인프라 보안 구축 프로젝트

2025

01. 목표시스템 구성도

운영시스템 현황

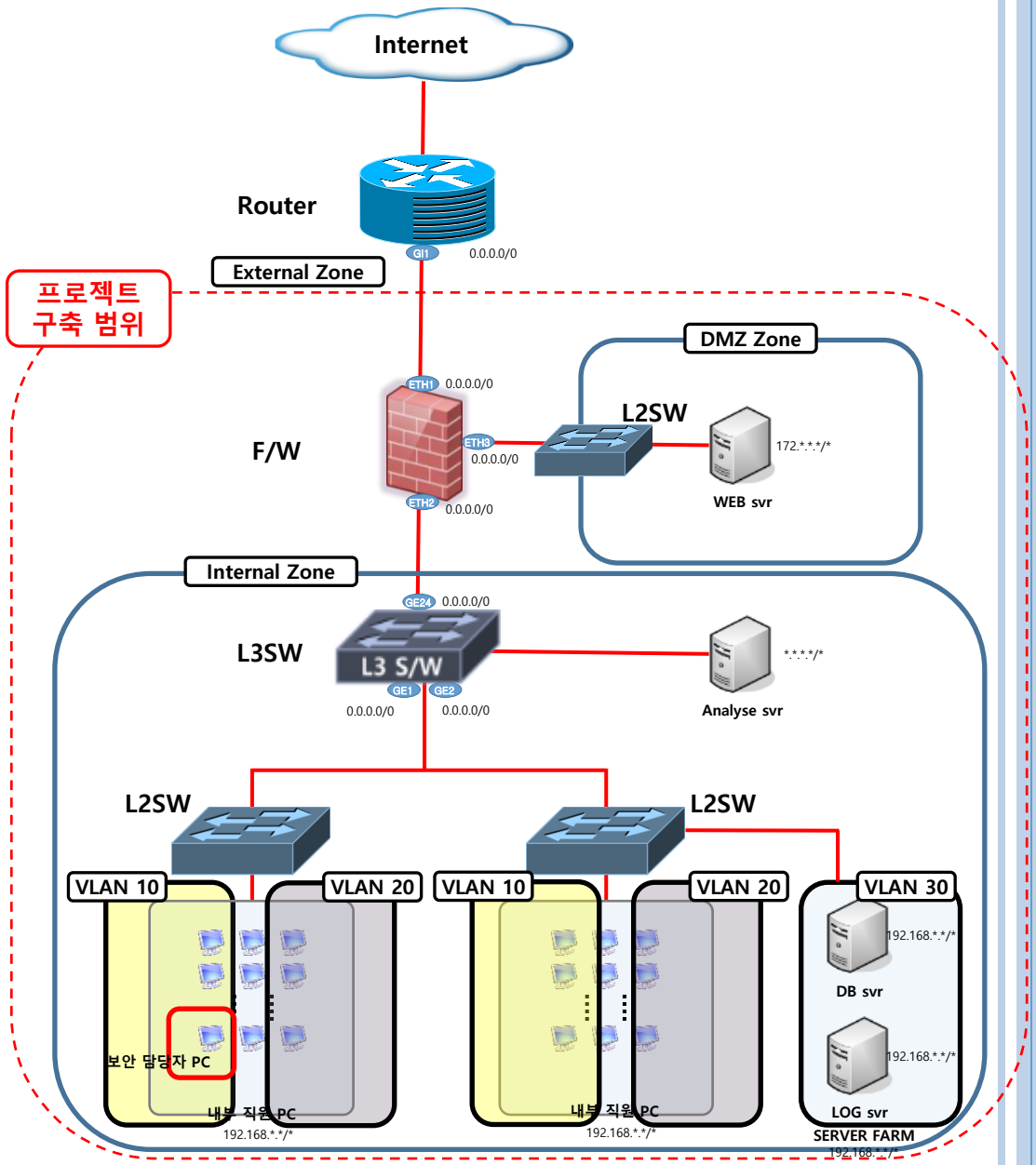
방화벽 : Ahnlab Trusguard 50B

L3 스위치 : CISCO C3650

L2 스위치 : CISCO C3650

서버 : Ubuntu or Rocky linux or
Windows Server 중 선택

기타 툴 및 S/W
- Apache web app.
- Mysql DBMS
- Wireshark
- .....



02. 프로젝트 시나리오

- 스타트업 IT 기업인 CB 정보통신의 인프라 보안 구축 프로젝트를 수주하여 시스템을 구축할 예정이다.
  - **프로젝트 수행기간 : 2025.08.28 ~ 11.06**

    o 설계, 구축, 산출물(PPT+영상) 제작 전체 수행

- 프로젝트 요구사항은 다음과 같다.
  - **네트워크 대역 정의**

    1. 내부 / 외부 / DMZ 영역 분리

    o 내부 영역 : 사용자 네트워크 대역 2개, SERVER FARM 네트워크 대역 1개 운영

    - 192.168.x.x/24

    o DMZ 영역 : WEB서버 네트워크 대역 1개 운영

    - 172.16.x.x/24

    o NAT 설정을 위한 공인IP를 제외한 모든 IP는 임의의 사설IP대역을 설정하여 운영

    - NAT IP 별도 안내

02. 프로젝트 시나리오

- 프로젝트 요구사항은 다음과 같다. (계속)
  - **시스템 운영 정책**

1. 대민 서비스 WEB서버 1대 운영(DMZ 영역)
   o 게시판 기능을 보유한 웹 페이지(DBMS 연동)
2. DMZ WEB서버와 연동된 DB서버 1대 운영(내부 SERVER FARM)
   o DBMS : mariadb or mysql 구축
3. 시스템 로그 관리 및 백업을 위한 LOG서버 운영(내부 SERVER FARM)
   o RAID-1 기능을 활용하여 방화벽, switch syslog 디렉터리 설정
   - 디스크 용량 : 5GB*2EA / mount point : /var/log/syslog
4. 각 시스템별 hostname을 중복되지 않도록 설정

02. 프로젝트 시나리오

- 프로젝트 요구사항은 다음과 같다. (계속)
  - **보안 운영 정책**

1. 보안시스템(방화벽)의 관리자 원격 접속(web console)은 내부 보안 담당자 1명만 접속 가능하도록 접근제어 설정

o 방화벽 GUI 메뉴에서 설정

2. 방화벽

o NAT정책 - SNAT(dynamic NAT)

- 공인IP는 프로젝트 진행 시 IP/SM 안내
- 내부 직원 PC의 사설IP는 할당받은 공인IP를 통해 내부 → 외부 통신

o NAT정책 - DNAT(static NAT)

- DMZ web서버는 할당받은 공인IP를 통해 내/외부 → DMZ 통신

02. 프로젝트 시나리오

- 프로젝트 요구사항은 다음과 같다. (계속)
  - **보안 운영 정책(계속)**

    2. 방화벽 (계속)

    o Packet Filtering 정책

    - 내부 직원은 외부의 모든 네트워크로 접속 가능하도록 설정
    - DMZ web서버의 원격 접속은 내부 보안 담당자 1명만 접속 가능하도록 설정 (SSH or RDP)
    - DMZ web서버의 웹페이지 접속은 내/외부에서 누구나 접속 가능하도록 설정
    - DMZ web서버와 내부 서버 팜 DB서버는 web↔DB 연동 port만 통신 가능하도록 설정
    - 악성코드 유포 의심 IP대역(210.95.199.0/24)에 대해 내부/DMZ ↔ 외부 양방향 통신 차단
    - 내부 서버 팜 로그서버는 DMZ web서버, 방화벽 시스템 로그를 받을 수 있도록 설정
    - 내부 서버 팜 대역은 외부에서 접속할 수 없도록 설정
    - NTP서버와 내부 시스템의 연동을 위한 허용 정책 설정

02. 프로젝트 시나리오

- 프로젝트 요구사항은 다음과 같다. (계속)
  - **보안 운영 정책(계속)**

3. Network switch

o 내부 사설 IP를 외부/DMZ와 통신할 수 있도록 L3 switch에서 static routing 설정

o L3 switch와 방화벽 사이 물리적 연결 구간은 내부에서 중복되지 않는 ip 대역을 지정하여 구간 네트워크로 구성

o 비 인가자의 스위치 접근 제어를 위해 원격접속 시 banner/login/enable password 설정

- banner : '비인가자 접근 금지' 관련 영문 문구 삽입
- enable password : 1234 설정

o 내부 영역 L2 스위치는 VLAN ID 3개 생성하여 VLAN 구성, 스위치 간 trunk 기능으로 VLAN ID 1, 10, 20, 30 공유

o L2 switch interface 구성

- 각 스위치별 1~10번 interface : VLAN 10 할당 (내부 사용자 대역)
- 각 스위치별 11~20번 interface : VLAN 20 할당 (내부 사용자 대역)
- L2 switch#2 21~23번 interface : VLAN 30 할당 (내부 서버 팜 대역)
- 각 스위치별 24번 interface : trunk 설정, L3 switch와 uplink port 연결

02. 프로젝트 시나리오

- 프로젝트 요구사항은 다음과 같다. (계속)
  - **보안 운영 정책(계속)**

4. Traffic monitoring
   - o 내부 사용자 PC → DMZ WEB서버 접속 여부를 L3 switch에서 port mirroring 기능과 wireshark를 활용하여 실시간 모니터링

5. server farm 대역 설정
   - o L2 switch#2 서버 팜 대역에 DB서버, log서버 구축
   - o log서버 : 방화벽, switch, web server log를 rsyslog를 통해 백업 실시
   - o DB서버 : iptables 패킷 필터링 정책으로 보안담당자만 원격접속 허용, web서버에서 DBMS로 요청이 오는 패킷만 허용, 그 외에 접속 시도하는 모든 패킷은 /var/log/syslog 파일에 로그를 기록한 뒤 차단

6. NTP 설정
   - o 침해사고 및 장애 발생 시, timeline 구성을 위해 구축 시스템 별 NTP 서버 설정
   - o NTP 서버 : time.bora.net
   - o 설정 시스템 : 각 서버, 네트워크장비, 방화벽, PC

03. 프로젝트 진행방식

- 매 주 목요일 주간보고 작성 및 보고
  - **양식에 맞춰 팀원별 진행상황, 팀 전체 진행상황 작성**

    o 목요일 17시 보고회 진행

  - **팀별로 역할 분담, 최초 1set 완성 후 검수 진행**

    o 검수 완료 후 본인이 맡은 part에 대해 기술 공유

  - **전체 장비 초기화 후 1인 1set 구축**

    o 화면 캡처, PPT 형식으로 캡처한 화면과 기술내용 작성(취업준비 시 포트폴리오 활용)

  - **프로젝트 발표회(대전캠퍼스 자체) 시 출품할 영상 제작**

    o 2~3분 분량의 양식을 이미지와 자막으로 작성하여 영상 제작(팀 단위 1개씩 제작)

    o 프로젝트 발표회 예정일자 : 10월말~11월초