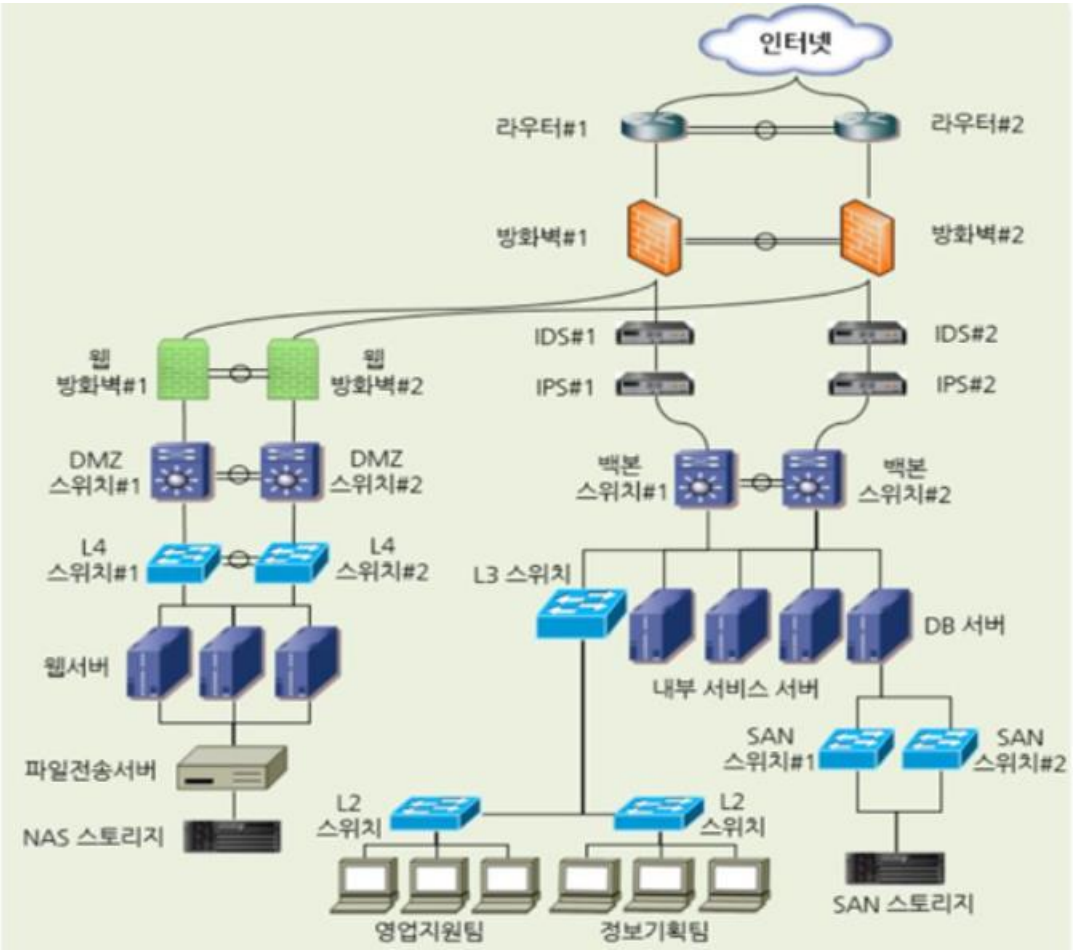
사내망 구성도 분석

내부망, 외부망, DMZ 영역별 장비 구성과 배치 이유

26AI 조영규

목차

1. 사내망 구성도



1.1 보안망 구성

- 회사 대 회사로 서비스 연동을 하는 대외망을 사용하는 것이 아니면. 일반적으로 방화벽을 기준으로 내부망, 외부망, DMZ 3가지 망으로 구성된다.

1.2 내부망

- Intranet (Private/Trust Zone)
- 물리적으로 분리된 망
- 접근 통제 시스템에 의해 인터넷으로 직접 접근이 불가능하도록 통제/차단되어 있는 구간
- 조직 내부 직원만 접근이 가능하다.

1.3 외부망

- Internet (Untrust Zone)

- 인터넷과 직접 연결된 네트워크 영역으로, 외부 사용자나 인터넷을 통해 외부에서 직접 접근이 가능한 구간이다.

- 보안 위협에 가장 많이 노출된다.

1.4 DMZ

- DMZ (public/Service Zone)

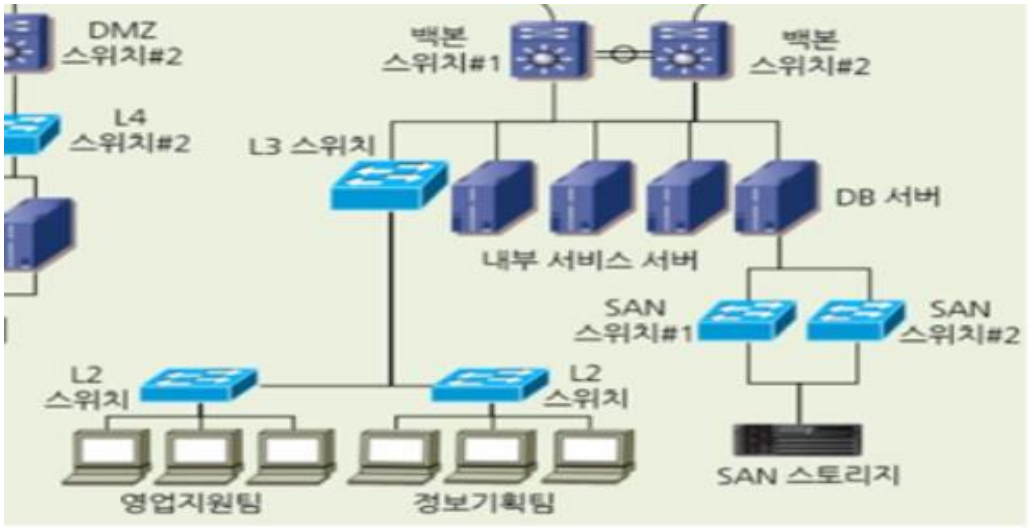
- 외부망과 내부망 사이에 위치한 중간지점으로, 접근 통제 시스템을 통해 접근 통제를 수행한다.

- 외부에 서비스를 제공하면서 내부 자원/시스템을 보호하기 위해 외내부망 사이에 접근 통제를 수행한다.

- 침입 차단 시스템으로 보호한다. (방화벽, IDS/IPS 등)

2. 각 구역별 분석

2.1내부망



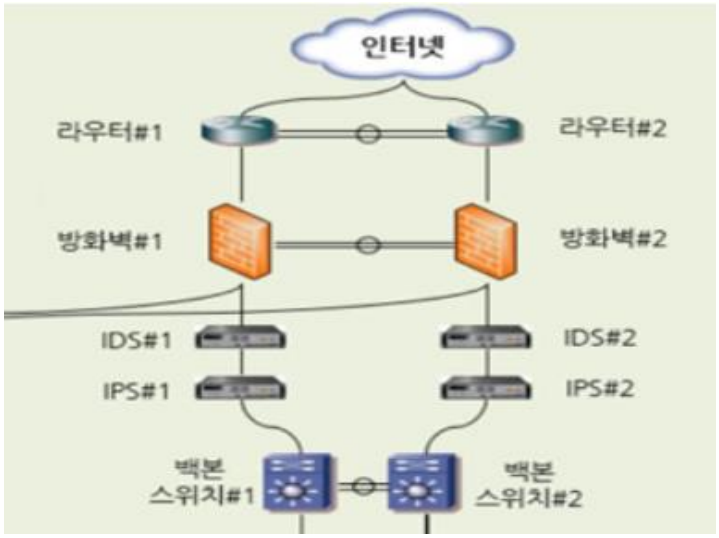
2.1.1 주요 배치 장비

- 내부망에는 내부 서비스 서버, 데이터베이스 서버, 사내 부서의 end-point, 스토리지 등이 있는 것을 확인할 수 있다.

- 내부망은 보안 수준이 가장 높고, 외부의 접근을 차단하기 때문에 보안이 중요한 자산들 (DB, WAS, Storage, 업무 서버 등) 위주로 배치가 되어 있다.

- 또한, 사내 직원들이 이용하는 내부 사용자존이 구성되어 있다.

2.2 외부망



2.2.1 주요 배치 장비

- 외부망, 인터넷망은 인터넷에 직접 연결되어 있어 보안 수준이 가장 낮다.

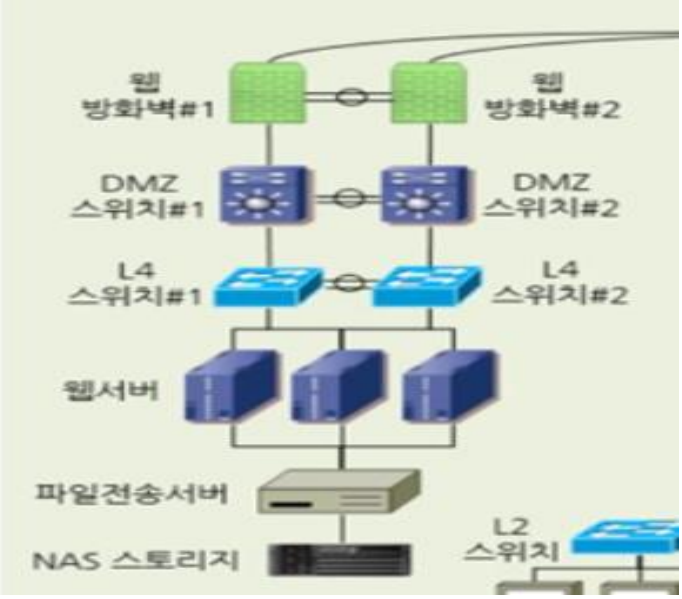
- 라우터를 거쳐온 데이터들을 방화벽을 통해 1차적으로 걸러내고, IDS, IPS를 통해 2차적으로 걸러낸 패킷들을 내부망 또는 DMZ로 전달한다.

- 방화벽만으로는 완전한 차단이나 접근 제어가 불가능해 IDS나 IPS와 같은 장비를 사용하여 보완을 한다. 특히, 악성 코드에 대한 공격을 방어하기 위해서는 IDS/IPS와 같이 7계층 데이터까지 확인할 수 있는 기능이 필요하다.

- IDS는 침입 탐지 시스템으로, 공격을 탐지하여 관리자에게 알리는 기능을 한다. 차단 기능도 있어 IPS 자리에 사용할 수도 있지만, 약한 성능을 가지고 있다. NIDS와 HIDS가 존재하며, NIDS는 네트워크 상에서 일어나는 침입 시도를 탐지하고, HIDS는 호스트의 자원 사용, 로그 등을 분석하여 침입 여부를 탐지한다.

- IPS는 IDS의 탐지 기능과 방화벽의 차단 기능을 결합한 장비로, 이상 행위 탐지를 통해 알려지지 않은 공격 패턴에 대응한다. 공격에 대한 사전 방지를 조치하는 것으로 In-Line 방식으로 설치 및 운영한다. (In-Line: 물리적 경로 상에 장비를 설치. 모든 트래픽을 감지할 수 있다.)

2.3 DMZ



2.3.1 주요 배치 장비

- DMZ는 내부망과 외부망 사이에 위치하여 양쪽에서 서비스를 이용할 수 있도록 해주는 네트워크 영역이다. 외부에 서비스를 제공하면서도 내부망을 노출시키지 않고 보호하는 역할을 한다.

- DMZ 스위치를 통해 방화벽을 지나온 트래픽들을 DMZ 서버로 전달하고, 내부망과 DMZ 사이의 트래픽 흐름을 제어한다.

- DMZ는 외부에 서비스를 제공하기 위한 서버들을 배치한다. (웹서버, 파일 전송 서버 등)

3. 추가할 장비

- 기존 망 구성에서 장비를 추가한다면, 보안 관제를 위한 장비들을 추가로 설치할 것이다.
- 내부망과 DMZ 사이 또는 내부망에 관제망을 설치하여 보안을 높일 것이다.
- 통합 로그 관리 시스템과 관리 서버, 네트워크 장비를 통합 관리하는 NMS, 서버의 하드웨어 자원과 운영체제, 애플리케이션 등을 통합 모니터링하는 SMS, 보안 장비 및 로그를 통합 관리하는 ESM 장비를 설치하여 보안성을 높여 내부망을 지킬 수 있도록 할 것이다.