

경로와 방화벽

경로

모든 네트워크에는 다음과 같은 경로가 있다.

- 한 네트워크에 있는 여러 인스턴스가 서로 직접 트래픽을 전송할 수 있게 해주는 경로
- 네트워크 외부의 대상으로 패킷을 전달하는 기본 경로는

방화벽 규칙에서도 해당 패킷을 허용해야 한다.

방화벽

- VPC 네트워크는 분산형 방화벽으로 작동한다.
- 방화벽 규칙은 전체 네트워크에 적용된다.
- 연결은 인스턴스 수준에서 허용되거나 거부된다.
- 방화벽 규칙은 Stateful이다.
- 묵시적으로 모든 인그레스를 거부하고, 모든 이그레스를 허용한다.

Egress 정책

조건:

- 대상 CIDR 범위
- 프로토콜
- 포트

작업:

- 허용: 일치하는 이그레스 연결 허용
- 거부: 일치하는 이그레스 연결 차단

Ingress 정책

조건:

- 소스 CIDR 범위
- 프로토콜
- 포트

작업;

- 허용: 일치하는 인그레스 연결 허용
- 거부: 일치하는 인그레스 연결 차단