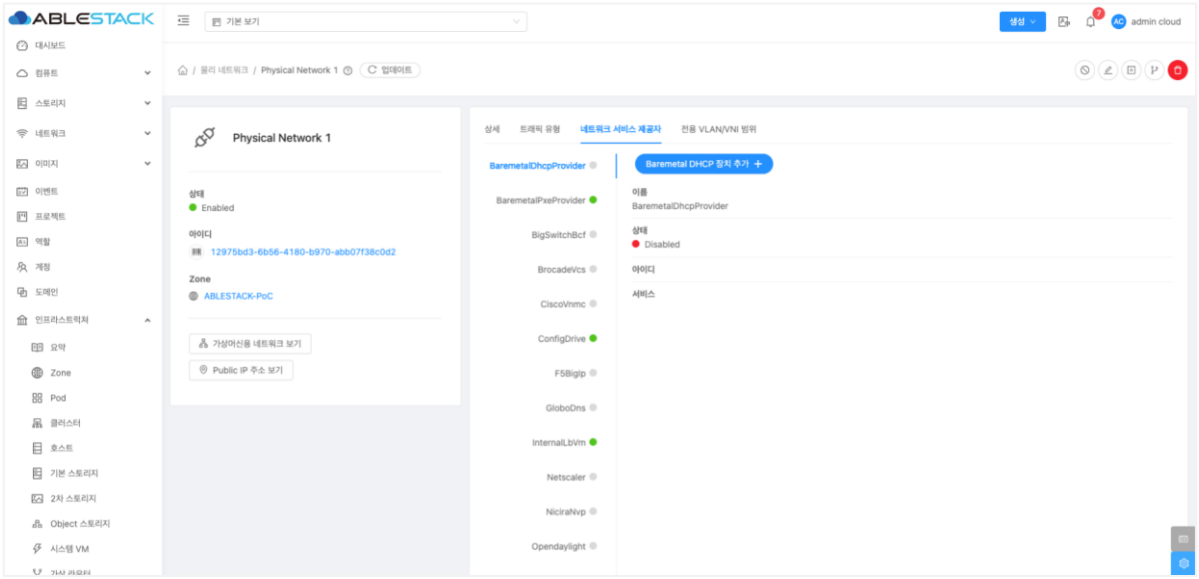
1. ABLESTACK Link(마이크로 세그먼테이션) 활성화
2. 마이크로 세그먼테이션 네트워크 오퍼링 생성
3. 마이크로 세그먼테이션 네트워크 생성
4. 보안정책 생성
5. 가상머신 생성 및 보안정책 적용
6. 보안정책 관리 및 업데이트

ABLESTACK Link(마이크로 세그먼테이션) 활성화

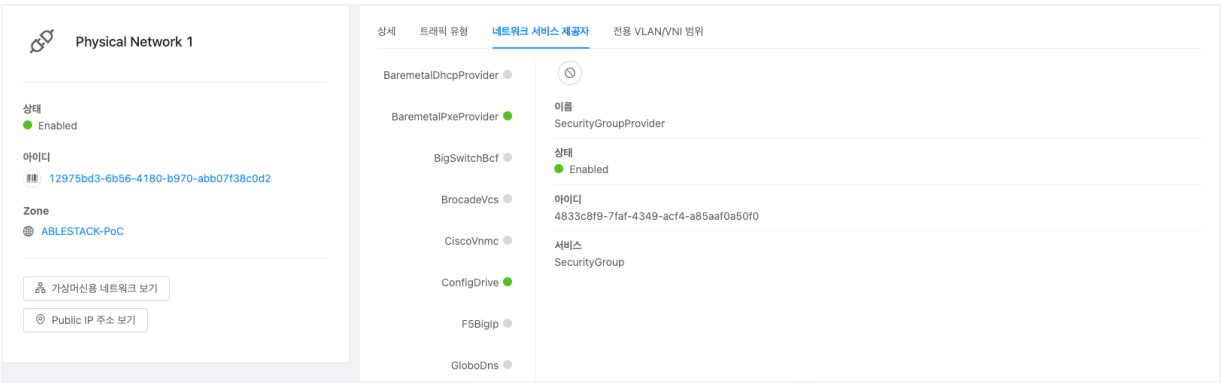
ABLESTACK에서 마이크로 세그먼테이션 기능을 사용하기 위해서는 관련 기능을 먼저 활성화 해야 합니다. 기본적으로 ABLESTACK은 마이크로 세그먼테이션 기능을 활성화 하지 않으며 일반적인 가상 네트워크를 생성하고 가상머신을 연결하여 구성하며, 각 가상머신 간의 네트워크는 통제되지 않습니다.

마이크로 세그먼테이션은 기존에 만들어진 가상머신과 네트워크에 영향을 미치지 않으며, 마이크로 세그먼테이션 기능이 활성화된 네트워크에 연결된 가상머신에만 영향을 미칩니다.

기능을 활성화 하기 위해 다음과 같이 "인프라스트럭쳐 > Zone > Zone 상세화면 > 물리 네트워크 탭 > 물리 네트워크 선택하여 상세 > 네트워크 서비스 제공자" 화면을 표시합니다.



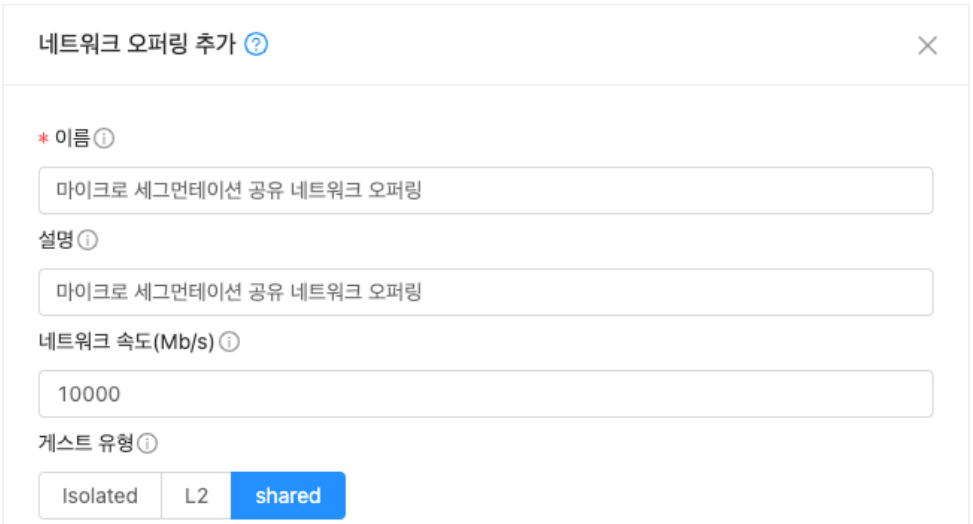
해당 화면에서 Security Group Provider를 선택한 뒤, 다음과 같이 "활성화" 버튼을 클릭하여 표시되는 대화상자에서 "확인"을 눌러 마이크로 세그먼테이션 서비스를 활성화 합니다.

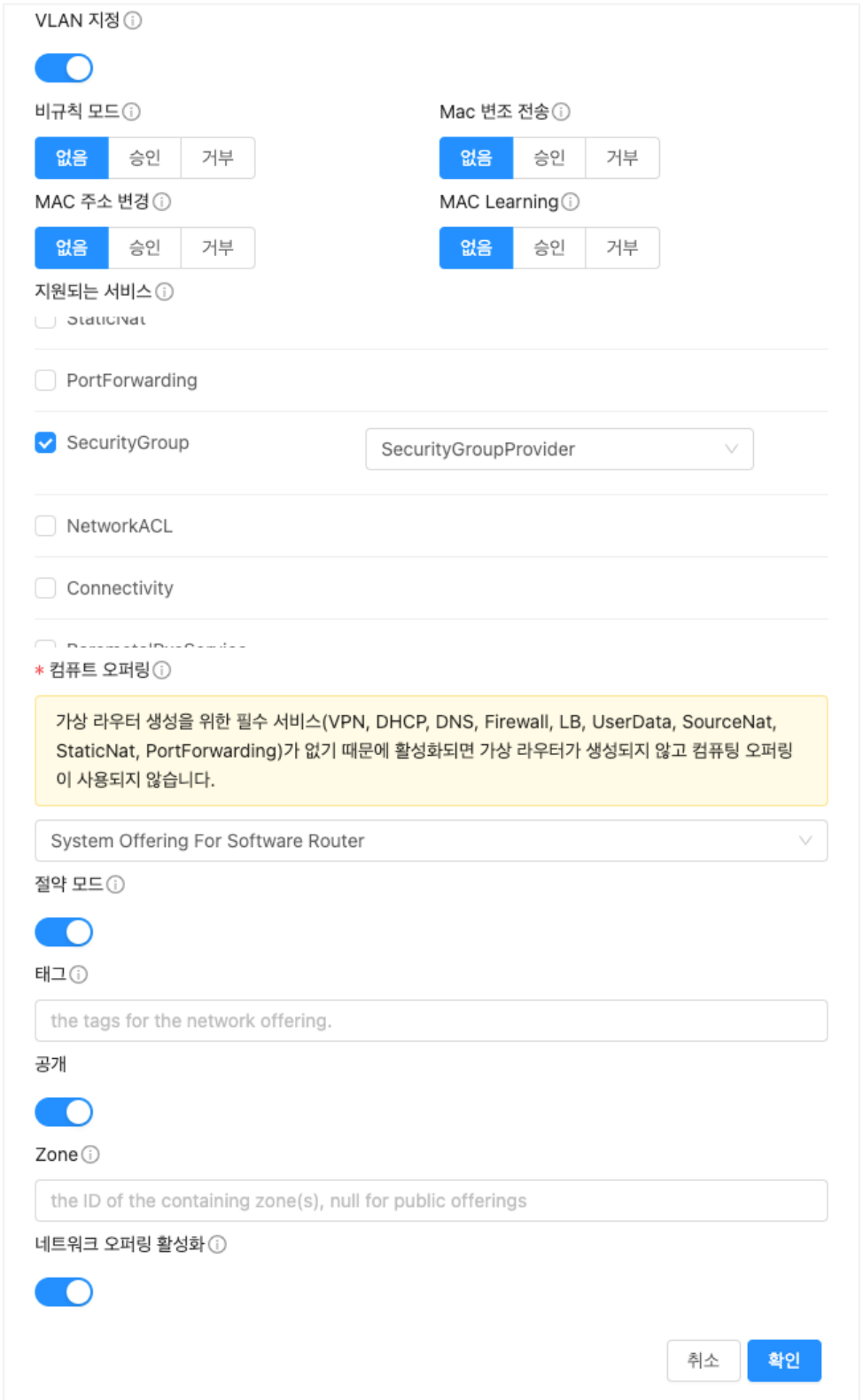


마이크로 세그먼테이션 네트워크 오퍼링 생성

물리 네트워크에 대해 마이크로 세그먼테이션 기능을 활성화 한 후에는 마이크로 세그먼테이션 기능을 사용할 수 있는 네트워크 오퍼링을 만들어야 합니다.

마이크로 세그먼테이션 기능을 Zone 수준의 공유 네트워크에서 사용할 수 있으며, 이를 위해 Mold의 "서비스 오퍼링 > 네트워크 오퍼링" 화면에서 "네트워크 오퍼링 추가" 버튼을 클릭하여 공유 네트워크 오퍼링을 다음과 같이 생성해야 합니다.




VLAN 지정
비규칙 모드
없음
승인
거부
Mac 변조 전송
없음
승인
거부
MAC 주소 변경
없음
승인
거부
MAC Learning
없음
승인
거부
지원되는 서비스
PortForwarding
SecurityGroup
SecurityGroupProvider
NetworkACL
Connectivity
* 컴퓨트 오퍼링
가상 라우터 생성을 위한 필수 서비스(VPN, DHCP, DNS, Firewall, LB, UserData, SourceNat, StaticNat, PortForwarding)가 없기 때문에 활성화되면 가상 라우터가 생성되지 않고 컴퓨팅 오퍼링이 사용되지 않습니다.
System Offering For Software Router
절약 모드
태그
the tags for the network offering.
공개
Zone
the ID of the containing zone(s), null for public offerings
네트워크 오퍼링 활성화
취소
확인

위 화면에서 마이크로 세그먼테이션 기능을 사용하고 테스트하기 위해 다음의 항목의 값을 확인합니다.

•게스트 유형 : Shared
•VLAN 지정 : 활성화
•지원되는 서비스
- Dhcp : ConfigDrive
- Dns : ConfigDrive
- UserData : ConfigDrive
- SecurityGroup : SecurityGroupProvider

•네트워크 오퍼링 활성화 : 활성화

위와 같이 항목의 값을 설정한 후 "확인" 버튼을 클릭하여 네트워크 오퍼링을 생성합니다.

마이크로 세그먼테이션 네트워크 생성

마이크로 세그먼테이션을 사용하기 위해서는 가상머신에 연결하기 위한 네트워크 생성 시 해당 네트워크의 오퍼링을 위에서 생성한 마이크로 세그먼테이션 서비스가 가능한 오퍼링을 선택해서 생성해야 합니다.

Mold 화면에서 "네트워크 > 가상머신용 네트워크" 메뉴를 선택하여 "네트워크 추가" 버튼을 클릭한 후 다음과 같이 대화상자의 항목을 입력합니다.


네트워크 추가
Isolated
L2
shared
* 이름
Micro Segmentation VLAN 201 Shared Network
설명
Micro Segmentation VLAN 201 Shared Network
* Zone
ABLESTACK-PoC
물리 네트워크
Physical Network 1
* VLAN/VNI
201
VLAN ID/범위 중복 우회
Secondary VLAN 유형
없음
커뮤니티
isolated
비규칙
범위
모두
도메인
계정
프로젝트
* 네트워크 오퍼링
마이크로 세그먼테이션 공유 네트워크 오퍼링
IPv4
IPv4 게이트웨이
192.168.1.254
IPv4 넷마스크
255.255.255.0
IPv4 시작 IP
192.168.1.1
IPv4 종료 IP
192.168.1.253
DNS 1
8.8.8.8
DNS 2
1.1.1.1
IPv6
IPv6 게이트웨이
the gateway of the IPv6 network. Req...
IPv6 CIDR
the CIDR of IPv6 network, must be at l...
IPv6 시작 IP
the beginning IPv6 address in the IPv...
IPv6 종료 IP
the ending IPv6 address in the IPv6 n...
IPv6 DNS1
the first IPv6 DNS for the network
IPv6 DNS2
the second IPv6 DNS for the network
네트워크 도메인
network domain
IP 주소 사용 숨기기
취소
확인

'네트워크 추가' 대화상자에서 주의하여 입력해야 할 항목은 다음과 같습니다.

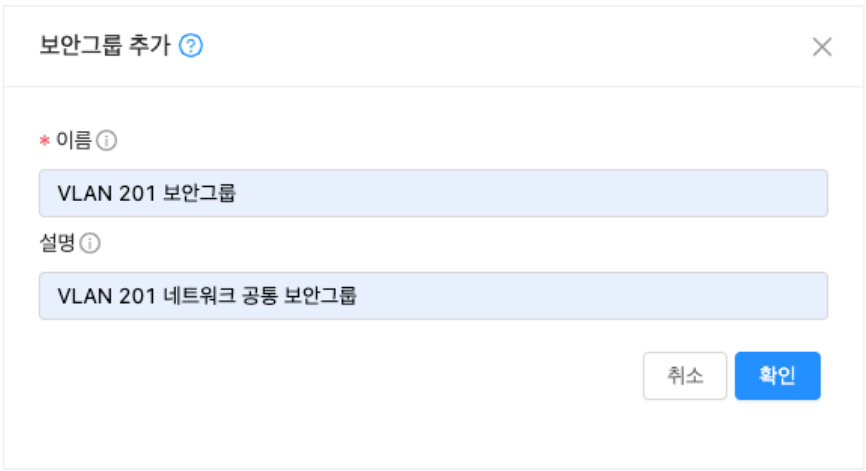
•물리 네트워크 : 마이크로 세그먼테이션 기능(Security Group)을 활성화 한 물리 네트워크를 선택
•VLAN/VNI : 적합한 VLAN ID 입력
•VLAN ID 범위 중복 우회 : 활성화
•네트워크 오퍼링 : 앞서 생성한 마이크로 세그먼테이션 공유 네트워크 오퍼링 선택
•IPv4 : 사용자 네트워크 환경에 맞는 네트워크 정보 입력

모든 항목을 설정한 후 "확인" 버튼을 클릭하여 네트워크를 추가합니다.

보안 정책 생성

마이크로 세그먼테이션 기능을 활성화 하면 Mold의 "네트워크" 메뉴에 "보안그룹" 메뉴가 활성화 됩니다. 해당 메뉴로 이동하여 보안 그룹 정책을 생성할 수 있습니다.

기본적으로 보안 그룹은 가상머신 네트워크에 대해 모든 outbound 트래픽은 허용되고, 모든 inbound 트래픽은 거부되는 default 보안 그룹이 제공됩니다. 만약 사용자가 조직 단위 또는 네트워크 단위로 보안 그룹을 생성하고 싶다면 해당 메뉴 화면에서 "보안그룹 추가" 버튼을 클릭합니다.

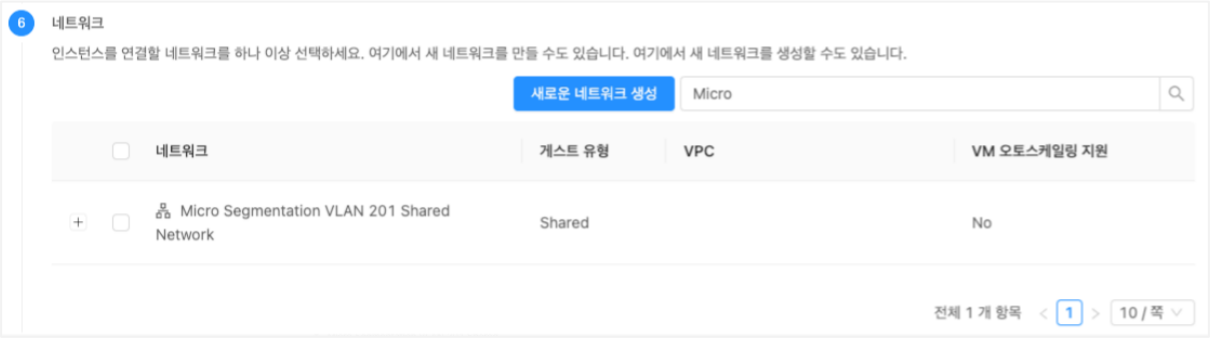


모든 항목을 입력한 후 "확인" 버튼을 클릭합니다.

새롭게 생성된 보안 그룹도 역시 default 보안그룹과 동일하게 outbound 트래픽은 허용, inbound 트래픽은 거부 정책이 설정됩니다.

가상머신 생성 및 보안 정책 설정

마이크로 세그먼테이션 기능이 활성화 된 네트워크를 준비한 후 해당 네트워크에 연결된 가상머신을 생성합니다.



위와 같이 마이크로 세그먼테이션을 적용하여 가상머신을 생성합니다.

본 예시에서는 해당 네트워크를 사용하는 가상머신 3개를 만들어서 마이크로 세그먼테이션이 정상적으로 작동하는지를 확인하도록 구성합니다. 생성하는 가상머신의 초기 IP 정보와 보안그룹 정보는 다음과 같습니다.

모든 항목을 입력한 후 "확인" 버튼을 클릭합니다.

새롭게 생성된 보안 그룹도 역시 default 보안그룹과 동일하게 outbound 트래픽은 허용, inbound 트래픽은 거부 정책이 설정됩니다.

가상머신 생성 및 보안 정책 설정

마이크로 세그먼테이션 기능이 활성화 된 네트워크를 준비한 후 해당 네트워크에 연결된 가상머신을 생성합니다.

가상머신명	네트워크	IP 주소	초기 보안그룹
SG-192-168-1-1	Micro Segmentation VLAN 201 Shared Network	192.168.1.1	VLAN 201 보안그룹
SG-192-168-1-2	Micro Segmentation VLAN 201 Shared Network	192.168.1.2	VLAN 201 보안그룹
SG-192-168-1-3	Micro Segmentation VLAN 201 Shared Network	192.168.1.3	VLAN 201 보안그룹

리눅스 가상머신은 기본적으로 ping과 ssh로의 상호 연결이 가능합니다. 하지만 마이크로 세그먼테이션이 적용된 가상머신의 경우 가상머신의 방화벽은 ping, ssh가 가능하도록 설정되어 있을지라도 상호 통신이 불가능합니다.

먼저 해당 가상머신의 방화벽 설정을 확인하면 다음과 같습니다.

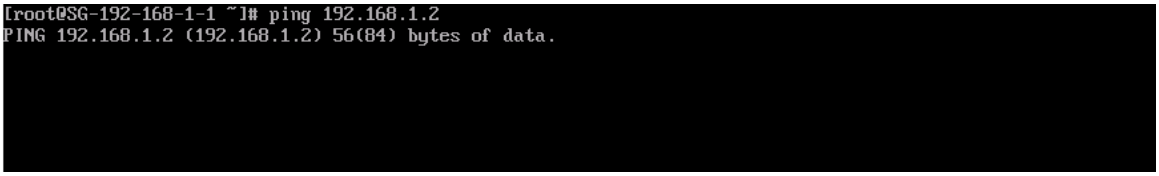
```
[root@SG-192-168-1-1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

각 가상머신을 확인하면 icmp-block-inversion이 no로 설정되어 있어서 icmp가 열려 있고, services에 ssh가 포함되어 있어 22번 포트가 열려 있는 것을 확인할 수 있습니다. 보안그룹이 설정되어 있는 상태에서 다음의 명령을 실행합니다.

```
Bash

ping 192.168.1.2
```

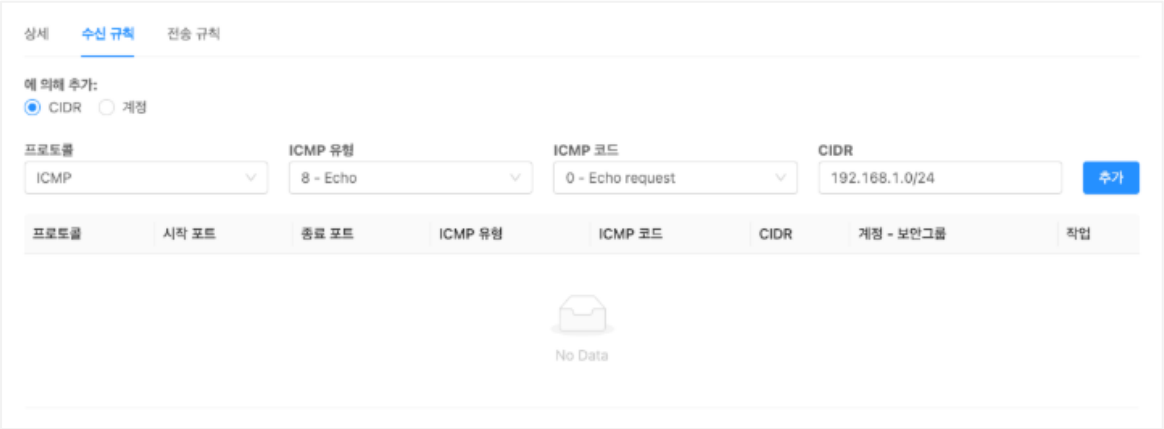
다음과 같이 가상머신 내부 방화벽 설정과는 달리, 보안그룹 설정에 따라 ping 요청에 대한 응답을 받을 수 없는 것을 확인할 수 있습니다.



보안정책 관리 및 업데이트

적용된 보안정책에 새로운 정책을 등록하거나 수정하는 것은 언제든 가능합니다. 가상머신 실행 중에도 해당 정책을 수정할 수 있으며 해당 정책은 바로 가상머신에서 확인할 수 있습니다.

예를 들어 가상머신 간 ping 명령이 가능하도록 변경하려면 "네트워크 > 보안그룹"으로 이동하여 정책을 등록하고자 하는 보안그룹을 선택하여 상세화면으로 이동한 후 "수신 규칙" 탭을 클릭하여 다음과 같이 정책을 추가합니다.



정책을 추가하면 해당 가상머신에서 즉시 ping 요청, 응답이 정상적으로 이루어지는 것을 확인할 수 있습니다.

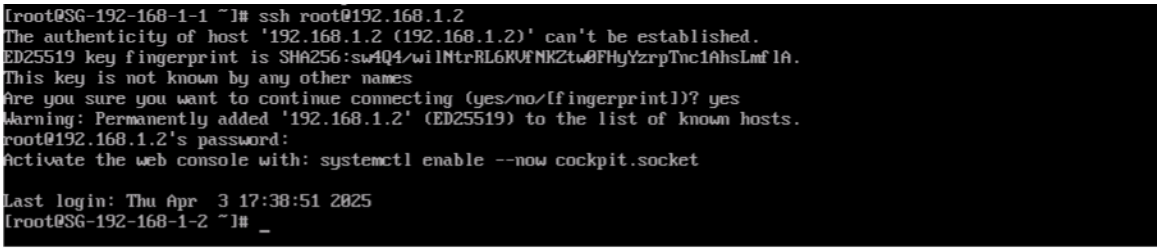
```
[root@SG-192-168-1-1 ~]# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=847 ttl=64 time=0.247 ms
64 bytes from 192.168.1.2: icmp_seq=848 ttl=64 time=0.233 ms
64 bytes from 192.168.1.2: icmp_seq=849 ttl=64 time=0.242 ms
64 bytes from 192.168.1.2: icmp_seq=850 ttl=64 time=0.198 ms
64 bytes from 192.168.1.2: icmp_seq=851 ttl=64 time=0.217 ms
64 bytes from 192.168.1.2: icmp_seq=852 ttl=64 time=0.191 ms
64 bytes from 192.168.1.2: icmp_seq=853 ttl=64 time=0.223 ms
64 bytes from 192.168.1.2: icmp_seq=854 ttl=64 time=0.230 ms
64 bytes from 192.168.1.2: icmp_seq=855 ttl=64 time=0.226 ms
64 bytes from 192.168.1.2: icmp_seq=856 ttl=64 time=0.245 ms
64 bytes from 192.168.1.2: icmp_seq=857 ttl=64 time=0.243 ms
```

해당 보안그룹에 ssh 서비스가 가능하도록 보안정책을 수정하여 정상적으로 ssh 연결이 가능하도록 수정합니다. 수정 전에는 다음과 같이 가상머신 내에서 ssh 접속이 불가능 합니다.

```
[root@SG-192-168-1-1 ~]# ssh root@192.168.1.2
ssh: connect to host 192.168.1.2 port 22: Connection timed out
[root@SG-192-168-1-1 ~]#
```

보안그룹에 다음과 같이 ssh가 가능하도록 보안정책을 추가합니다.

다음과 같이 ssh 접속이 정상적으로 이루어지는 것을 확인할 수 있습니다.



ABLECLOUD

All about data & cloud

주식회사 에이블클라우드 www.ablestack.co.kr

주소 | 서울시 영등포구 영신로 220, KnK디지털타워 1901호

연구소 | 대전시 대덕구 대화로 106번길 66, 펜타플렉스 810~812호

대표전화 | 02-456-7667

이메일 | sales@ablestack.co.kr

공식홈페이지