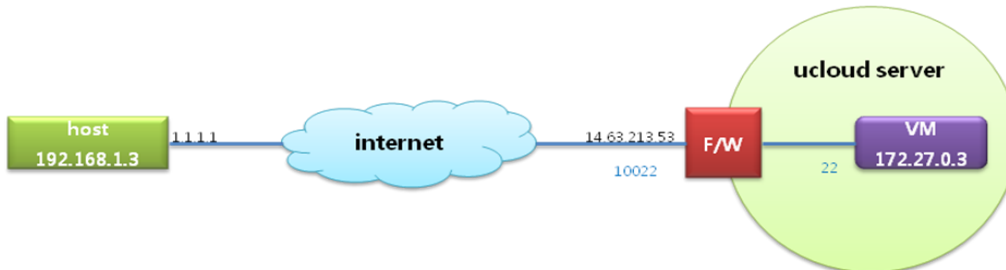


# Firewall 기능 사용법

## 1. Firewall 개요

인터넷으로부터 유입되는 패킷에 대하여 차단 또는 허용해주는 룰을 정의하는 기능입니다. ucloud server는 모든 패킷을 차단하는 것이 기본 정책이며 필요에 따라 허용할 룰을 정의할 수 있습니다.



## 2. 서비스 특징

- Firewall Rule 설정 메뉴: ucloud server > 네트워크 > Firewall

설명	Firewall	Port Forwarding	Load Balancer
Source CIDR	Protocol	Start Port	End Port
0.0.0.0/0	TCP		
0.0.0.0/32	tcp	333	333
			추가
			삭제

- 고객이 신청한 public IP에 대한 모든 트래픽은 기본적으로 차단됩니다.
- Source IP(CIDR 형식)를 지정하여 해당 IP에서 들어오는 트래픽에 한해 Port range를 지정하여 개방합니다.  
(예. FTP포트(21번)을 Port Forwarding 시 기존에는 Any IP에서 접속 가능하였으나, Firewall 기능을 이용하면 특정 IP만 선별적으로 접속 가능하게 설정이 가능합니다)
- 현재 Port Forwarding/Load Balancer를 추가하는 경우 모든 소스 IP(0.0.0.0/0)에 대해 해당포트는 자동으로 Open되도록 Firewall rule이 추가됩니다.

## 3. 설정 방법 예시

\* 고객 호스트에서 ucloud server로 SSH 접속하기 위한 Firewall rule 설정 방법

- 1) 고객의 ucloud server에 할당된 public IP에 고객 VM의 22번 port에 대하여 Port Forwarding이 설정되어 있어야 합니다.

(여기에서는 public IP 의 10022번 Port를 VM의 22번 port로 Port Forwarding 설정)

- 2) Port Forwarding 또는 Load Balancer rule을 추가/삭제 시 지정한 public port에 대하여 모든 IP/네트워크의 접근을 허용하는 Firewall Rule도 같이 추가/삭제 됩니다. 만약, 모든 IP/네트워크가 아닌 특정 IP/네트워크만의 접근을 허용하려면 다음과 같이 설정하시면 됩니다.

a. 고객 호스트에서 [www.whatismyip.com](http://www.whatismyip.com)에 접속하여 해당 호스트가 실제 인터넷에 접속할 때 사용하는 IP 주소를 파악 (1.1.1.1 이라고 가정)

b. Firewall 설정화면에서 아래와 같이 입력 후 rule 추가

- Source CIDR: 1.1.1.1/32

- Protocol: TCP

- Start Port: 10022

- End Port: 10022

#### 참고. Firewall 설정 입력 항목 설명

- 4.1 Source CIDR: ucloud server로 액세스를 허용하는 소스 IP 또는 네트워크 대역을 정의
- CIDR은 network 대역을 정의하는 방법입니다.
  - 0.0.0.0/0 은 모든 IP/네트워크의 접근을 허용하는 정책입니다.
  - 특정 호스트의 접근만을 허용하려면 '호스트IP/32'로 설정하면 됩니다.
  - 특정 네트워크의 접근을 허용하려면 '네트워크IP/MaskBit'로 설정하면 됩니다.  
(예. 1.1.1.0/24 는 1.1.1.2 ~ 1.1.1.254 대역의 네트워크로부터의 접근을 허용)
  - Source CIDR은 public IP이어야 합니다. ucloud server에 접근하려는 호스트의 실제 public IP 는 <http://www.whatismyip.com> 사이트 등을 통해 확인 할 수 있습니다.
- 4.2 Protocol: 접근을 허용할 protocol 정의
- TCP protocol을 사용하여 접근하는 IP/네트워크를 허용하려면 TCP를 선택합니다.
  - UDP protocol을 사용하여 접근하는 IP/네트워크를 허용하려면 UDP를 선택합니다.
  - ping을 허용하려면 ICMP를 선택합니다.
- 4.3 Start Port, End Port: 접근 허용할 public port 대역 정의
- 지정한 Start Port 부터 End Port 사이의 port에 대하여 접근을 허용하도록 설정합니다.
  - 포트는 1 ~ 65535까지 지정 가능합니다.
  - Start Port = 1, End Port = 65535 이면 모든 포트에 대한 접근을 허용합니다.