1. KorealT 사이트에서 제안서에 기재된 보안 요구사항 일부를 아래의 그림에서 확인한 후 보안 요구사항에 대한 인적, 물적 자원을 나열하고 무진동 차량 배송을 통한 일정 계획을 수립하시오.

요구사항 분류		보안
요구사항 고유번호		SCR-01
요구사항 명칭		Network 비인가 접근 통제
요구사항 상세 설명	정의	서비스에 대한 Network Level 비인가 접근 통제
	세부 내용	o 지정된 Traffic만 허용, 기타 Traffic은 차단 o 내부 Network에서 비인가 Web Server 접근 차단 ※ 주식, Game, 도박, 성인 Site 등 o Web, Mail 기반 Traffic의 첨부 File 악성코드 검사 o IP / MAC Address Binding o 기타

요구사항 분류		보안
요구사항 고유번호		SCR-02
요구사항 명칭		알려진 공격 탐지 및 차단
요구사항 상세 설명	정의	Web, Database 등의 기본적인 Application에 대한 위협 차단
	세부 내용	o Signature 기반 Network Level의 공격 차단 o 사용자 정의 기반 Signature 관리 o DDOS 공격 탐지 및 차단 o 기타

▶ **SCR-01** : Network 비인가 접근 통제

- 지정된 트래픽만 허용 / 다른것은 차단
- 내 / 외부망 분리
- 악성코드 검사 및 사이트 접근 통제

▶ **SCR-02** : 알려진 공격 탐지 및 차단

- 애플리케이션, 웹, DB기반 공격 차단
- Signature 기반 공격 차단
- DDOS공격 탐지 및 차단

▶ **인적 자원**

- 보안 아키텍트 (1명)
- 네트워크 엔지니어 (2명)
- 보안 솔루션 전문가 (2명)
- 시스템 관리자 (1명)
- QA/테스트 인력 (1명)

▶ 물적 자원

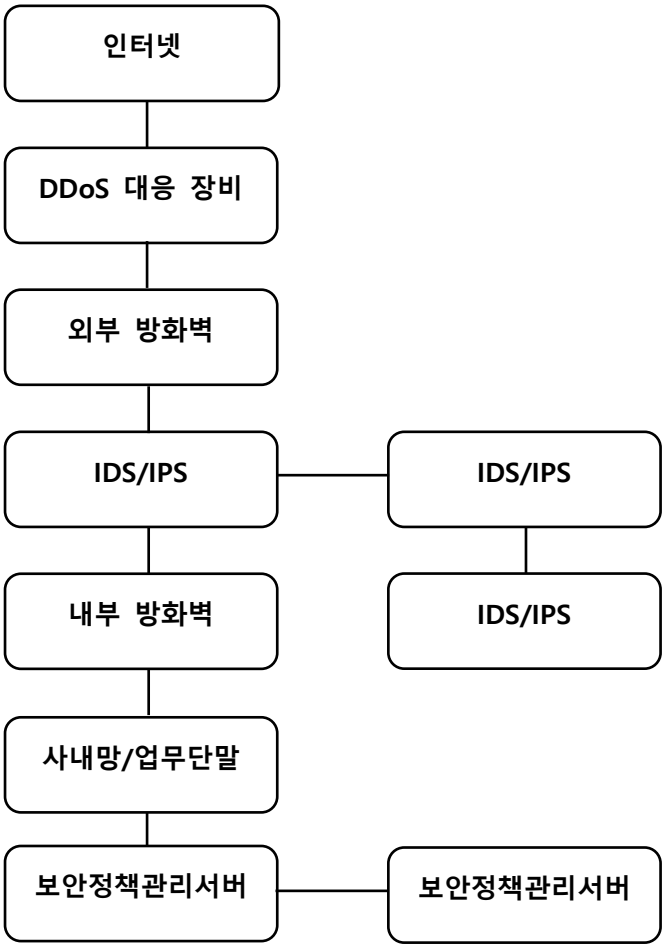
- 설치 도구(펜치, 케이블) (1세트)
- 방화벽 (2대)
- 침입 탐지 시스템 (2대)
- 웹 방화벽 (1대)
- 악성코드 검사 솔루션 (1대)
- 보안정책 관리 서버 (1대)
- 무진동 차량 (1대)

▶ 무진동 차량 배송을 통한 일정 계획

- 보안 장비 입고 및 검수
- 무진동 차량 적재 및 출발 준비
- 현장 도착 및 장비 반입
- 장비 설치 및 시스템 연동
- 기능 점검 및 시뮬레이션 공격 테스트
- 운영자 고육 및 기술 인계

2. 1번에서의 보안 범위 설정을 통해 보안 기술 적용 위치를 도출하여 표로 만들고 네트워크 다이어그램에 각각의 위치를 표기하고 보안 기술간 상호 관계에 대해 서술하시오.

요구사항 ID	보안 기술명	적용 위치	목적
SCR-01	방화벽	외부망 ↔ 내부망 경계	비인가 트래픽 차단, 포트/프로토콜 제어
	IP/MAC Address Binding	내부망 (사내 단말/서버)	내부 비인가 단말 접근 통제
	안티바이러스 솔루션	Web, Mail 서버 앞단	첨부파일 등 악성코드 탐지
SCR-02	침입탐지시스템 (IDS/IPS)	방화벽 내부 또는 병렬 구간	네트워크 기반 시그니처 공격 탐지/차단
	웹 방화벽 (WAF)	웹 서버 앞단	SQLi, XSS 등 애플리케이션 공격 차단
	DDoS 대응 장비	방화벽 외부 또는 ISP 연동 구간	대량 트래픽 공격 탐지 및 차단
공통	보안 정책 관리 서버	내부 보안존	시그니처 관리, 로깅 / 모니터링



▶ 보안 기술 간 상호관계 설명

- 방화벽(Firewall)은 외부와 내부 네트워크 간의 경계 역할을 하며, 모든 통신 흐름을 필터링하여 비인가 접근을 차단합니다. 내부망과 DMZ 영역 간에도 별도로 구성되어 세분화된 통제 역할을 합니다.

- DDoS 대응 장비는 인터넷단 상단에 위치하여 대량 트래픽을 사전에 식별, 차단함으로써 방화벽 및 IDS/IPS 장비의 과부하를 방지합니다.

- IDS/IPS는 방화벽을 통과한 트래픽을 분석하여 알려진 공격(Signature 기반) 및 이상 트래픽을 탐지하며, IPS 기능이 활성화된 경우 실시간 차단도 수행합니다.

- WAF는 웹 트래픽에 특화된 보안 장비로, 웹 애플리케이션 공격(SQL Injection, XSS 등)을 방어하며 Web Server 앞단에 위치하여 사전 필터링 역할을 합니다

- IP/MAC Binding은 내부 사용자의 IP와 MAC 주소를 1:1로 고정하여 위장 또는 임의 변경된 단말 접근을 차단합니다.

- 안티바이러스 솔루션은 Web 및 Mail 서버의 첨부파일, 전송 데이터에 포함된 악성 코드 및 스크립트를 탐지하여 시스템 감염을 방지합니다.

- 보안정책 관리 서버는 IDS/IPS, WAF, DDoS 장비의 시그니처 및 정책을 통합 관리하고, 각 보안 장비에서 수집한 로그를 중앙 집중하여 분석/감사 기능을 수행합니다.

3. KoreaIt 보안 설계에 따른 보안 구축 시 직접비용과 간접비용의 종류에 대해 서술하고 구축 일정을 관리하기 위한 기법 중 PERT 기법에 대해 서술하시오. 또한 보안구축계획서에 포함되는 일반적인 내용 중 보안 구축 범위와 검증 방법을 포함하여 간단하게 보안구축계획서를 작성하시오.

▶ **직접비용**

- 장비 구매비 (방화벽, IDS/IPS, WAF 등 하드웨어)
- 보안 솔루션 도입비 (소프트웨어 라이센스 및 설치비용)
- 인건비 (설계, 구축, 테스트에 투입되는 인력비)
- 운송비 (무진동 차량 운송비, 장비 물류 관련 운송 비용)
- 교육비 (관리자 및 운영자 보안 시스템 사용 교육 비용)

▶ **간접비용**

- 서비스 중단 비용 (설치 기간 동안 발생할 수 있는 서비스 중단 손실)
- 유지보스 및 운영비 (시스템 유지보수 계약, 정기 점검, 기술지원 비용)
- 전력 및 공간 비용 (보안 장비 운영에 따른 전기, 냉각, 공간 사용 비용)
- 문서화 및 인증 대응 비용 (ISMS 등 인증대응 및 문서화 작업 비용)
- 대체 인력 비용 (구축 기간 동안 대체 인력을 투입해야 할 경우의 비용)

▶ **PERT 기법 (Program Evaluation and Review Technique)**

- 정확한 일정을 산출할 수 없을 경우 많이 사용
- 프로젝트를 작업단위로 분할하여 각 작업 간의 선후 관계를 도식화
- 각 작업의 기간을 세가지 추정값으로 예측 (낙관적 시간, 비관적 시간, 가장 가능성 높은 시간)
- 예상 일정 = (비관 + 4 x 평균 + 낙관) / 6
- 주 경로를 분석해 일정 지연 가능성 및 리스크 파악

▶ 보안 구축 계획서

1. 프로젝트 개요

사업명: Korealt 보안 시스템 구축

목표: 외부 비인가 접근 차단 및 웹 공격 방어 체계 구축

기간: 2025년 6월 1일 ~ 2025년 6월 20일 (20일간)

2. 보안 구축 범위

구분	대상 시스템	주요 기능
네트워크 보안	방화벽, DDoS 대응 장비	외부 트래픽 제어, 공격 차단
시스템 보안	IDS/IPS, WAF	시그니처 기반 공격 탐지 및 웹방어
엔드포인트 보안	안티바이러스, IP/MAC Binding	악성코드 탐지, 내부 단말 인증
관리 체계	정책 관리 서버	시그니처 통합 관리, 로그 수집

3. 보안 검증 방법

구분	검증 항목	방법
기능 검증	장비 동작, 시그니처 탐지 여부	시뮬레이션 공격 도구 이용
성능 검증	트래픽 처리량, 응답 속도	Traffic Generator 사용
운영성 검증	정책 관리, 로그 분석	보안 운영자 실습 테스트
취약성 검증	시스템 취약점 존재 여부	모의 해킹(Penetration Test) 진행

4. 구축 일정

D-5: 장비 입고 및 무진동 차량 탑재

D-3: 현장 반입 및 설치

D-Day: 운영 및 검증 수행

D+1: 인계 및 교육