사내망 구성도 분석 및 보안 강화 제안 보고서

1. 분석 개요

이 보고서는 주어진 사내망 구성도를 기반으로, 내부망/외부망/DMZ 영역별 구성 구조를 분석하고 각 장비의 역할과 배치 이유를 설명한 뒤, 보안 강화를 위한 개선 제안을 포함합니다.

---

2. 네트워크 영역 구분 및 구성도 해석

외부망 (External Network)

- **라우터 #1, #2**: 인터넷 게이트웨이, 중복 구성을 통해 가용성 확보
- **방화벽 #1, #2**: 인터넷에서 유입되는 트래픽 제어 및 필터링
- **IDS/IPS #1, #2**: 침입 탐지/차단 기능 수행, 실시간 공격 대응을 위한 장비

➡ 외부망은 인터넷과 내부망 사이에서 **최초 방어선 역할**을 수행합니다.

DMZ (Demilitarized Zone)

- **웹 방화벽 #1, #2**: 웹 애플리케이션 보안 담당 (XSS, SQLi 등 탐지)
- **DMZ 스위치 #1, #2**: DMZ 장비 간 트래픽 분산 및 연결
- **L4 스위치 #1, #2**: 로드 밸런싱 (웹 서버 트래픽 분산)
- **웹서버, 파일업로드 서버**: 외부 사용자에게 공개되는 서버

➡ DMZ는 외부와 내부망 사이에서 **완충지대 역할**을 하며, 외부에 공개되는 자원을 이곳에 배치함으로써 내부망 보호 효과를 가집니다.

내부망 (Internal Network)

- **L3 스위치, L2 스위치**: 부서 간 통신과 세분화된 네트워크 경로 구성
- **내부 서비스 서버**: ERP, 그룹웨어, 사내 포털 등의 서비스 제공

- **DB 서버**: 중요 데이터 저장, DMZ와 직접 연결되지 않음
- **SAN/NAS 스토리지**: 백업 및 고용량 데이터 저장 장치
- **정보지원팀, 경보시스템, 업무단말**: 사용자 단말 및 통합보안 관리 시스템

➡ 내부망은 **업무 연속성, 데이터 보호, 권한 기반 접근 제어**가 핵심입니다.

---

3. 장비 배치 이유 및 특징

장비	역할	배치 이유
IDS/IPS	침입 탐지 및 차단	외부망 유입 트래픽 감시 및 대응
웹 방화벽	웹 공격 방어	DMZ의 웹서버 보호, HTTP/S 필터링
L4 스위치	로드 밸런싱	고가용성, 부하 분산
DB 서버	민감 정보 저장	내부망 깊숙한 위치, 직접 노출 차단
NAS/SAN	백업 및 스토리지	안정적 데이터 저장 및 이중화
L3/L2 스위치	라우팅 및 부서별 분리	부서 간 네트워크 흐름 분리 및 제어

---

4. 보안 강화 제안

추가할 장비/기능

제안 항목	기대 효과
AI 기반 WAF	자동화된 지능형 웹 공격 대응
ZTNA (Zero Trust Network Access)	사용자/디바이스 기반 인증 중심 접근제어
NAC (Network Access Control)	허가된 단말만 접속 허용, 내부 보안 강화
SIEM	로그 통합, 위협 탐지, 사고 대응 분석
이중화 DR 센터	장애 시 재해 복구 체계 확보

제거/통합 고려

항목	고려 사유
RC4/MD5 기반	TLS 취약 알고리즘 제거

항목	고려 사유
서버 중복 L2 스위치	과잉 중복 시 비용 증가 → 최적화 필요

5. 결론

- 주어진 구성도는 기본적인 **계층형 보안 설계 원칙**을 준수하고 있음
- 다만 **TLS 보안 수준, 지능형 위협 대응, 단말 인증** 측면에서 현대화가 필요함
- 본 보고서를 기반으로 사내망 보안 강화 전략을 수립할 수 있음