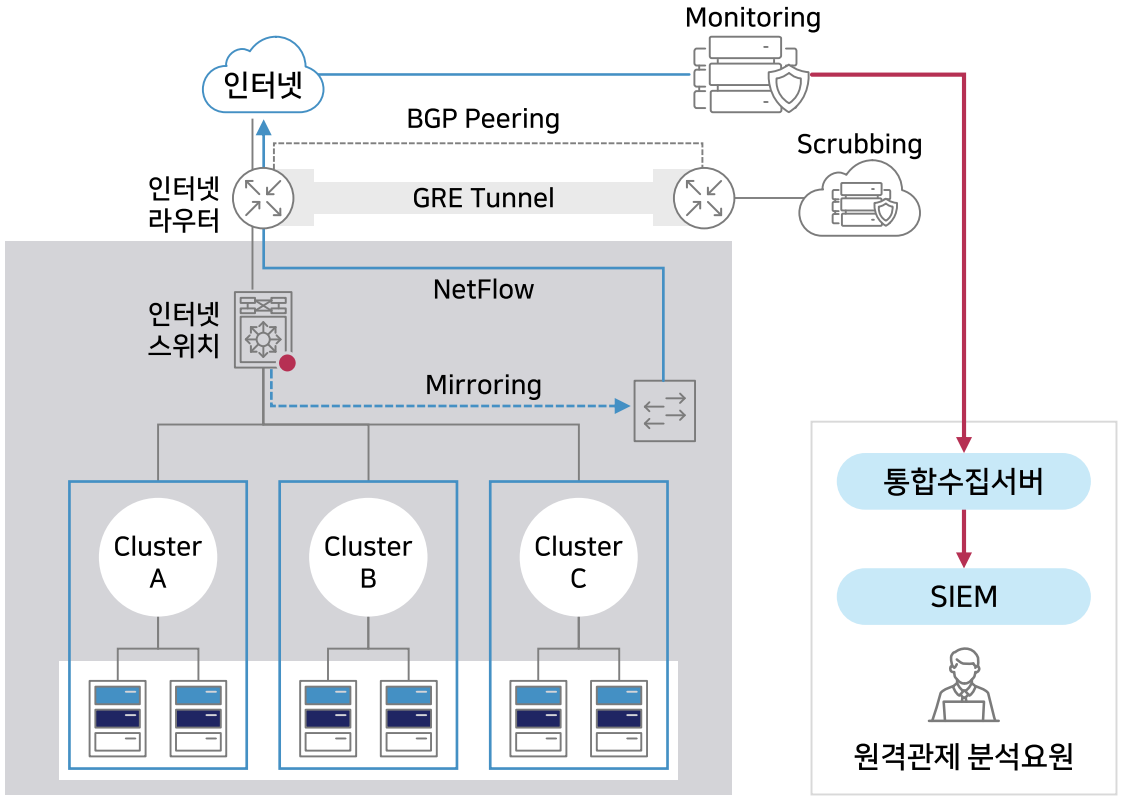
보안관제 서비스 – DDoS 관제

DDoS 관제는 웹사이트에 DDoS 공격 발생시 신속히 탐지하고 공격 트래픽을 차단하여 홈페이지가 정상적으로 동작하도록 보호하는 서비스입니다

DDoS 관제 구성



로그수집 및 이벤트 탐지/경보 체계

로그 수집

- DDoS 서비스는 NetFlow 정보에 기반한 트래픽 분석/DDoS 공격을 탐지
- 탐지 로그를 수집하여 통합수집서버로 전송
- 네트워크 프로토콜에 관계없이 고객 전체 네트워크를 보호하는 서비스
  - BGP전파를 통해 트래픽을 우회하며, GRE 터널을 이용해 정상 트래픽 전달

이벤트탐지

- **탐지** : 학습된 임계치 이상의 대용량 트래픽 탐지
- **분석** : 서비스 영향도 파악
- **차단** : 트래픽 유입경로 변경 및 공격 트래픽 필터로 차단

경보/통보 기준

확인	긴급
• 단순 임계치 Peak • 서비스 영향도 파악 • 메일/유선 통보	• 서비스 영향도 파악 • 공격 차단 • 긴급상황전파(유선/메일)