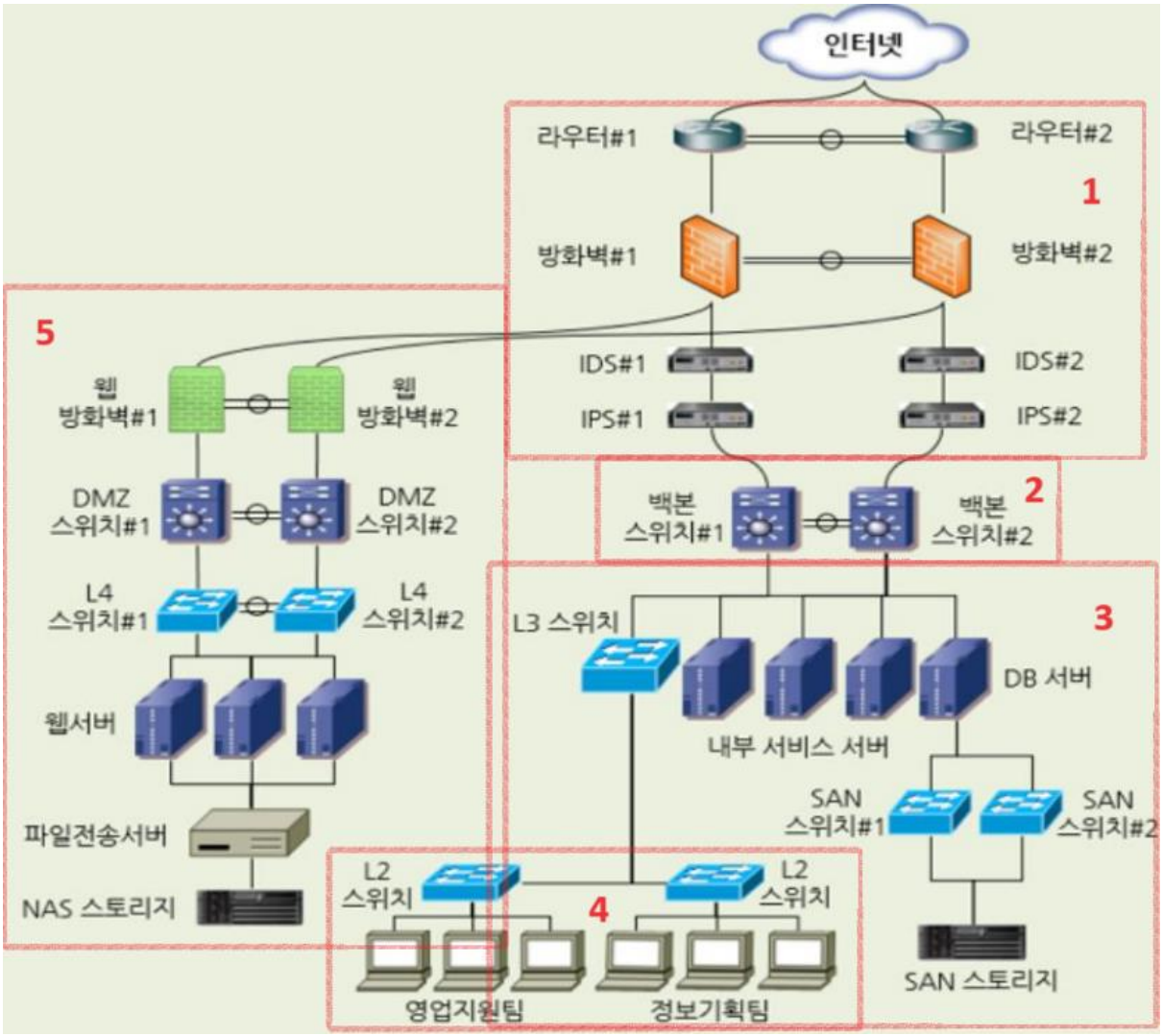
사내망 구성도 분석

내부망, 외부망, DMZ 영역별 장비 구성과 배치 이유 설명

하단의 구성도를 기반으로 사내망 구성 형태를 이해하기 위한 보고서입니다. 이미지에 표시된 번호별로 구역을 나누어 설명합니다.



1. **Internet Zone**
   - 목적: 외부 인터넷과의 연결을 담당하며 DMZ Zone과 통신
   - 구성: 외부 라우터, 방화벽, IDS, IPS

- 외부 사용자와의 통신이 가능하며 내부망과 직접 연결되지 않아 보안성이 향상됩니다. 라우터는 외부 ISP와 연결되며 NAT 및 QoS를 설정할 수 있습니다. 방화벽은 외부에서 들어오는 트래픽을 1차적으로 필터링합니다. 이들은 외부 공격을 차단하고 내부망으로 접근을 통제하기 위해 구성합니다.

2. **Backbone Switch**
   - 목적: 모든 Zone을 고속으로 연결하는 중심 스위치
   - 구성: 라우터 기능 탑재된 멀티레이어 스위치
   - 모든 Zone을 안정적으로 연결하고 네트워크 병목 현상을 방지합니다. VLAN 및 QoS 설정으로 유연한 트래픽 제어가 가능합니다. 이중화를 통해 장애 발생 시 자동으로 우회 가능합니다.

3. **Server Zone**
   - 목적: 내부 업무용 서버를 집중 배치하여 보안 및 관리 효율화
   - 구성: DB 서버, SAN 스토리지 등
   - 민감한 정보를 보호하고 서버 간 통신을 최적화합니다. 보안 정책 적용이 용이합니다.

4. **Worker Zone**
   - 목적: 일반 직원들의 단말기 및 업무 환경 제공
   - 구성: PC, 노트북, 프린터 등
   - 사용자 단말기 격리로 보안을 강화합니다. 내부 자원 접근 제어가 가능하며 악성코드 감염 시 확산 방지 및 사용자 모니터링이 용이합니다.

5. **DMZ Zone**
   - 목적: 외부에 노출되는 서버를 배치하여 내부망을 보호합니다.
   - 구성: 웹 서버, WAF(웹 공격 방화벽), FTP 서버, NAS 스토리지 등

- 외부에서 접근 가능한 서비스를 운영하고 외부 공격에서 격리될 수 있습니다. 내부망과 이중 방화벽으로 분리하여 보호할 수 있습니다. 침입 탐지 시스템과의 연계가 용이합니다.

✧ 사내망 보완 제안 사항

1. Server Zone에 IDS/IPS를 설치하여 내부 트래픽을 감시하고 이상을 빠르게 탐지합니다. Server Zone은 DB, ERP, AD 등 중요 시스템이 집중된 영역으로 침입자가 접근할 경우 치명적인 피해가 발생할 수 있습니다. IDS는 탐지 및 경고, IPS는 탐지 후 즉시 차단 기능을 제공하여 능동적인 보안 대응이 가능합니다. 서버 간 통신 흐름을 분석하여 제로데이 공격이나 내부 이상 행위도 조기에 식별 가능합니다.

2. Worker Zone에 NAC를 설치하여 접속 제어 및 보안 상태 확인을 통해 비인가 접근 및 감염 확산을 방지합니다. 직원 단말기는 가장 취약한 보안 지점 중 하나로 악성코드 감염이나 비인가 USB 사용 등으로 인해 내부망 위협이 발생할 수 있습니다. NAC는 사용자 인증, 단말기 보안 상태 검사(OS 패치, 백신 설치 여부 등), 정책 기반 접근 제어를 수행합니다. BYOD 환경이나 원격 근무 시에도 접속 장비의 보안 상태를 검증하여 위험 요소를 사전에 차단할 수 있습니다.