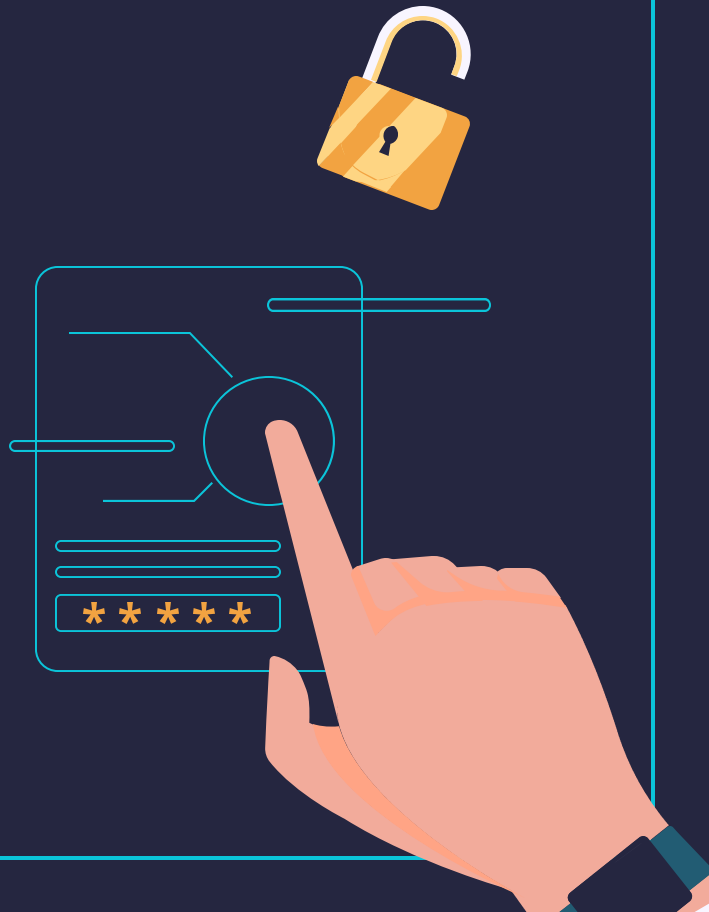
푸드파이터
밥세권

정보 보호 컨설팅 기반 네트워크 웹 보안 사업

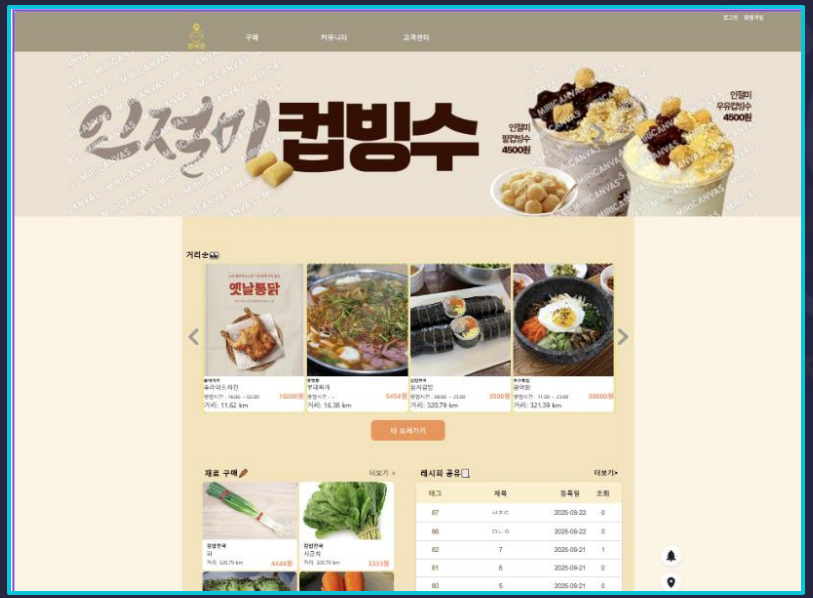


목차

01

프로젝트 배경

고객사 설명 (본사)

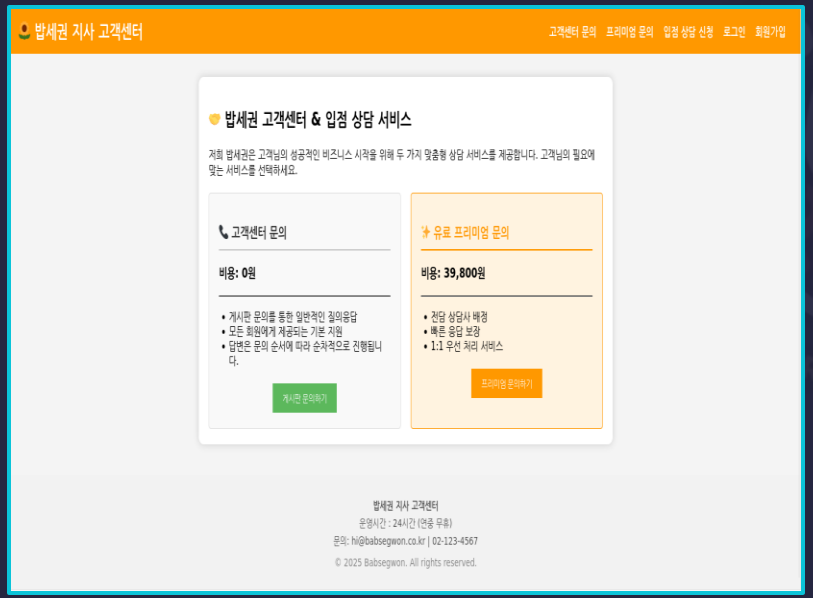


판매자 잉여 재고 판매 저렴한 가격에 구매 가능

재고 최적화로 외식비 절감과 환경 개선 실현

밥세권 www.babsegwon.com

고객사 설명 (지사)



고객 문의 게시판

판매자 입점 신청

지사 고객센터 운영

밥세권

www.babhelp.com

추진 배경


사회

‘가짜 비요르카’ 체포에 대한 보복성 해킹…경찰 34만 명 신상 유출

By Haninpost Indonesia - October 9, 2025

FREE

341K Indonesian National Police Personnel Database

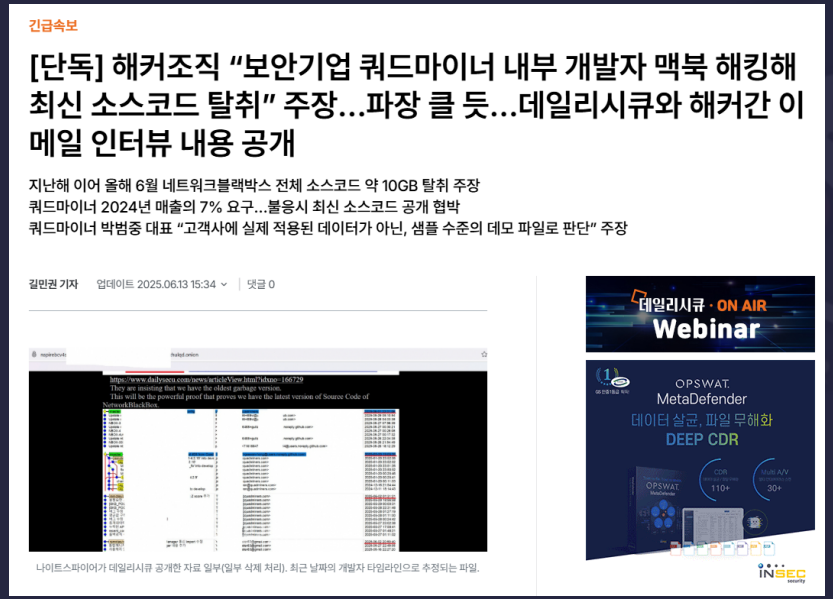
Bjorka • Sat Oct 04 2025 • #Indonesia

KEPOLISIAN NEGARA
REPUBLIK INDONESIA

‘가짜 비요르카’ 체포에 대한
보복성 해킹…경찰 34만 명 신상 유출

비요르카를 사칭한
남성을 체포한 지 하루 만에 발생한 것으로,
사실상 **보복성 공격**

추진 배경


긴급속보

[단독] 해커조직 “보안기업 쿼드마이너 내부 개발자 맥북 해킹해 최신 소스코드 탈취” 주장…파장 클 듯…데일리시큐와 해커간 이메일 인터뷰 내용 공개

지난해 이어 올해 6월 네트워크블랙박스 전체 소스코드 약 10GB 탈취 주장
쿼드마이너 2024년 매출의 7% 요구…불응시 최신 소스코드 공개 협박
쿼드마이너 박범중 대표 “고객사에 실제 적용된 데이터가 아닌, 샘플 수준의 데모 파일로 판단” 주장

김민권 기자 업데이트 2025.06.13 15:34 | 댓글 0

나이트스파이어가 데일리시큐 공개한 자료 일부(일부 삭제 처리). 최근 날짜의 개발자 타임라인으로 추정되는 파일.

“쿼드마이너, 과거 공격 무시…
이번엔 끝까지 간다”

나이트스파이어는 지난 2024년 11월과 2025년 6월, **두 차례에 걸쳐 쿼드마이너를 해킹했다**고 밝혔다.

이에 대해 나이트스파이어는
“이번에는 작년처럼 끝내지 않겠다”
며 **보복성 공격**임을 간접적으로 시사했다.

시나리오 요약

Namhyux Tovalds

고객의 분노 표출

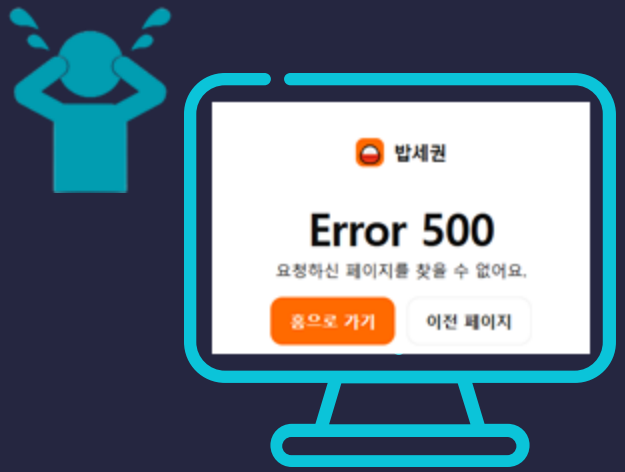
시나리오 요약

모든 네트워크
보안 설정 비활성화

밥세권 보안팀의
미흡한 초기 대응

데이터 베이스 삭제

시나리오 요약



밥세권 서비스 마비

“푸드 파이터” 에게 보안 요청

사업 목표

(C)onfidentiality

- 서비스의 취약점 선별 및 보완
- 주요 기능의 보안 강화

(I)ntegrity

- 데이터 변조 및 위조 차단
- 회원 정보. 결제 정보 등 데이터 암호화 및 접근 통제 강화

(A)VAILABILITY

- 서비스 중단 위험 최소화
- 트래픽 증가에도 서비스 유지

(O)PERATIONS

- 보안 점검 체계 정립
- 보안정책 문서화 및 내재화 완료

사용 툴

사용 도구

GNS 1.5.3

Putty 0.83

VMWare 17.6.2

Packet tracer 8.2.2

Wireshark 4.4.9

문서 도구

Word

PPT

Excel

한글

협업 도구

Notion

Discord

Google Drive

Kakao Talk

NAS

사용 툴

사용 장비

Windows Server 2016
Windows 10

Rocky Linux 8.1

Sophos 9

kail 2024.4-amd64

PHP Server 7.2.24

Apache Tomcat 9.0

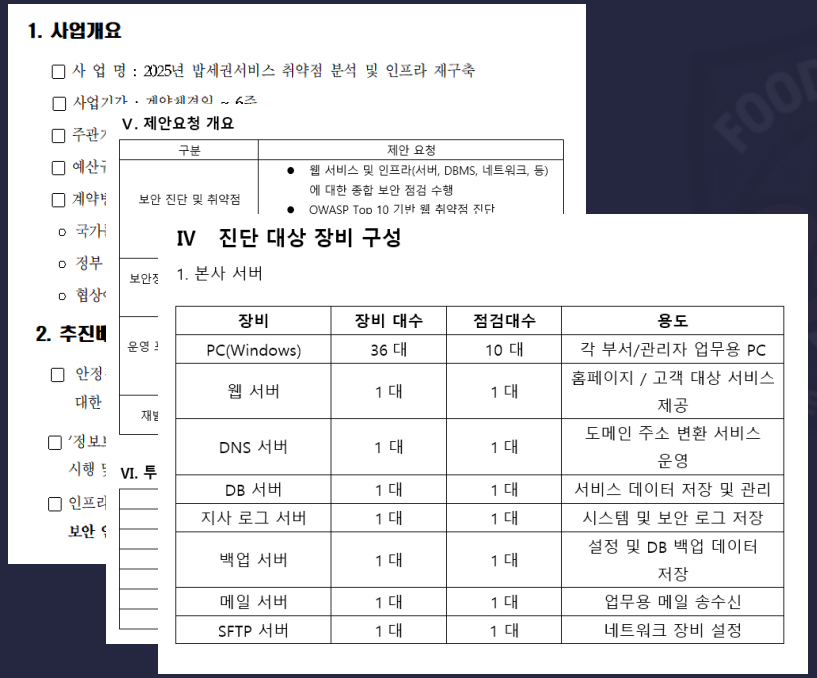
Cisco Router : Cisco 3660 Series 12.4(15)T9
Cisco L3 SW : Cisco 3745 Router 12.4(11)T

CentOS 7

수행 일정

구조	Task	1w	2w	3w	4w	5w	6w
프로젝트 관리	제안서 작성	3일					
	킥 오프 미팅	1일					
	일정 수립	2일					
취약점 분석 및 평가	취약점 점검 대상 식별 및 분류	2일					
	취약점 본 점검(분석/평가)		5일				
	취약점 위험 분석/평가 수행			3일			
보안 정책 수립 및 조치 지원	취약점 개선 방안 도출			2일			
	취약점 조치 지원(보안설정)				7일		
	취약점 이행점검 수행					2일	
모의 해킹	모의해킹					3일	
문서화 및 보고	정보보안 지침 및 규정					3일	
	단기, 중기 보호대책 수립					2일	
	최종 보고						1일

사업 목적



1. 사업개요

□ 사 업 명 : 2025년 밥세권서비스 취약점 분석 및 인프라 재구축

□ 사업기간 : 계약체결일 ~ 6주

□ 주관기

□ 예산규

□ 계약방

○ 국가계

○ 정부

○ 협상에

2. 추진배

□ 안정

대한

□ 정보시

시행 등

□ 인프라

보안 우

V. 제안요청 개요

구분	제안 요청
보안 진단 및 취약점	● 웹 서비스 및 인프라(서버, DBMS, 네트워크, 등)에 대한 종합 보안 점검 수행 ● OWASP Top 10 기반 웹 취약점 진단
보안정	
운영	
재발	

VI. 투

Ⅳ 진단 대상 장비 구성

1. 본사 서버

장비	장비 대수	점검대수	용도
PC(Windows)	36 대	10 대	각 부서/관리자 업무용 PC
웹 서버	1 대	1 대	홈페이지 / 고객 대상 서비스 제공
DNS 서버	1 대	1 대	도메인 주소 변환 서비스 운영
DB 서버	1 대	1 대	서비스 데이터 저장 및 관리
지사 로그 서버	1 대	1 대	시스템 및 보안 로그 저장
백업 서버	1 대	1 대	설정 및 DB 백업 데이터 저장
메일 서버	1 대	1 대	업무용 메일 송수신
SFTP 서버	1 대	1 대	네트워크 장비 설정

- **제안서에 따른 내용**으로 수행
- **자산 식별** 및 분류
- 보안 구성 및 **정책 분석**
- **취약점 점검** 및 **위험도 평가**
- 개선조치 방안 수립
- 보고서 작성 및 전달

02

분석 및 점검

자산 범위

분류	역할	본사	지사	합계
PC(Windows)	부서별 PC	36 대	30 대	66 대
Window Server	DNS, DHCP	2 대	2 대	4 대
Linux Server	SFTP, Mail, Log, DB, Backup, Web	6 대	6 대	12 대
L2 Switch	스위치, VLAN 세팅	4 대	3 대	7 대
L3 Switch	백본, 스위치, 라우팅	4 대	4 대	8 대
L4 Switch	로드 밸런싱	2 대	0 대	2 대
Security Device	UTM, WAF, 방화벽	3 대	2 대	5 대
합 계		58 대	46 대	104 대

점검 범위

WINDOW SERVER 4대 / 4대
WINDOW PC 16대 / 66대

리눅스 서버 12대 / 12대

DBMS 2대 / 2대

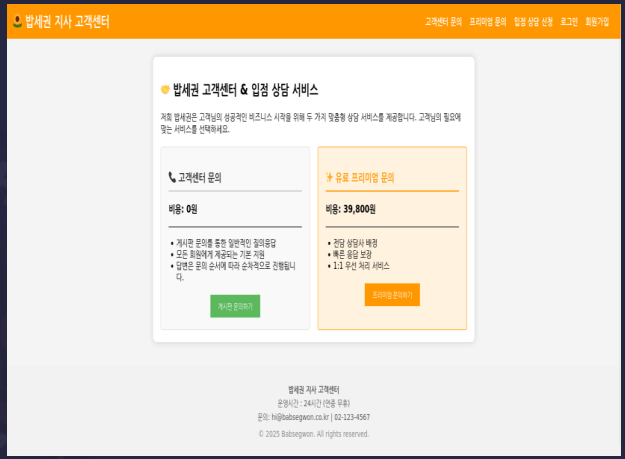
L3 스위치 8대 / 8대

UTM 2대 / 2대

점검 44 대 / 총 104 대

점검 범위

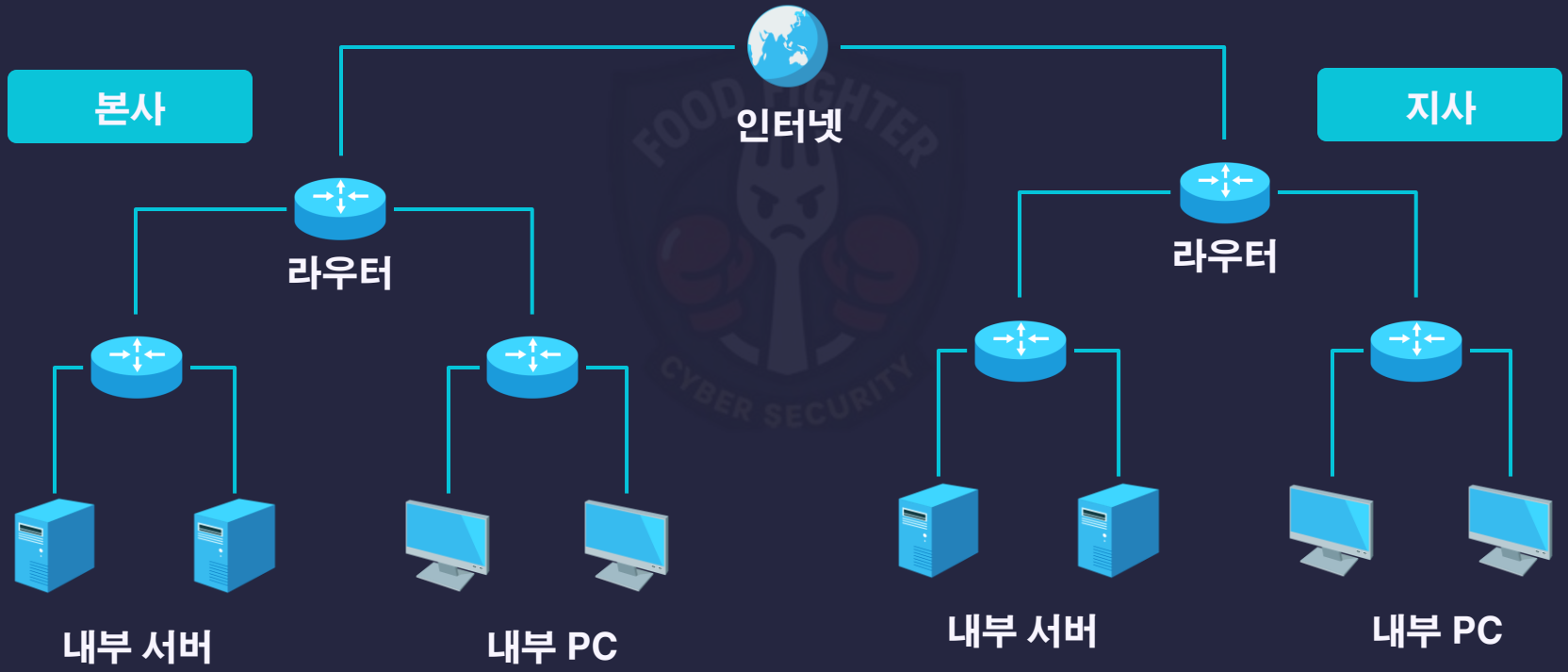
지사 웹 페이지



점검 18 페이지 / 총 18 페이지

인프라 구성

기존 인프라



기존 인프라 문제점

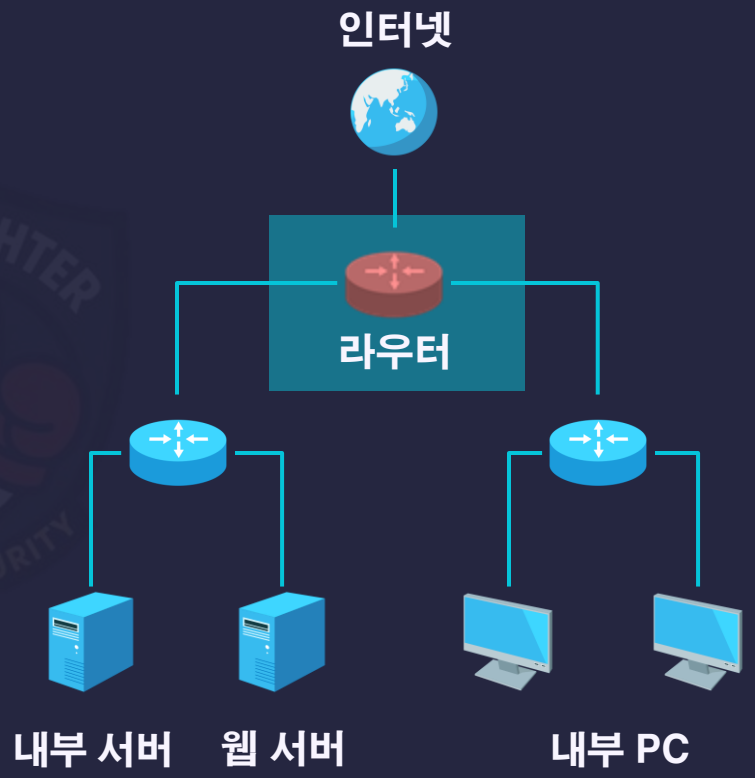
● 장비 이중화 미비
단일 장비 장애 시 전체 서비스 마비

● 보안 장비 없음
DDOS, 웹 해킹 등 외부 공격에 취약

● DMZ 내부망 구분 없음
내부망 직접 노출 및 침투 용이

● ACL 권한 체계 미흡
불필요한 접근 허용 상태 유지

● 백업 서버 없음
데이터 손실 시 복구 불가



기존 인프라 문제점

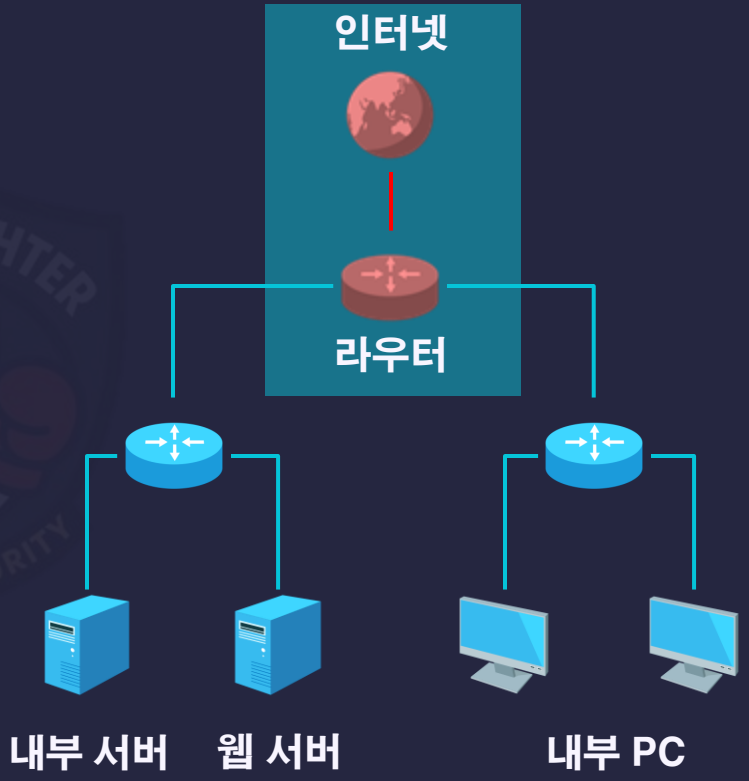
● 장비 이중화 미비
단일 장비 장애 시 전체 서비스 마비

● 보안 장비 없음
DDOS, 웹 해킹 등 외부 공격에 취약

● DMZ 내부망 구분 없음
내부망 직접 노출 및 침투 용이

● ACL 권한 체계 미흡
불필요한 접근 허용 상태 유지

● 백업 서버 없음
데이터 손실 시 복구 불가



기존 인프라 문제점

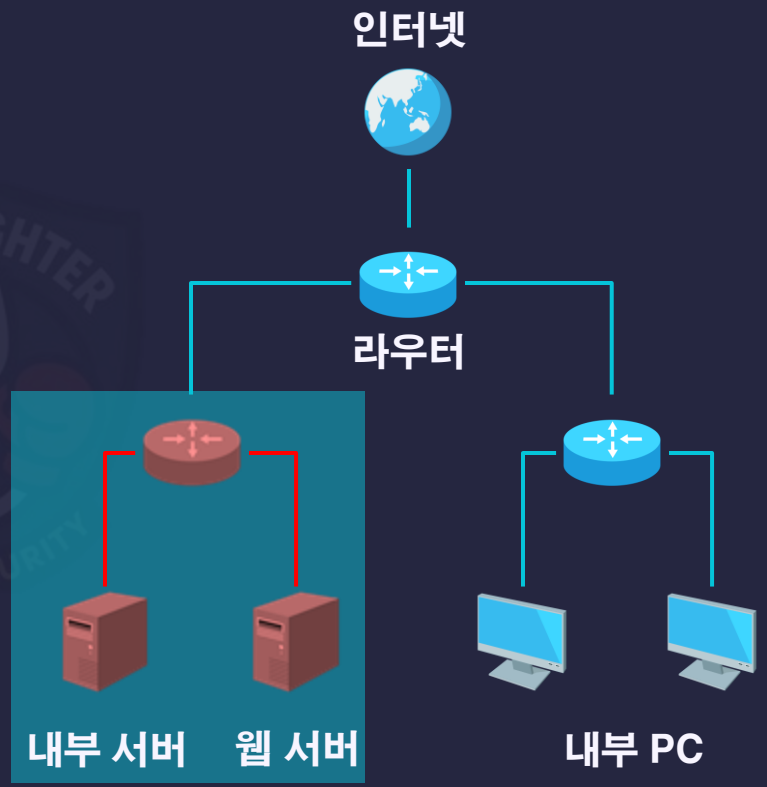
- **장비 이중화 미비**
  단일 장비 장애 시 전체 서비스 마비

- **보안 장비 없음**
  DDOS, 웹 해킹 등 외부 공격에 취약

- **DMZ 내부망 구분 없음**
  내부망 직접 노출 및 침투 용이

- **ACL 권한 체계 미흡**
  불필요한 접근 허용 상태 유지

- **백업 서버 없음**
  데이터 손실 시 복구 불가



기존 인프라 문제점

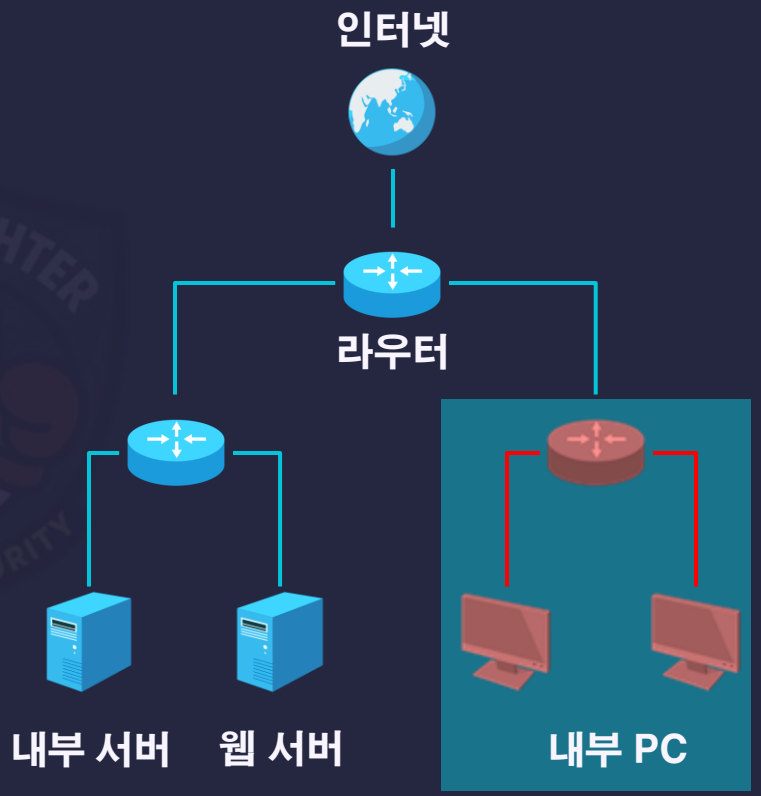
● 장비 이중화 미비
단일 장비 장애 시 전체 서비스 마비

● 보안 장비 없음
DDOS, 웹 해킹 등 외부 공격에 취약

● DMZ 내부망 구분 없음
내부망 직접 노출 및 침투 용이

● ACL 권한 체계 미흡
불필요한 접근 허용 상태 유지

● 백업 서버 없음
데이터 손실 시 복구 불가



기존 인프라 문제점

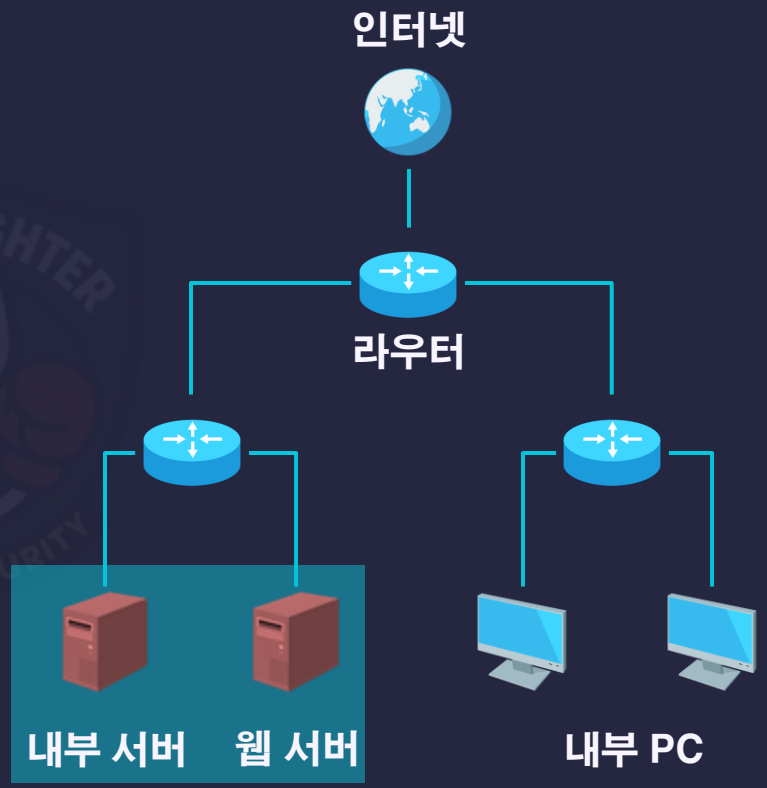
● 장비 이중화 미비
단일 장비 장애 시 전체 서비스 마비

● 보안 장비 없음
DDOS, 웹 해킹 등 외부 공격에 취약

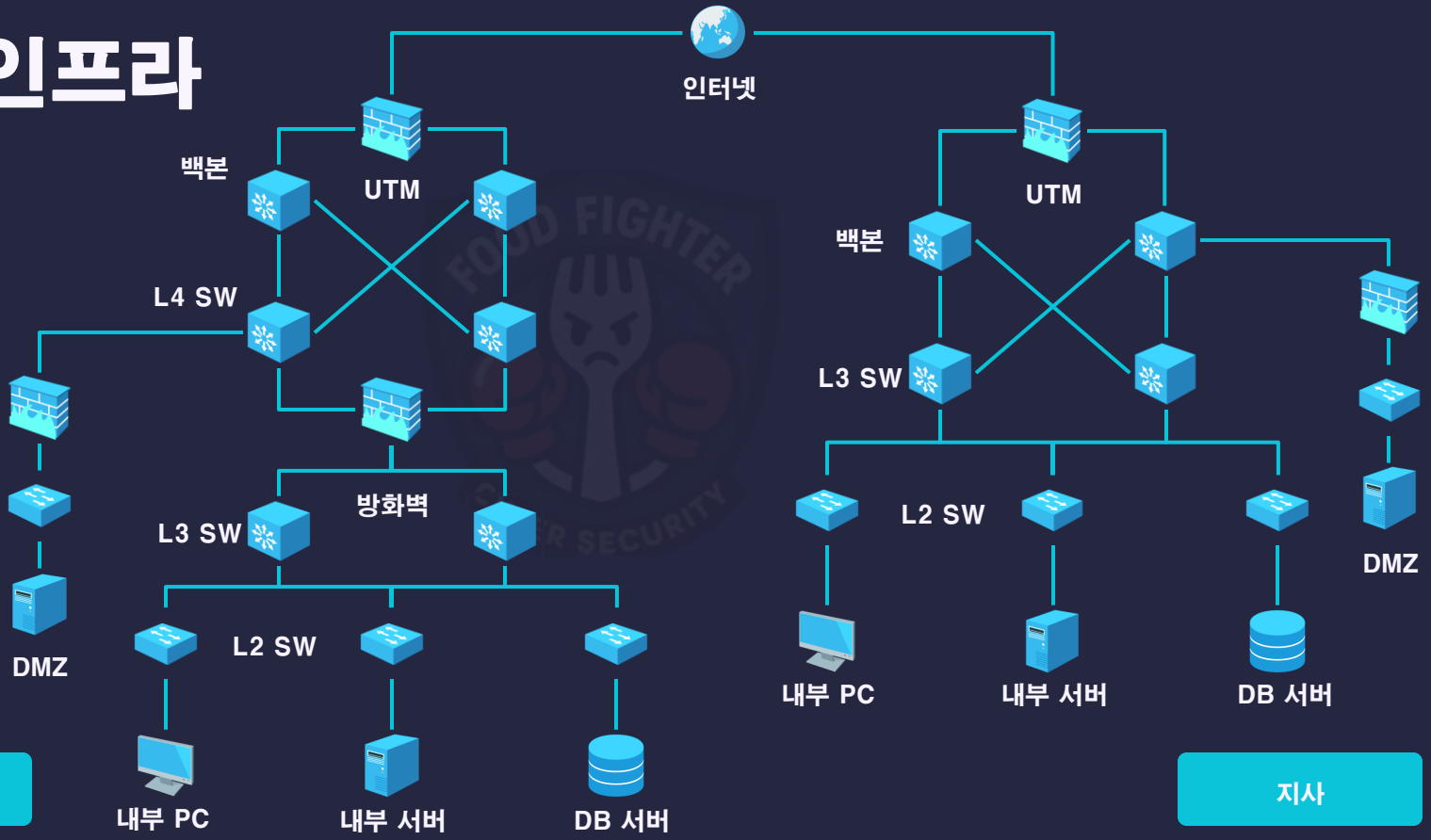
● DMZ 내부망 구분 없음
내부망 직접 노출 및 침투 용이

● ACL 권한 체계 미흡
불필요한 접근 허용 상태 유지

● 백업 서버 없음
데이터 손실 시 복구 불가



개선 인프라


인터넷
백본
UTM
L4 SW
방화벽
L3 SW
L2 SW
DMZ
내부 PC
내부 서버
DB 서버
본사
UTM
백본
L3 SW
L2 SW
DMZ
내부 PC
내부 서버
DB 서버
지사

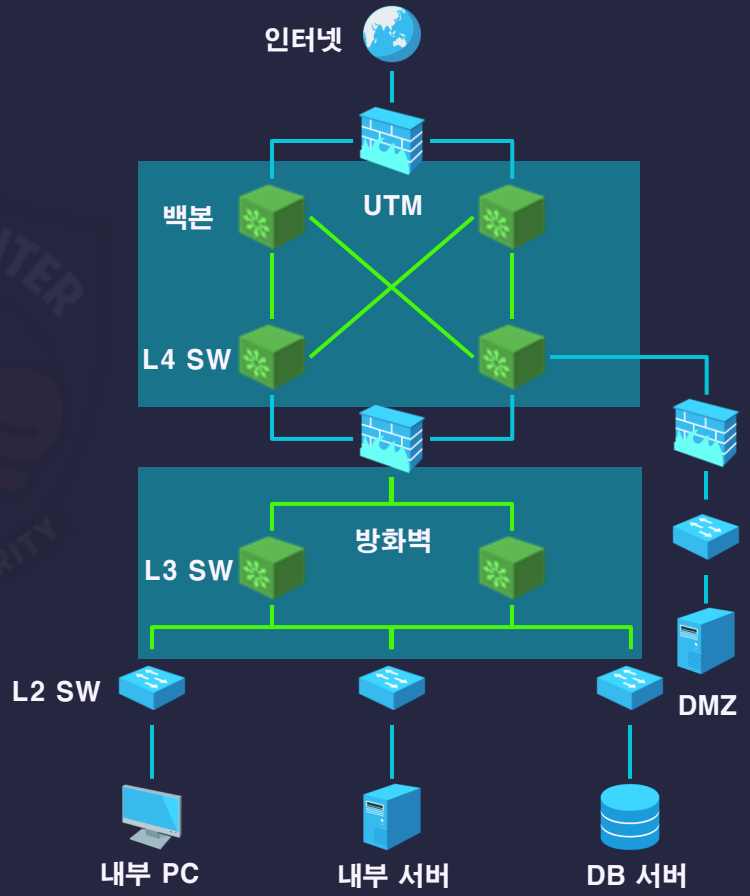
개선된 인프라

● **네트워크 장비 이중화**
장애 시 자동 전환, 무중단 운영 가능

● **UTM 장비 도입**
DDOS 방어, IPS/IDS 기능

● **망 분리**
서비스 망 / 업무망 논리적 분리

● **로그 및 파일 백업 서버 구성**
파일 손실시 대응 체계 마련



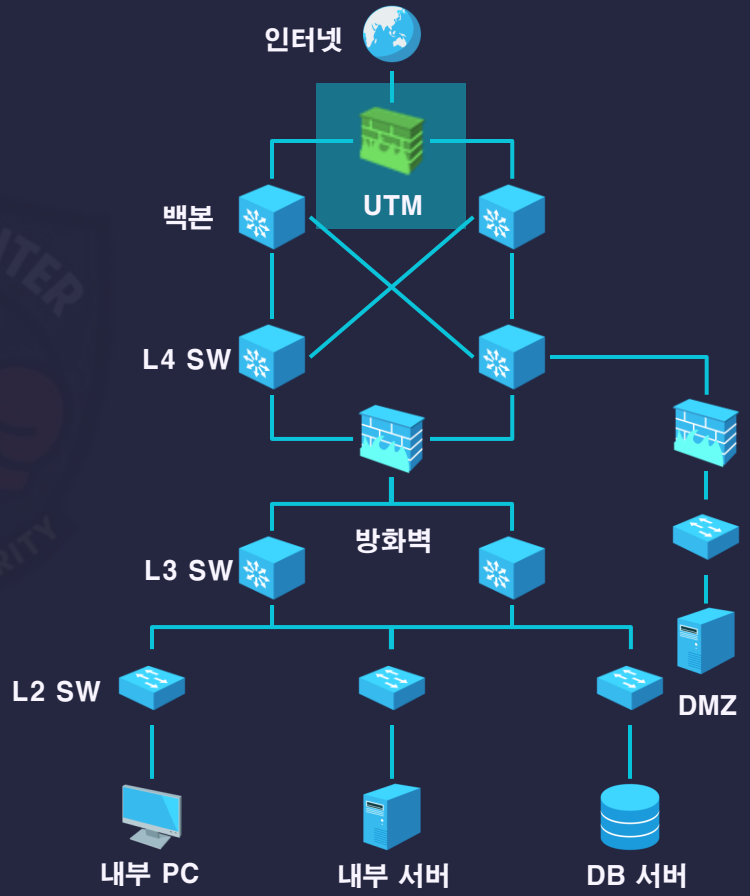
개선된 인프라

● **네트워크 장비 이중화**
장애 시 자동 전환, 무중단 운영 가능

● **UTM 장비 도입**
DDOS 방어, IPS/IDS 기능

● **망 분리**
서비스 망 / 업무망 논리적 분리

● **로그 및 파일 백업 서버 구성**
파일 손실시 대응 체계 마련



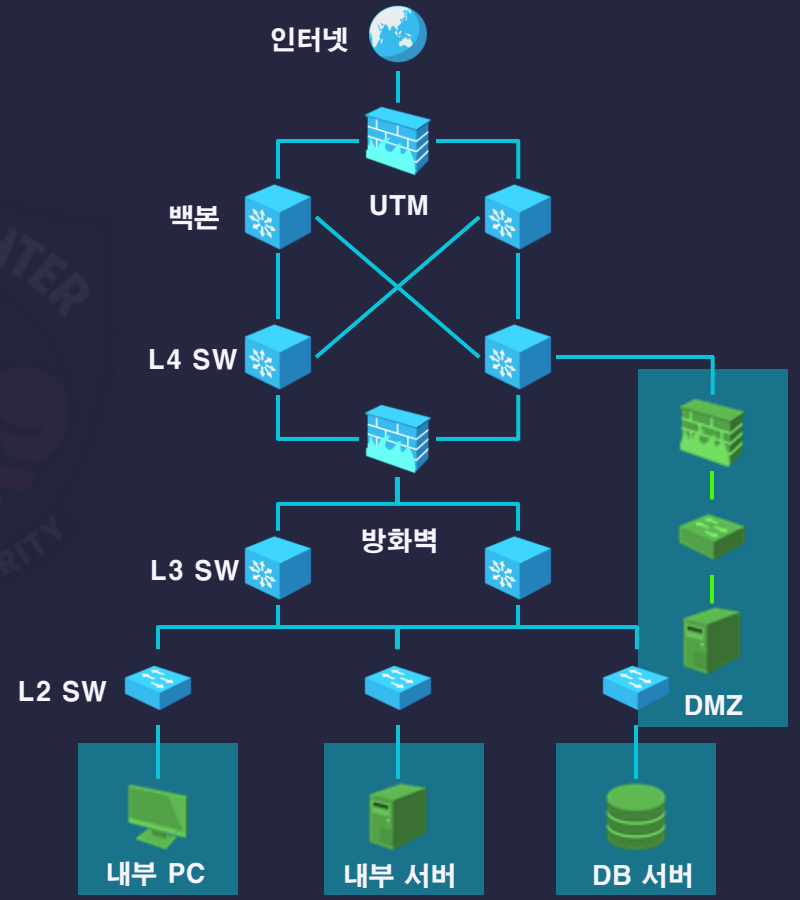
개선된 인프라

● **네트워크 장비 이중화**
장애 시 자동 전환, 무중단 운영 가능

● **UTM 장비 도입**
DDOS 방어, IPS/IDS 기능

● **망 분리**
서비스 망 / 업무망 논리적 분리

● **로그 및 파일 백업 서버 구성**
파일 손실시 대응 체계 마련



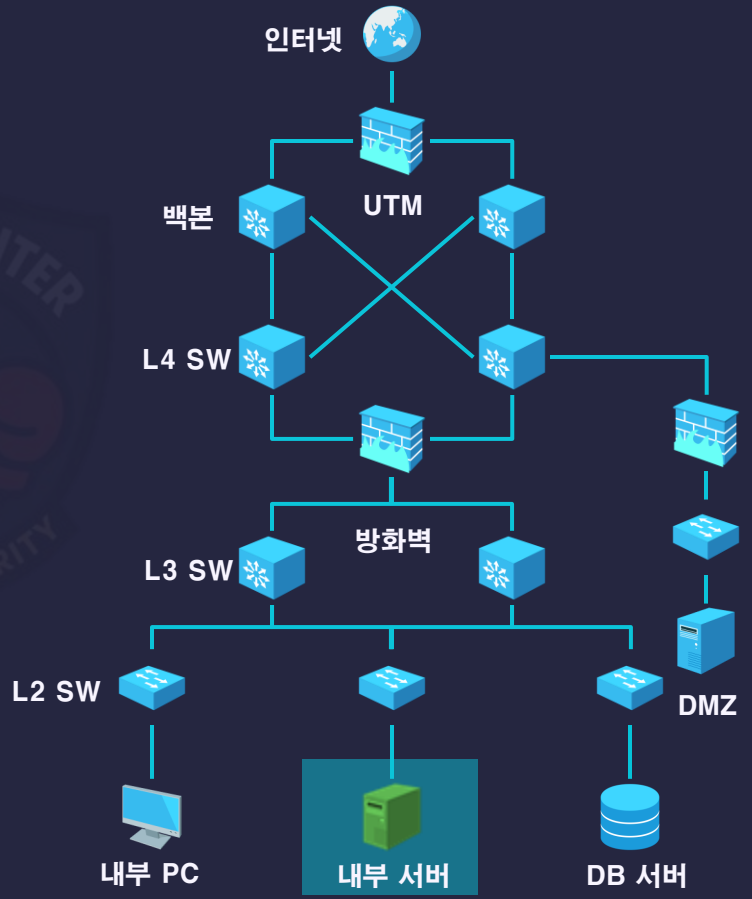
개선된 인프라

● **네트워크 장비 이중화**
장애 시 자동 전환, 무중단 운영 가능

● **UTM 장비 도입**
DDOS 방어, IPS/IDS 기능

● **망 분리**
서비스 망 / 업무망 논리적 분리

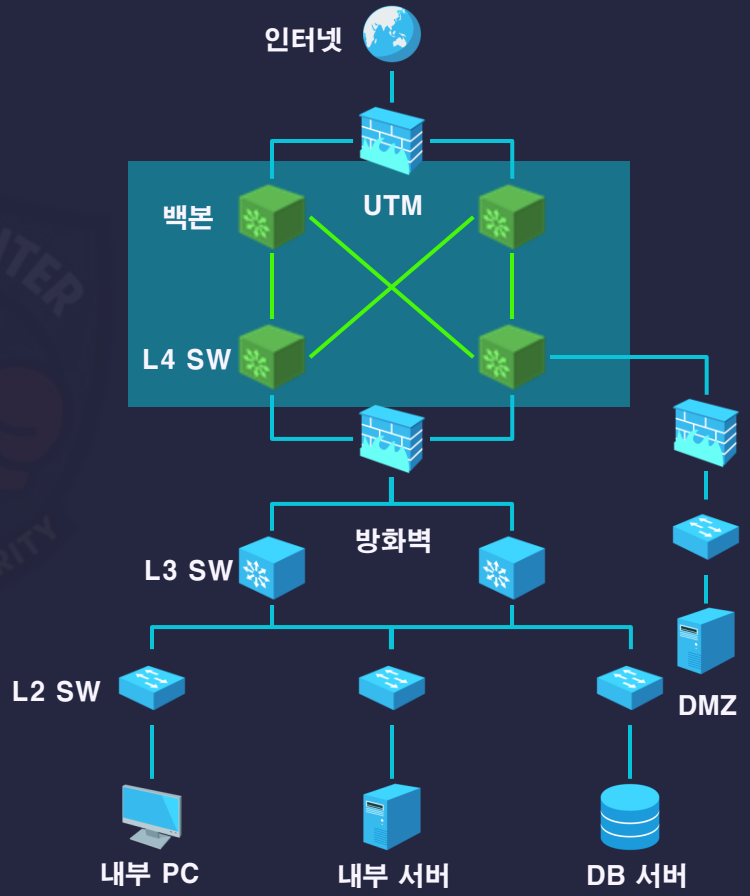
● **로그 및 파일 백업 서버 구성**
파일 손실시 대응 체계 마련



개선된 인프라

● **ACL 및 접근 제어 강화**
민감 자산에 대한 접근 최소화

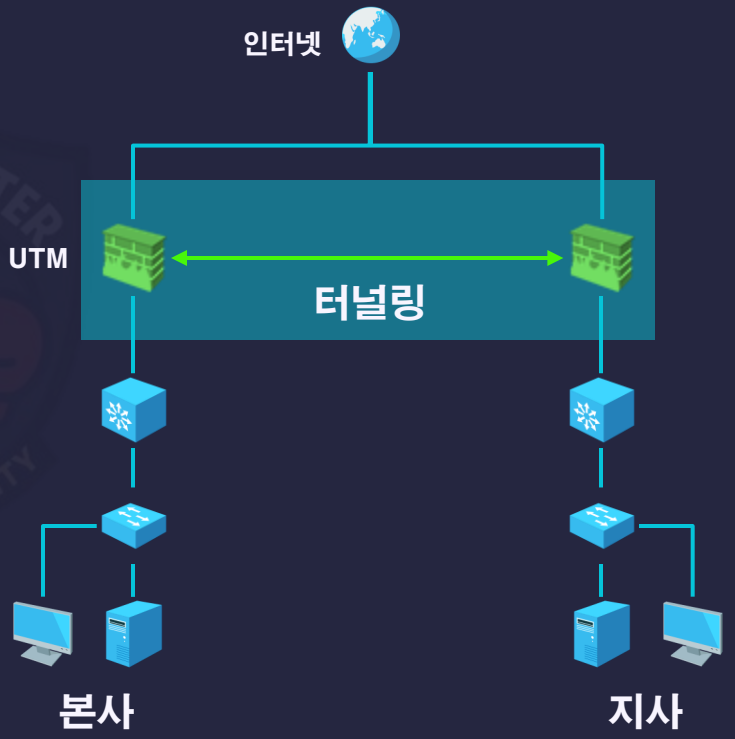
● **GRE+IPsec 구성**
본사 · 지사 간 안전한 통신 보장



개선된 인프라

● ACL 및 접근 제어 강화
민감 자산에 대한 접근 최소화

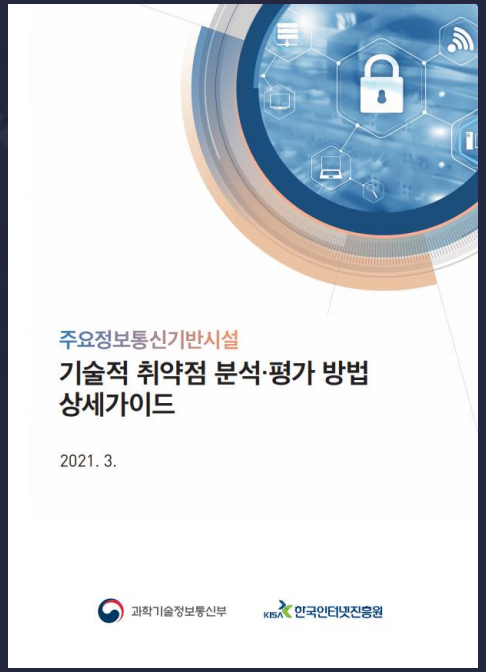
● GRE+IPsec 구성
본사 · 지사 간 안전한 통신 보장



취약점 리스트

평가 기준

주요 정보 통신 기반 시설 과
전자 금융 기반 시설 취약점
평가 방법 기준으로 취약점 파악
및 **점검 실행**



UNIX

주통 기반	금융 기반	위험도	점검 항목
U-02	SRV-075	상	패스워드 복잡성 설정
U-03	SRV-127	상	계정 잠금 임계값 설정
U-04	SRV-012	상	패스워드 파일 보호
U-05	SRV-121	상	root 홈, 패스 디렉터리 권한 및 패스 설정
U-06	SRV-096	상	파일 및 디렉터리 소유자 설정
U-07	SRV-096	상	/etc/passwd 파일 소유자 및 권한 설정
U-13	SRV-091	상	SUID, SGID, Sticky bit 설정 파일 점검
U-14	SRV-095	상	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정
U-37	SRV-042	상	웹 서비스 상위 디렉토리 접근 금지
U-46	SRV-069	중	패스워드 최소 길이 설정

WINDOWS

주통 기반	금융 기반	위험도	점검 항목
W-01	SRV-072	상	Administrator 계정 이름 변경 또는 보안성 강화
W-02	SRV-078	상	Guest 계정 비활성화
W-06	SRV-073	상	관리자 그룹에 최소한의 사용자 포함
W-07	SRV-020	상	공유 권한 및 사용자 그룹 설정
W-08	SRV-018	상	하드디스크 기본 공유 제거
W-29	SRV-066	상	DNS Zone Transfer 설정
W-30	SRV-034	상	RDS(Remonte Data Services) 제거
W-34	SRV-115	상	로그의 정기적 검토 및 보고
W-63	SRV-173	중	DNS 서비스 구동 점검
W-71	SRV-062	중	원격에서 이벤트 로그파일 접근 차단

DBMS

주통 기반	금융 기반	위험도	점검 항목
D-01	DBMS-001	상	기본 계정의 패스워드, 권한 등을 변경하여 사용
D-02	DBMS-003	상	데이터베이스의 불필요 계정을 제거하거나, 잠금설정 후 사용
D-03	DBMS-007	상	패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정
D-04	DBMS-004	상	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용
D-05	DBMS-013	상	원격에서 DB 서버로의 접속 제한
D-06	DBMS-004	상	DBA 이외의 인가되지 않은 사용자 시스템 테이블에 접근할 수 없도록 설정
D-10	DBMS-016	상	데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용
D-13	DBMS-020	중	DB 사용자 계정을 개별적으로 부여하여 사용
D-17	DBMS-022	중	데이터베이스의 주요 설정 파일, 패스워드 파일 등과 같은 파일들의 접근 권한 설정
D-21	DBMS-024	중	인가되지 않은 GRANT OPTION 사용 제한

보안 장비

주통 기반	금융 기반	위험도	점검 항목
S-01	ISS-017	상	보안장비 Default 계정 변경
S-02	ISS-018	상	보안장비 Default 패스워드 변경
S-03	ISS-020	상	보안장비 계정별 권한 설정
S-04	ISS-019	상	보안장비 계정 관리
S-05	ISS-021	상	보안장비 원격 관리 접근 통제
S-06	ISS-016	상	보안장비 보안 접속
S-07	ISS-024	상	Session timeout 설정
S-08	ISS-005	상	벤더에서 제공하는 최신 업데이트 적용
S-09	ISS-001	상	정책 관리
S-10	ISS-004	상	NAT 설정

네트워크 장비

주통 기반	금융 기반	위험도	점검 항목
N-01	NET-56	상	패스워드 설정
N-02	NET-12	상	패스워드 복잡도 설정
N-03	NET-11	상	암호화된 패스워드 사용
N-14	NET-52	상	사용하지 않는 인터페이스의 Shutdown 설정
N-05	NET-14	상	Session Timeout 설정
N-06	NET-48	상	최신 보안 패치 및 벤더 권고사항 적용
N-12	NET-40	상	Spoofing 방지 필터링 적용 또는 보안장비 사용
N-13	NET-47	상	DDoS 공격 방어 설정 또는 DDoS 장비 사용
N-29	NET-30	중	CDP 서비스 차단
N-32	NET-26	중	Proxy ARP 차단

웹

주통 기반	금융 기반	위험도	점검 항목
FU	SER-002	상	악성파일 업로드
FD	SER-010	상	파일 다운로드
AE	SER-039	상	관리자 페이지 노출 여부
IN	SER-003	상	부적절한 이용자 인가 여부
SC	SER-033	상	불충분한 세션종료 처리
XS	SER-041	상	크로스사이트 스크립팅 (XSS)
CF	SER-028	상	크로스사이트 요청변조 (CSRF)
DI	SER-029	상	디렉토리 목록 노출
IL	SER-020	상	화면 내 중요정보 평문노출 여부
SI	SER-001	상	SQL Injection

03

수행 결과

팀원 소개

김기수 / PM

전체 총괄,
네트워크 구축, 보안 장비,
PHP 웹서버 구축, 모의해킹

최장현 / PL

지사 리눅스 서버 구축,
MariaDB 구축, 모의해킹

이남혁 / 수행원

본사 리눅스 서버 구축,
PHP 웹서버 구축,
MariaDB 구축, 모의해킹

팀원 소개

강버들 / 수행원

본사 네트워크 구축,
보안장비, 모의해킹

이태호 / 수행원

지사 네트워크 구축,
PHP웹서버 구축,
보안 장비, 모의해킹

이서진 / 수행원

윈도우 서버 구축,
MariaDB 구축, 모의해킹

김기수

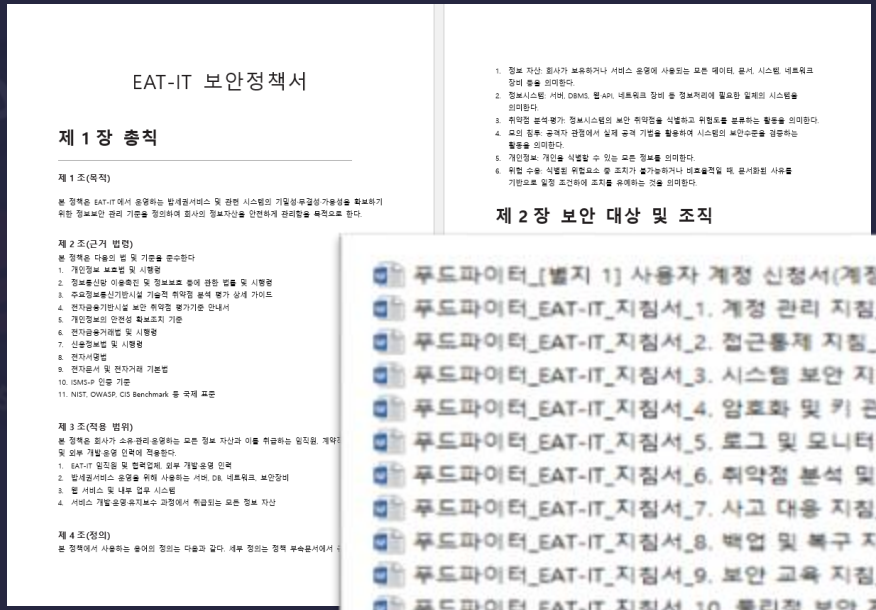
- 총괄
- 보안 규정 · 지침 · 절차 검토 결과 보고서
- 모의 해킹

프로젝트 총괄

소통 · 작업일지 · 제안서 준수

보안 규정 · 지침 · 절차 검토 결과 보고서

- 정책 · 지침의 **정합성 확보**를 위한 문서 검토 수행
- 계정 · 접근 · 로그 · 시스템 · 암호화 영역 중심 분석
- ISMS-P 및 주요정보통신기반시설 가이드 기반 점검



EAT-IT 보안정책서

제 1 장 총칙

제 1 조(목적)

본 정책은 EAT-IT 에서 운영하는 법률검서비스 및 관련 시스템의 기밀성·무결성·가용성을 확보하기 위한 정보보안 관리 기준을 정의하여 회사의 정보자산을 안전하게 관리함을 목적으로 한다.

제 2 조(근거 법령)

본 정책은 다음의 법 및 기준을 준수한다

1. 개인정보 보호법 및 시행령
2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 시행령
3. 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드
4. 전자금융기반시설 보안 취약점 평가기준 안내서
5. 개인정보의 안전성 확보조치 기준
6. 전자금융거래법 및 시행령
7. 신용정보법 및 시행령
8. 전자서명법
9. 전자문서 및 전자거래 기본법
10. ISMS-P 인증 기준
11. NIST, OWASP, CIS Benchmark 등 국제 표준

제 3 조(적용 범위)

본 정책은 회사가 소유·관리·운영하는 모든 정보 자산과 이를 취급하는 임직원, 계약직 및 외부 개발·운영 인력에 적용한다.

1. EAT-IT 임직원 및 협력업체, 외부 개발·운영 인력
2. 법률검서비스 운영을 위해 사용하는 서버, DB, 네트워크, 보안장비
3. 웹 서비스 및 내부 업무 시스템
4. 서비스 개발·운영·유지보수 과정에서 취급되는 모든 정보 자산

제 4 조(정의)

본 정책에서 사용하는 용어의 정의는 다음과 같다. 세부 정의는 정책 부속문서에서 [illegible]

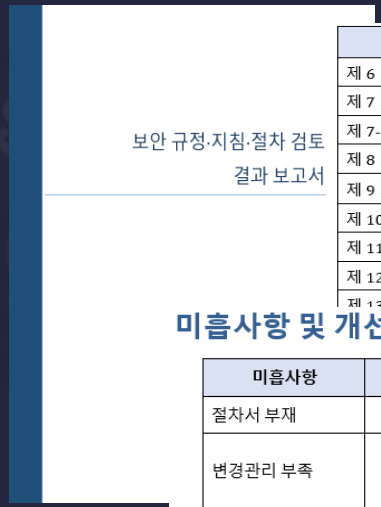
1. 정보 자산: 회사가 보유하거나 서비스 운영에 사용되는 모든 데이터, 문서, 시스템, 네트워크 장비 등을 의미한다.
2. 정보시스템: 서버, DBMS, 웹 API, 네트워크 장비 등 정보처리에 필요한 일체의 시스템을 의미한다.
3. 취약점 분석 평가: 정보시스템의 보안 취약점을 식별하고 위험도를 분류하는 활동을 의미한다.
4. 모의 침투: 공격자 관점에서 실제 공격 기법을 활용하여 시스템의 보안수준을 검증하는 활동을 의미한다.
5. 개인정보: 개인을 식별할 수 있는 모든 정보를 의미한다.
6. 위험 수용: 식별된 위험요소 중 조치가 불가능하거나 비효율적일 때, 문서화된 사유를 기반으로 일정 조건하에 조치를 유예하는 것을 의미한다.

제 2 장 보안 대상 및 조직

푸드파이터_[별지 1] 사용자 계정 신청서(계정 [illegible]
푸드파이터_EAT-IT_지침서_1. 계정 관리 지침_v
푸드파이터_EAT-IT_지침서_2. 접근통제 지침_v1
푸드파이터_EAT-IT_지침서_3. 시스템 보안 지침_
푸드파이터_EAT-IT_지침서_4. 암호화 및 키 관리
푸드파이터_EAT-IT_지침서_5. 로그 및 모니터링
푸드파이터_EAT-IT_지침서_6. 취약점 분석 및 모
푸드파이터_EAT-IT_지침서_7. 사고 대응 지침_v
푸드파이터_EAT-IT_지침서_8. 백업 및 복구 지침
푸드파이터_EAT-IT_지침서_9. 보안 교육 지침_v
푸드파이터_EAT-IT_지침서_10. 물리적 보안 지침

보안 규정 · 지침 · 절차 검토 결과 보고서

- **정책 · 지침 매핑표 작성** 및 미비점 식별
- 보안 요구사항 대비 부족한 항목 정리



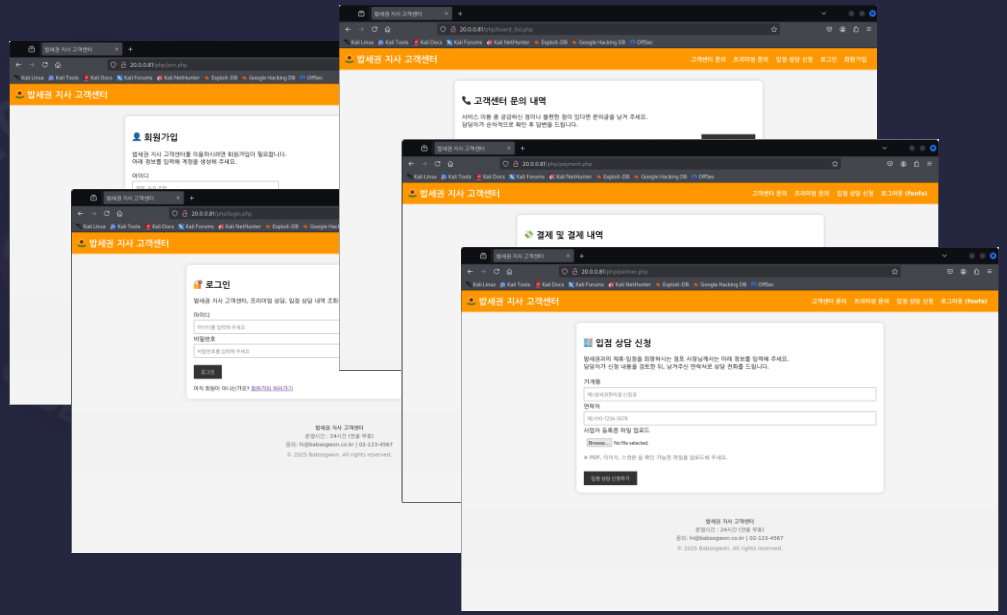
정책 조항	대응 지침	구현 수준
제 6 조 계정·접근통제	계정 관리 지침 / 접근통제 지침	양호
제 7 조 네트워크 보호	접근통제 지침	양호
제 7-1 조 보안장비	접근통제 지침 / 로그 및 모니터링 지침	양호
제 8 조 시스템 보안	시스템 보안 지침	양호
제 9 조 암호화	암호화 및 키 관리 지침	양호
제 10 조 로그 및 모니터링	로그 및 모니터링 지침	양호
제 11 조 결제 보안	접근통제·암호화·로그·백업 지침	매우 양호
제 12 조 취약점 분석 및 모의침투	취약점 분석 및 모의침투 지침	양호
제 13 조 사고 대응	사고 대응 지침	양호
		양호
		양호
		양호

미흡사항 및 개선방안 요약표

미흡사항	영향도	개선 항목	비고
절차서 부재	High	절차서 신규 작성	운영 표준화 및 감사 대응
변경관리 부족	High	변경관리 프로세스 구축	장애 원인 분석 및 추적
로그/탐지 기준 부족	Medium	로그 운영가이드 작성	SIEM 탐지 기준 명확화
용어 정의 불일치	Low	용어 표준화	문서 이해도 향상
신청서 연계 약함	Medium	신청서 흐름 명확화	계정·권한 흐름 가시화

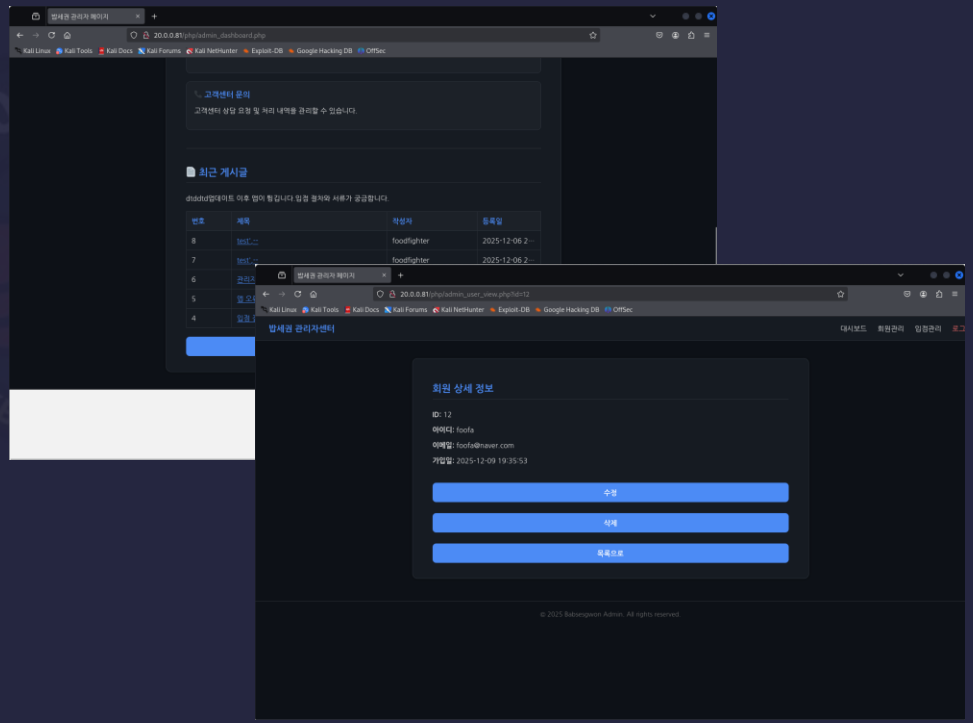
모의 해킹 점검 범위

- **웹 서비스 주요 기능**
  (회원가입, 로그인, 게시판)
- **관리자 기능**
  (파트너 및 사용자 조회 · 수정 등)



모의 해킹 점검 범위

- 웹 서비스 주요 기능
  (회원가입, 로그인, 게시판)
- 관리자 기능
  (파트너 및 사용자 조회 · 수정 등)



취약점 요약

- 서비스 주요기능 전반에서 보안 취약점 다수 확인
- 전반적인 보안 검증 미흡으로 고위험 취약점 다수 존재
- 즉각적인 조치 필요

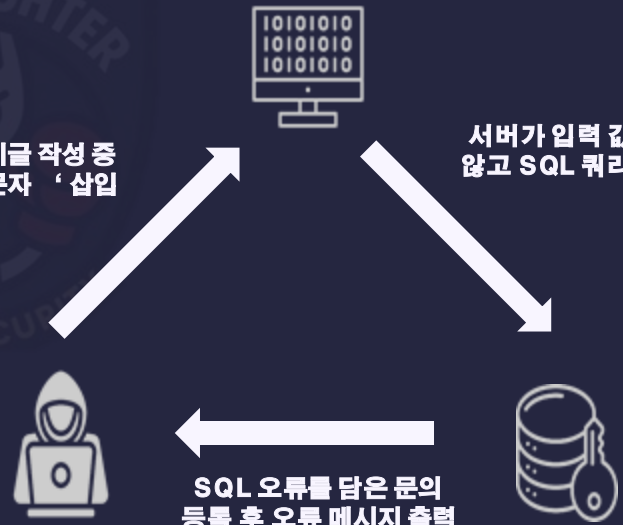
주통 기반	금융 기반	위험도	취약점
SI	SER-001	상	SQL Injection
IL	SER-020	상	화면 내 중요정보 평문노출 여부
CF	SER-028	상	크로스사이트 요청변조 (CSRF)
XS	SER-041	상	크로스사이트 스크립팅 (XSS)

모의 해킹 (문의게시판-DB 정보 노출)

babhelp.com/php/board_list.php

- 내부 정보 · 민감 정보 · 시스템 구조 **정보 등이 의도치 않게 노출되**는 보안 취약점
- **특수문자 입력** 후 오류 메시지를 관찰하기 위해 테스트 진행
- 제목에 **' 특수문자 입력** 후 게시글 등록

WEB	정보 누출	상	IL



모의 해킹 (문의게시판-DB 정보 노출)

- 특수문자(‘) 입력 시 SQL 에러 발생
- 오류 메시지에 DB 종류 및 INSERT 구문 일부 노출
- SQL Injection 공격 가능성 증가

개선 방안 (문의게시판-DB 정보 노출)

- 에러 메시지 출력 제거
- board_proc.php에 시큐어코딩 적용
- Prepared Statement로 DB정보노출, SQL Injection 동시 차단

기존 취약 코드

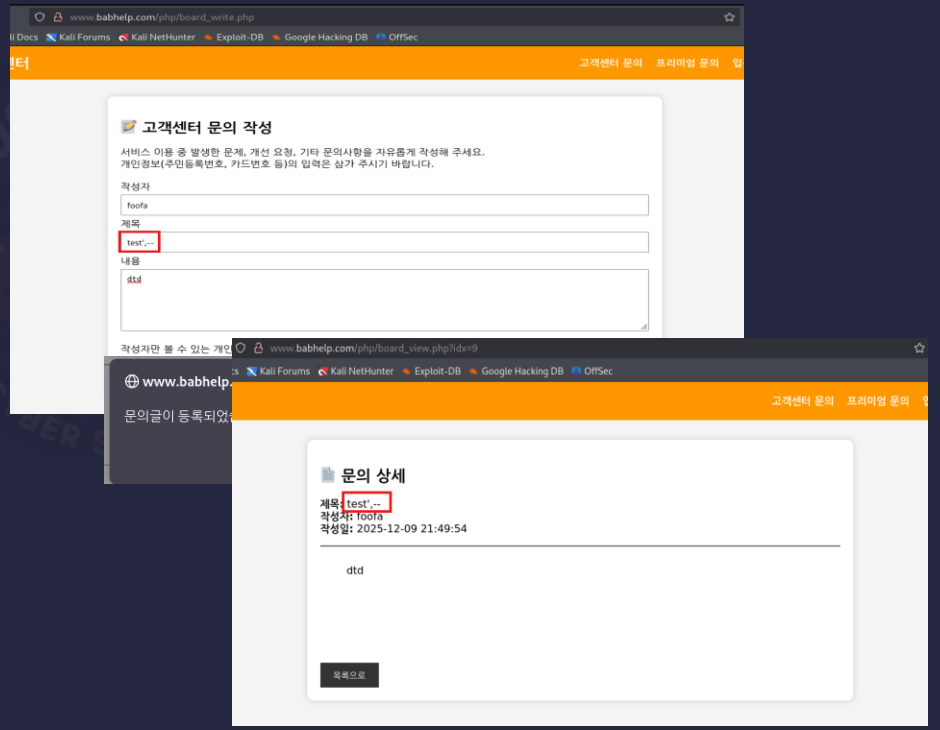
```
$sql = "INSERT INTO board (writer, title, content, user_id, is_private)
        VALUES ('$writer', '$title', '$content', '$user_id', '$is_private')";

$result = mysqli_query($conn, $sql);

if (!$result) {
    die('쿼리 실행 실패 : ' . mysqli_error($conn));
}

// 등록 후 목록으로 이동
echo "<script>alert('문의글이 등록되었습니다.'); location.href='board_list.php';</script>";
?>
```

Prepared Statement 사용

```
$stmt = $conn->prepare("
    INSERT INTO board (writer, title, content, user_id, is_private)
    VALUES (?, ?, ?, ?, ?)
");
```

개선 방안 (문의게시판-DB 정보 노출)

- 에러 메시지 출력 제거
- board_proc.php에 시큐어코딩 적용
- **Prepared Statement**로 DB정보노출, SQL Injection 동시 차단

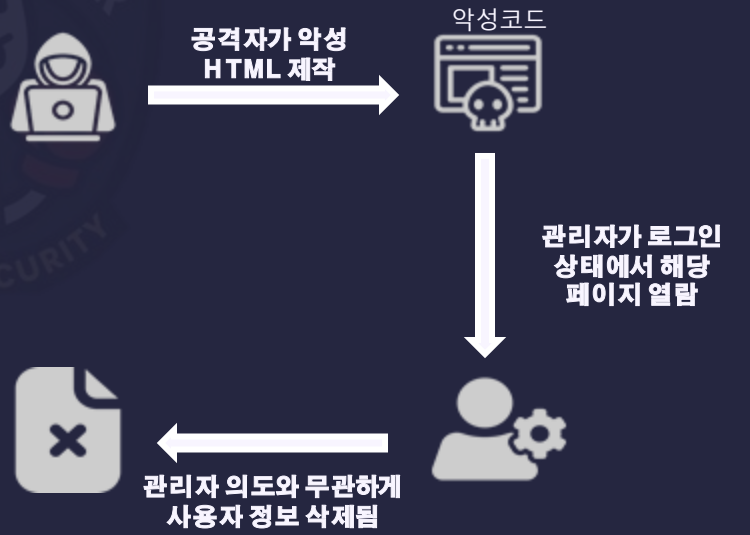


모의 해킹 (관리자 페이지-CSRF)

babhelp.com/php/admin_user_delete.php

- 로그인된 사용자를 속여서 의도하지 않은 요청을 서버에 강제로 보내게 만드는 공격
- CSRF 보호 토큰이 존재하지 않아 위험성 의심
- 공격자가 만든 HTML 페이지에 img src 태그를 이용해 삭제 요청 전송 코드 삽입
- 관리자 계정으로 로그인한 상태에서 악성 페이지 접속 테스트 진행

WEB	크로스사이트 리퀘스트 변조(CSRF)	상	CF



모의 해킹 (관리자 페이지-CSRF)

- **관리자 계정 권한으로** 사용자 **삭제 요청이 수행**됨
- 관리자 **의도와 무관**하게 강제 동작 가능
- **중요 정보 손실** 및 계정 탈취 후 추가 공격 가능성 증가

```
[root@BR_PHP_SEC php]# cat csrf_test.html
<img src="http://www.babhelp.com/php/admin_user_delete.php?id=1">

[root@BR_PHP_SEC php]#
```

최근 게시글

dddd

번호	제목	작성자	등록일
9	문의드립니다	hacking	2025-12-04 13:35:48
8	ddd	hacking	2025-11-28 16:47:10

게시판 전체 보기

```
MariaDB [babsegwon]> select * from users;
+----+----------+----------+-----------------+---------------------+
| id | username | password | email           | reg_date            |
+----+----------+----------+-----------------+---------------------+
|  2 | abc      | 123      | abc@abc.com     | 2025-11-26 21:56:19 |
|  4 | ss       | 12345    | ss@abc.com      | 2025-11-27 01:04:43 |
|  5 | aaabbb   | 123      | aaabbb@naver.com| 2025-11-27 10:16:06 |
|  6 | dlskagur | a1234    | skagur@naver.com| 2025-11-28 12:13:47 |
|  7 | hacking  | 1234     | hack@naver.com  | 2025-11-28 12:23:18 |
|  9 | test01   | 1234     | test01@naver.com| 2025-12-04 12:14:50 |
| 10 | rlawls   | a1234    | rlawls@gmail.com| 2025-12-04 12:14:50 |
| 11 | user123  | pass1    | user123@daum.net| 2025-12-04 12:14:50 |
| 12 | banana   | 1111     | banana@naver.com| 2025-12-04 12:14:50 |
| 13 | marketman| 2222     | market@kakao.com| 2025-12-04 12:14:50 |
+----+----------+----------+-----------------+---------------------+
10 rows in set (0.000 sec)
```

개선 방안 (관리자 페이지-CSRF)

- admin_header.php에서 세션 시작 및 관리자 전용 **CSRF 토큰** 자동 생성
- 회원 삭제나 정보 수정과 같은 **중요한 요청은 GET방식 금지**
- 삭제 쿼리는 **Prepared Statement**로 SQL Injection도 방어

admin_header.php

```php
<?php
// 세션 시작
if (session_status() === PHP_SESSION_NONE) {
    session_start();
}

// CSRF 토큰이 없으면 새로 생성
if (empty($_SESSION['csrf_token'])) {
    $_SESSION['csrf_token'] = bin2hex(random_bytes(32));
}
?>
```

admin_user_delete.php

```php
// 1. 요청 방식 확인 (GET 요청 차단)
if ($_SERVER['REQUEST_METHOD'] !== 'POST') {
    http_response_code(405);
    echo "<script>alert('허용되지 않은 요청 방식입니다.'); history.back();</script>";
    exit;
}

// 2. CSRF 토큰 검증
$sessionToken = $_SESSION['csrf_token'] ?? '';
$formToken    = $_POST['csrf_token'] ?? '';

if (!$sessionToken || !$formToken || !hash_equals($sessionToken, $formToken)) {
    http_response_code(403);
    echo "<script>alert('유효하지 않은 요청입니다.(CSRF 검증 실패)'); history.back();</script>";
    exit;
}
```

개선 방안 (관리자 페이지-CSRF)

- admin_header.php에서 세션 시작 및 관리자 전용 **CSRF 토큰** 자동 생성
- 회원 삭제나 정보 수정과 같은 **중요한 요청은 GET방식 금지**
- 삭제 쿼리는 **Prepared Statement**로 SQL Injection도 방어

```
[root@BR_PHP_SEC php]# cat csrf_test.html
<img src="http://www.babhelp.com/php/admin_user_delete.php?id=11">
```

번호	제목	작성자	등록일
9	test',--	foofa	2025-12-09 2…
8	test',--	foodfighter	2025-12-06 2…
7	test',--	foodfighter	2025-12-06 2…
6	관리자 계정 삭제 테스트	hacking	2025-12-04 1…
5	앱 오류 신고	guest01	2025-12-04 1…

회원 관리

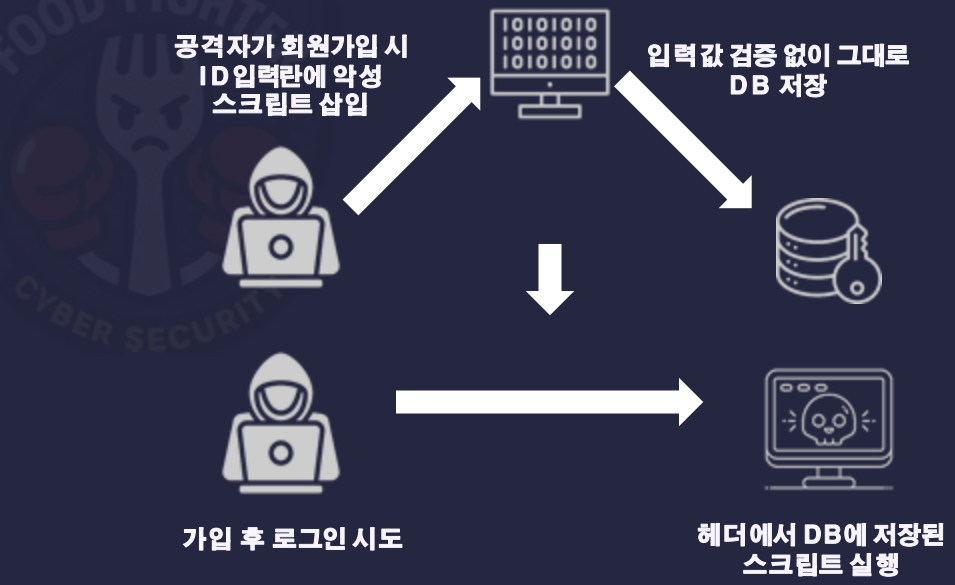
ID	아이디	이메일	가입일	관리
12	foofa	foofa@naver.com	2025-12-09 1…	보기 수정
11	foodfighter	foodfighter@naver.com	2025-12-06 2…	보기 수정

모의 해킹 (회원가입-Stored XSS)

babhelp.com/php/join.php

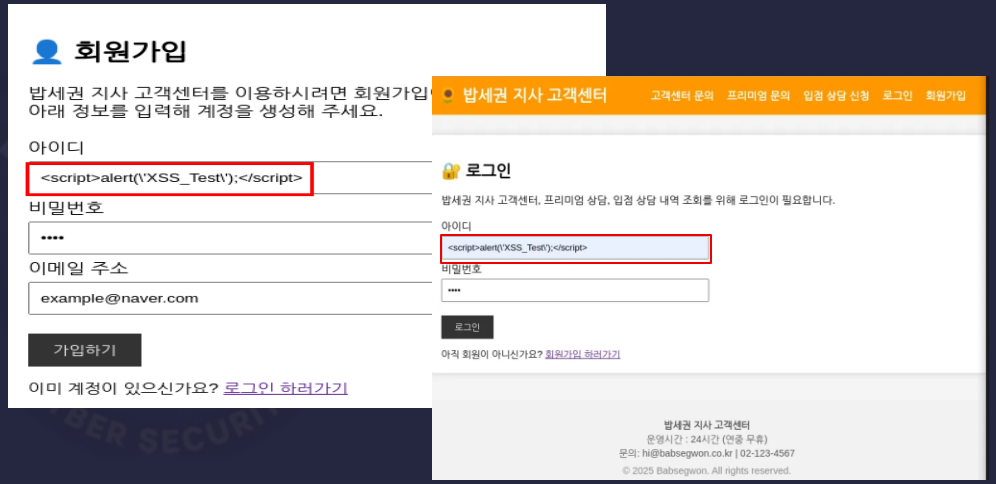
- 사용자가 입력한 스크립트가 **DB에 저장되었다가** 출력 시 그대로 실행되는 취약점
- 회원 **ID가** 화면 **헤더에** 그대로 **출력**되는 구조 확인
- 회원가입 시 **ID 입력란에** **스크립트 삽입**

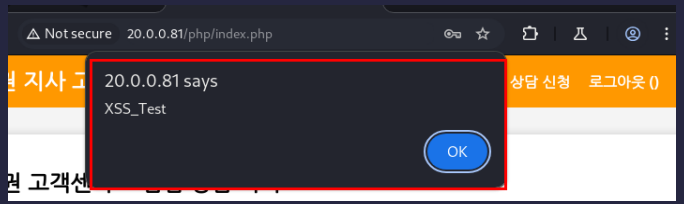
WEB	크로스사이트 스크립팅 (XSS)	상	XS



모의 해킹 (회원가입-Stored XSS)

- 회원가입 후 로그인 시 스크립트 실행 여부 확인
- 로그인 시 헤더 영역에 저장된 ID가 그대로 출력
- 그 순간, **DB에 저장된 스크립트**가 브라우저에서 실행
- **document.cookie**를 포함한 악성 스크립트를 삽입하여 사용자 **세션 쿠키 탈취 및 계정 하이재킹** 가능성 발생



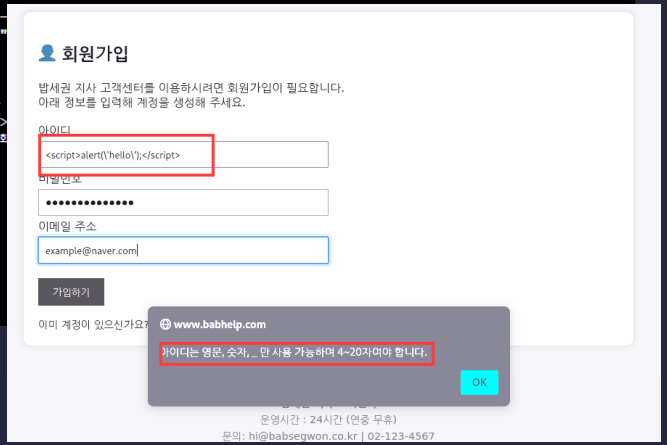


개선 방안 (회원가입-Stored XSS)

- 정규식으로 ID 입력란 입력 값 검증
- HTML 이스케이프 적용
- 사용자 입력을 안전한 문자로 변환
- 브라우저가 스크립트로 실행하지 못하도록 함

```
// 아이디 : 영문 숫자 _ 만 허용 4~20자 (정책에 맞게 조정 가능)
if (!preg_match('/^[a-zA-Z0-9_]{4,20}$/', $id)) {
    echo "<script>alert('아이디는 영문, 숫자, _ 만 사용 가능하며 4~20자여야 합니다.'); history.back();</script>";
    exit;
}
```

```
<?php
// XSS 방어 : username 출력 시 HTML 이스케이프 적용
$safe_username = htmlspecialchars($_SESSION['username'] ?? '', ENT_QUOTES, 'UTF-8');
?>

<!-- 로그인 사용자 -->
<a href="logout.php"

<?php else: ?>

<!-- 비로그인 사용자 -->
<a href="login.php">
<a href="join.php">

<?php endif; ?>
</nav>

</div>
</header>

<div class="container">
```



느낀점

- 이번 프로젝트를 총괄하면서 가장 크게 느낀 점은 **조율**의 중요성이었다
  여러 역할과 산출물이 동시에 맞물려 움직여야 했기 때문에, 일정과 품질,
  그리고 커뮤니케이션을 균형 있게 조정하는 일이 프로젝트 성공의 핵심임을 깨달았다.

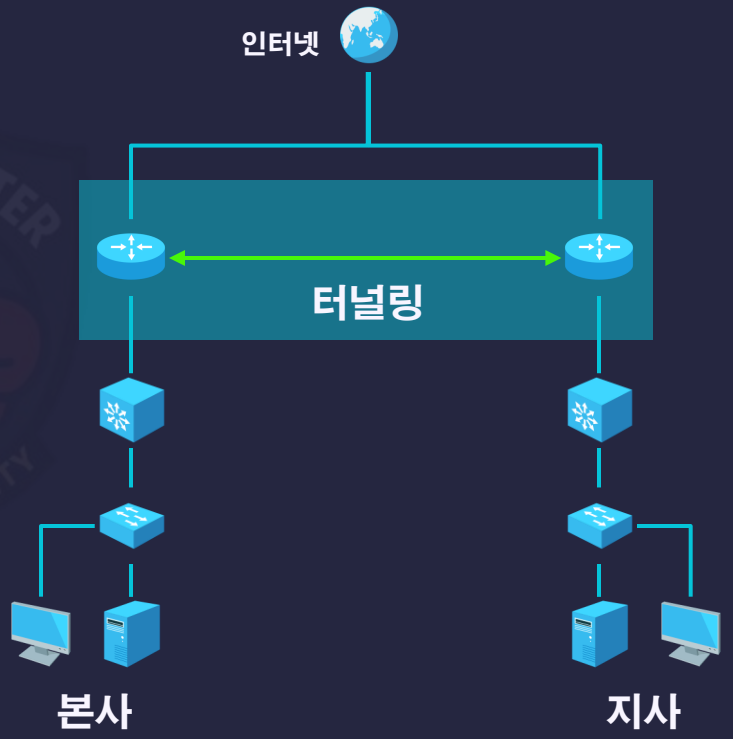
- 또 하나는 보안에 대한 인식 변화였다.
  보안은 기술적 설정만으로 완성되는 것이 아니라, **명확한 정책과 지침이 기반**이 될 때
  비로소 일관성과 지속성을 확보할 수 있다는 점을 깊이 체감했다.

- PM의 입장에서 보안을 바라보며, 기술적 보안 설정은 반드시 **정책이라는 기준**이 있어야
  방향성을 잃지 않는다는 것을 확인했다.

- 이번 과업을 통해 **정책 기반 보안**이 조직적 보안을 실현하는 핵심 요소임을 명확하게 이해할 수
  있었다.

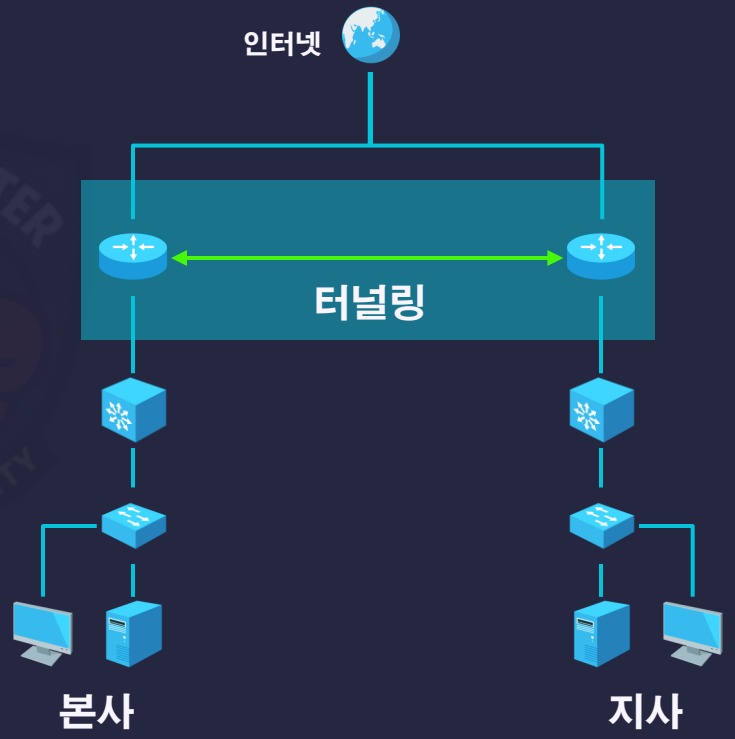
강버들

- 본사 · 지사 GRE over IPsec 적용
- OSPF
- 네트워크 장비 보안 적용



본사 · 지사 터널링 개요

- 본사 · 지사 **터널링** 적용
- **GRE 캡슐화**로 내부망 여러 서브넷을 **하나의 가상 링크**처럼 안정적으로 전달 가능



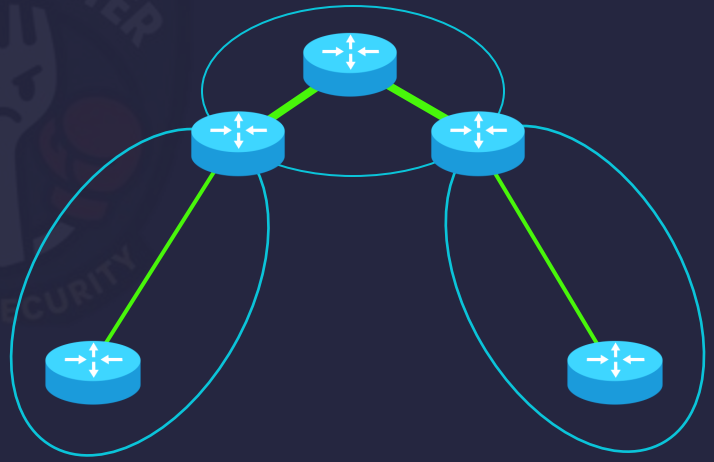
IPsec 암호화 구조 – Phase 1 ~ 2

- IPsec을 통해 데이터 기밀성 · 무결성 보장
- Phase 1: 보안 채널 수립 (ISAKMP/IKE 협상)
- Phase 2: 실제 데이터 암호화 (IPsec ESP 적용)
- GRE는 내부망을 운반, IPsec은 운반된 트래픽을 보호

OSPF 적용

- 링크 상태 기반 라우팅 프로토콜
- 네트워크 변경을 자동 감지하고 최적 경로 계산
- 장애 시 자동 복구
- 인프라 구조 확장 · 변경 시 운영 부담 최소화

OSPF 기반 네트워크 링크 구조 예시



OSPF Neighbor 형성

- 본사 · 지사 모두 **OSPF 기반 동적 라우팅** 구성
- **OSPF 적용**으로 라우터 간 경로 정보 자동 교환 · 동기화
- GRE 터널 인터페이스 상에서 **Neighbor** 관계 정상 성립

```
O       20.0.0.0/27 [110/11114] via 50.50.50.9, 01:09:19, Tunnel0
O       20.0.0.48/29 [110/11114] via 50.50.50.9, 01:09:19, Tunnel0
O       20.0.0.56/29 [110/11114] via 50.50.50.9, 01:09:19, Tunnel0
O       20.0.0.32/28 [110/11114] via 50.50.50.9, 01:09:21, Tunnel0
O       20.0.0.88/29 [110/11114] via 50.50.50.9, 01:09:21, Tunnel0
O       20.0.0.64/29 [110/11114] via 50.50.50.9, 01:09:21, Tunnel0
O       20.0.0.72/29 [110/11114] via 50.50.50.9, 01:09:21, Tunnel0
```

```
O       10.0.0.16/28 [110/11116] via 50.50.50.10, 01:11:25, Tunnel0
O       10.0.0.40/29 [110/11116] via 50.50.50.10, 01:11:25, Tunnel0
O       10.0.0.32/29 [110/11116] via 50.50.50.10, 01:11:27, Tunnel0
O       10.0.0.56/29 [110/11116] via 50.50.50.10, 01:11:27, Tunnel0
O       10.0.0.48/29 [110/11116] via 50.50.50.10, 01:11:27, Tunnel0
O       10.0.0.72/29 [110/11116] via 50.50.50.10, 01:11:27, Tunnel0
O       10.0.0.64/29 [110/11116] via 50.50.50.10, 01:11:27, Tunnel0
O       10.0.0.88/29 [110/11116] via 50.50.50.10, 01:11:27, Tunnel0
```

네트워크 트래픽 보안 설정

Network	기능 관리	DDoS 공격 방어 설정 또는 DDoS 장비 사용	상	N-13

- **비정상 Source IP**(내부망 발생 불가 주소)의 **유입 차단**
- **과도한 ICMP/SYN 트래픽 제한**으로 기본적인 DoS 영향 최소화
- 본사 · 지사 터널 구간은 필요한 프로토콜만 허용되도록 구성

네트워크 트래픽 보안 설정

- 비정상 Source IP(내부망 발생 불가 주소)의 유입 차단
- 과도한 ICMP/SYN 트래픽 제한으로 기본적인 DoS 영향 최소화
- 본사 · 지사 터널 구간은 필요한 프로토콜만 허용되도록 구성

Network	기능 관리	DDoS 공격 방어 설정 또는 DDoS 장비 사용	상	N-13

```
ip access-list extended ANTI_SPOOF
 deny   ip 0.0.0.0 0.255.255.255 any
 deny   ip 10.0.0.0 0.0.0.255 any
 deny   ip 127.0.0.0 0.255.255.255 any
 deny   ip 169.254.0.0 0.0.255.255 any
 deny   ip 172.16.0.0 0.15.255.255 any
 deny   ip 192.0.2.0 0.0.0.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 deny   ip 224.0.0.0 15.255.255.255 any
 permit ip any any
```

```
interface FastEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 ip access-group ANTI_SPOOF in
 ip nat outside
```

네트워크 트래픽 보안 설정

- 비정상 Source IP(내부망 발생 불가 주소)의 유입 차단
- 과도한 ICMP/SYN 트래픽 제한으로 기본적인 DoS 영향 최소화
- 본사 · 지사 터널 구간은 필요한 프로토콜만 허용되도록 구성

Network	기능 관리	DDoS 공격 방어 설정 또는 DDoS 장비 사용	상	N-13

```
    Class-map: ICMP-CLASS (match-all)
      51 packets, 4998 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol icmp
```

```
BR_UTM#ping 1.1.1.2 repeat 1000 size 1400

Type escape sequence to abort.
Sending 1000, 1400-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!
!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!
!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!
!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!
!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!
!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!
!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!
!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!
.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!
!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!
.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!
!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!.!
!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!
!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!.!
!!!!!!!!!!!!!.!!!!!!
Success rate is 93 percent (936/1000), round-trip min/avg/max = 28/57/80 ms
BR_UTM#
```

```
    Class-map: ICMP-CLASS (match-all)
      1132 packets, 1426936 bytes
      5 minute offered rate 30000 bps, drop rate 0 bps
      Match: protocol icmp
```

Trouble Shooting

NAT 예외 누락으로 인한 터널 실패

- 본사 · 지사 양쪽 모두 내부 트래픽이 NAT 대상에 포함되어 **IPsec 암호화가 적용되지 않는 문제 발생**
- IPsec 정책은 NAT 처리 이후 적용되므로 변형된 트래픽은 **Crypto ACL과 일치하지 않는 것으로 판단**
- **NAT_EXEMPT 재정의**하여 원본 트래픽 유지
- 본사 · 지사 간 라우팅/통신 정상화

NAT 예외 누락으로 인한 터널 실패

- 본사 · 지사 양쪽 모두 내부 트래픽이 NAT 대상에 포함되어 **IPsec 암호화가 적용되지 않는 문제 발생**
- IPsec 정책은 NAT 처리 이후 적용되므로 변형된 트래픽은 **Crypto ACL과 일치하지 않는 것으로 판단**
- **NAT_EXEMPT 재정의**하여 원본 트래픽 유지
- 본사 · 지사 간 라우팅/통신 정상화

```
!
ip access-list standard NAT_INSIDE
 permit 10.0.0.0 0.0.255.255
!
ip access-list extended NAT_EXEMPT
 permit ip 10.0.0.0 0.0.255.255 20.0.0.0 0.0.0.255
ip access-list extended VPN_ACL
 permit gre host 1.1.1.2 host 2.2.2.2
 permit gre host 2.2.2.2 host 1.1.1.2
 permit ip 10.0.0.0 0.0.255.255 20.0.0.0 0.0.0.255
 permit ip 20.0.0.0 0.0.0.255 10.0.0.0 0.0.255.255
no cdp log mismatch duplex
!
route-map NAT_HQ deny 10
 match ip address NAT_EXEMPT
!
route-map NAT_HQ permit 20
 match ip address NAT_INSIDE
!
```

OSPF Neighbor 형성

- 본사 · 지사 양쪽 모두 내부 트래픽이 NAT 대상에 포함되어 **IPsec 암호화가 적용되지 않는 문제 발생**
- IPsec 정책은 NAT 처리 이후 적용되므로 변형된 트래픽은 **Crypto ACL과 일치하지 않는 것으로 판단**
- **NAT_EXEMPT 재정의**하여 원본 트래픽 유지
- 본사 · 지사 간 라우팅/통신 정상화

isakmp

No.	Time	Source	Destination	Protocol	Length	Info
1758	654.147228	1.1.1.2	2.2.2.2	ISAKMP	206	Identity Protection (Main Mode)
1759	654.193177	2.2.2.2	1.1.1.2	ISAKMP	146	Identity Protection (Main Mode)
1760	654.209364	1.1.1.2	2.2.2.2	ISAKMP	346	Identity Protection (Main Mode)
1761	654.269907	2.2.2.2	1.1.1.2	ISAKMP	346	Identity Protection (Main Mode)
1762	654.299991	1.1.1.2	2.2.2.2	ISAKMP	142	Identity Protection (Main Mode)
1763	654.345909	2.2.2.2	1.1.1.2	ISAKMP	110	Identity Protection (Main Mode)
1764	654.359660	1.1.1.2	2.2.2.2	ISAKMP	206	Quick Mode
1765	654.389963	2.2.2.2	1.1.1.2	ISAKMP	206	Quick Mode
1766	654.405969	1.1.1.2	2.2.2.2	ISAKMP	102	Quick Mode

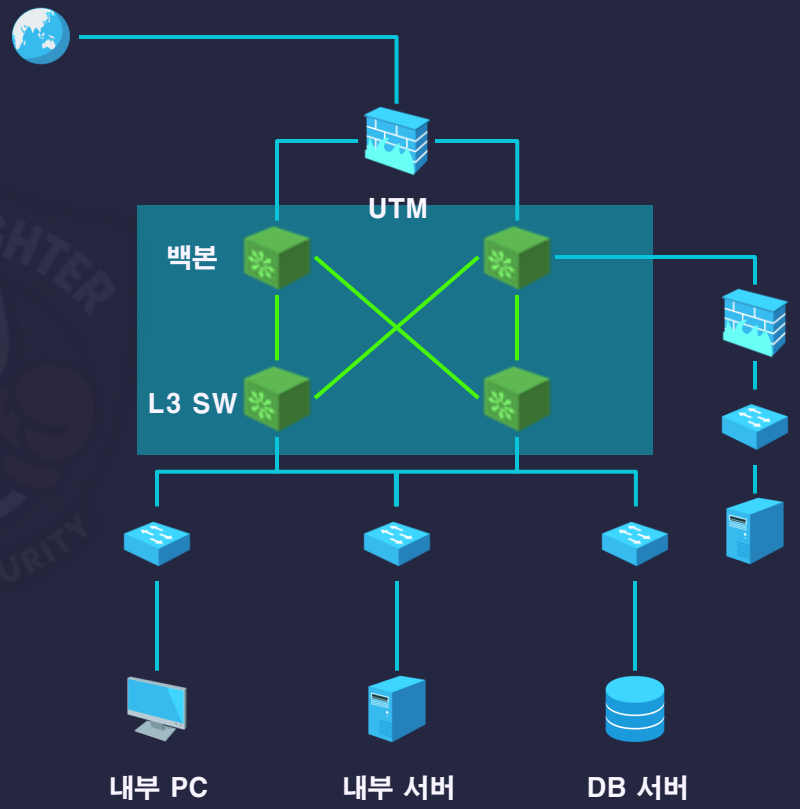
```
HQ_UTM#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.0.2           0   FULL/  -        00:00:35    50.50.50.9      Tunnel0
1.1.1.1           1   FULL/DR         00:00:36    10.0.1.10       FastEthernet1/0
HQ_UTM#
```

느낀점

- 이번 과업을 통해 인프라 구축 과정에서는 결코 **원인 없이 오류나 장애가 발생하지 않는다**는 사실을 다시 한 번 깨달았다.
- 논리적으로 완벽해 보였던 설계도 **실제 환경**에서는 장비의 설계 특성이나 버전 차이로 인해 **예상치 못한 제약**이 발생할 수 있음을 경험했다.
- 이러한 변수들을 세밀하게 파악하고 검증해 나가는 과정이 결국 **문제를 해결하는 가장 빠른 방법**임을 깊이 이해한 의미 있는 경험이었다.

이태호

- 서비스 차단
- 네트워크 이중화
- VLAN



서비스 차단(Proxy ARP)

- 라우터가 다른 **호스트를 대신해 ARP 요청에 응답**하는 기능
- 내부 유효 호스트 목록이 **노출되어 공격자의 정찰 활동을 쉽게 만듦**
- 라우터의 해당 인터페이스 설정 모드에서 **no ip proxy-arp** 명령어를 사용하여 기능을 명시적으로 비활성화

※ ARP : **IP 주소를 MAC 주소로** 변환

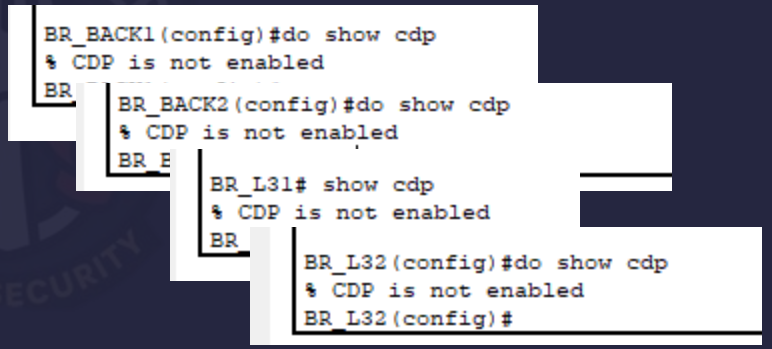
Network	기능 관리	Proxy arp 차단	중	N-29

```
interface Vlan110
 ip address 20.0.0.59 255.255.255.248
 ip helper-address 20.0.0.57
 no ip proxy-arp
 vrrp 110 ip 20.0.0.61
interface Vlan120
 ip address 20.0.0.65 255.255.255.248
 ip access-group 120 in
 ip helper-address 20.0.0.57
 no ip proxy-arp
 vrrp 120 ip 20.0.0.69
```

서비스 차단(CDP)

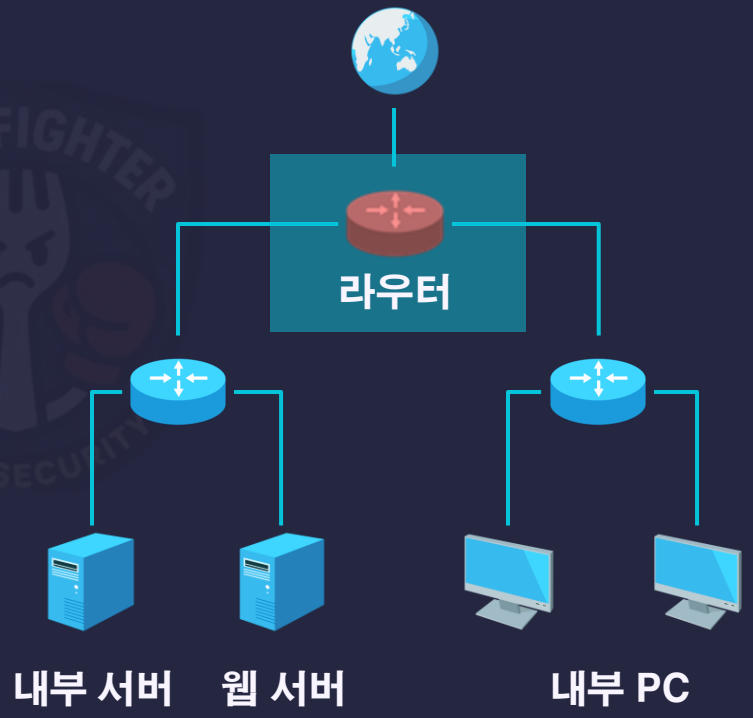
- Cisco 장비 간 **주변 장비 정보를 자동으로 탐색**하고 공유하기 위한 L2 프로토콜
- 장비 모델/OS 버전 등 **민감한 정보가 노출**되어 공격자의 네트워크 정찰 및 특정 **취약점 타겟 공격을 쉽게 만듦**
- 불필요한 정보 노출을 최소화하여 **정찰 단계의 공격을 방지**

Network	기능 관리	CDP 서비스 차단	중	N-32



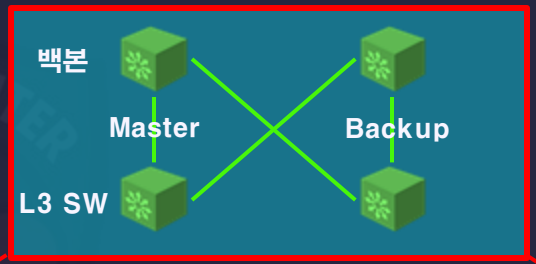
네트워크 이중화(취약)

- 장비 고장 시 **대체 수단이 없음**
- 서비스의 **연속성 및 가용성 하락**
- 장애 발생 시 업무가 즉시 중단되고 **복구 시간 증가**
- 서비스 중단으로 인한 **기업 신뢰도 하락**



네트워크 이중화(보안)

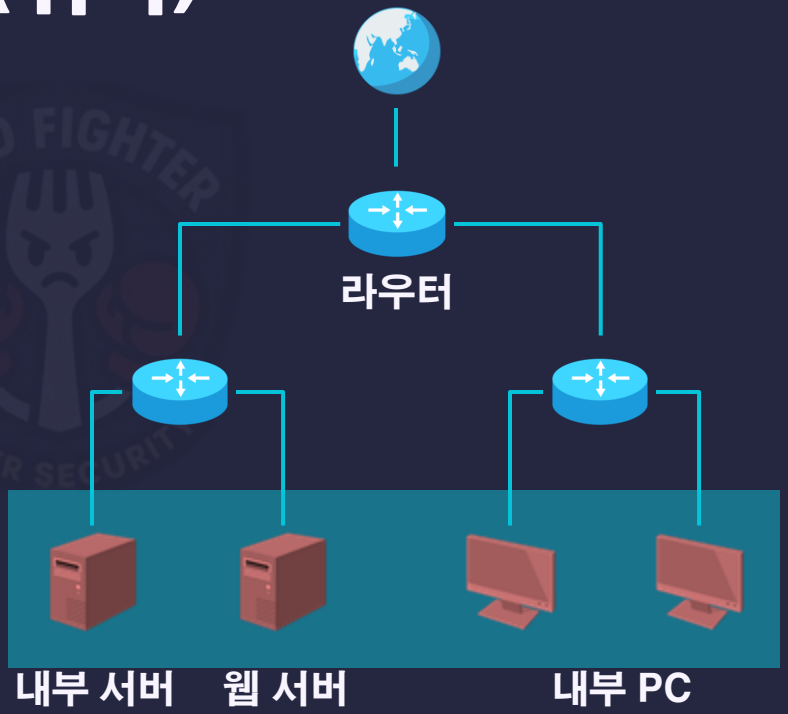
- 장애 발생 시에도 백업 경로가 즉시 작동하여 핵심 **서비스의 중단 없는 운영을 보장**
- 시스템이 항상 사용 가능한 상태를 유지, **네트워크의 전반적인 신뢰도 향상**
- 데이터 트래픽 증가에 대비하여 **네트워크 용량을 유연하게 확장할 수 있는 기반**을 마련




```
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
V1230              230 110 3570       Y  Backup  172.16.0.2      172.16.0.254
V1240              240 110 3570       Y  Backup  172.17.0.2      172.17.0.254
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
V1230              230 110 3570       Y  Master  172.16.0.2      172.16.0.254
V1240              240 110 3570       Y  Master  172.17.0.2      172.17.0.254
```

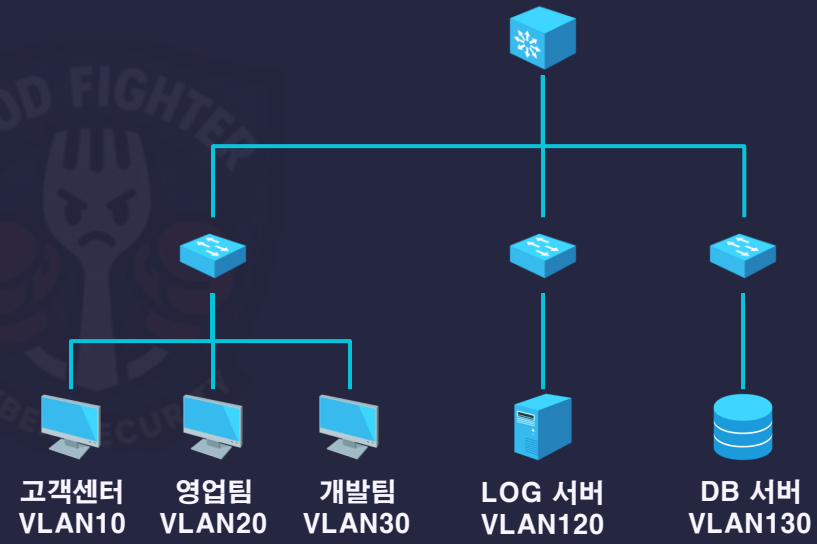
논리적 네트워크 분할(취약)

- 악성 트래픽 네트워크 전체로 확산
- 전체 네트워크 성능 저하 및 병목 현상을 유발
- 관리 및 문제 해결이 복잡하고 비효율적



논리적 네트워크 분할(보안)

- VLAN : 하나인 스위치를 여러 개의 네트워크로 나누는기술
- 네트워크를 여러 개의 논리적인 브로드캐스트 도메인으로 분할
- 민감한 데이터나 시스템에 대한 접근을 제한하여 보안 사고의 위험 감소
- 각 그룹에 필요한 만큼의 적절한 크기의 서브넷을 할당



Trouble Shooting

트러블 슈팅

- GNS 작업중 PC에서 외부 망으로 Ping을 보낼 수 없던 상황 발생
- 발생한 경로를 따라 설정 확인
- 광고는 잘 되어 있었으나 경로를 학습 실패

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   2WAY/DROTHER    00:00:34    172.17.0.4      Vlan240
3.3.3.1           1   FULL/BDR        00:00:34    172.17.0.1      Vlan240
3.3.3.2           1   FULL/DR         00:00:33    172.17.0.2      Vlan240
1.1.1.1           1   2WAY/DROTHER    00:00:34    172.16.0.4      Vlan230
3.3.3.1           1   FULL/BDR        00:00:34    172.16.0.1      Vlan230
3.3.3.2           1   FULL/DR         00:00:33    172.16.0.2      Vlan230
1.1.1.1           1   FULL/DR         00:00:34    20.0.0.44       Vlan20
1.1.1.1           1   FULL/BDR        00:00:35    20.0.0.27       Vlan10
L3SW1(config)#do show standby bri
```

```
ateway of last resort is not set

  20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
     20.0.0.0/27 is directly connected, Vlan10
     20.0.0.32/28 is directly connected, Vlan20
  172.17.0.0/24 is subnetted, 1 subnets
     172.17.0.0 is directly connected, Vlan240
  172.16.0.0/24 is subnetted, 1 subnets
     172.16.0.0 is directly connected, Vlan230
```

트러블 슈팅

- Trunk 설정을 한 포트 확인 결과 **설정이 다른 것을 확인**
- 설정을 일치시킨 후 정상적으로 핑이 가는 것을 확인

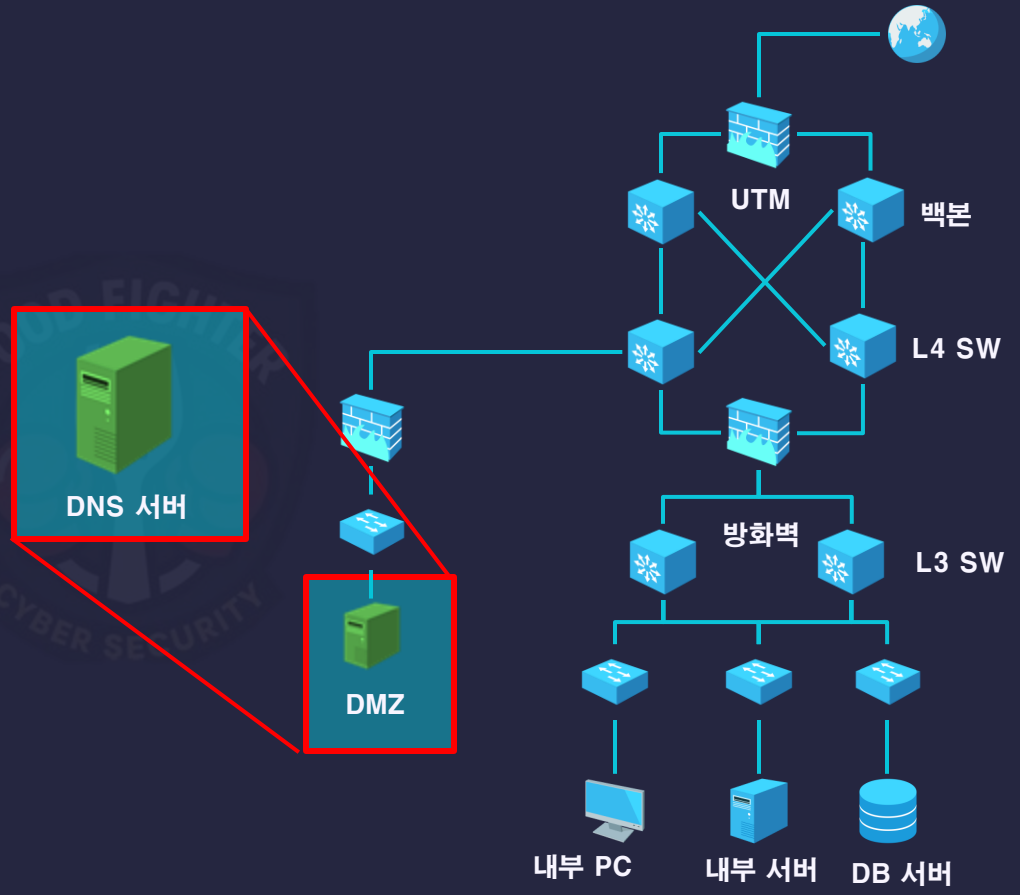
```
PC1> ping 20.0.0.29
84 bytes from 20.0.0.29 icmp_seq=1 ttl=255 time=29.920 ms
84 bytes from 20.0.0.29 icmp_seq=2 ttl=255 time=14.960 ms

PC1> ping 20.0.0.28
84 bytes from 20.0.0.28 icmp_seq=1 ttl=255 time=29.920 ms
84 bytes from 20.0.0.28 icmp_seq=2 ttl=255 time=29.920 ms
84 bytes from 20.0.0.28 icmp_seq=3 ttl=255 time=29.919 ms

PC1> ping 172.16.0.3
84 bytes from 172.16.0.3 icmp_seq=1 ttl=255 time=29.919 ms
84 bytes from 172.16.0.3 icmp_seq=2 ttl=255 time=14.960 ms
84 bytes from 172.16.0.3 icmp_seq=3 ttl=255 time=29.920 ms

PC1> ping 172.16.0.1
172.16.0.1 icmp_seq=1 timeout
84 bytes from 172.16.0.1 icmp_seq=2 ttl=254 time=74.800 ms
84 bytes from 172.16.0.1 icmp_seq=3 ttl=254 time=59.840 ms
```

느낀점

- 네트워크 이중화를 통해 단일 장애 지점을 제거하면서 **안정성과 통신 연속성을 확보할 수 있었다.**
- 또한 VLAN을 적용해 논리적으로 망을 분리함으로써 보안을 강화하고 **트래픽 관리도 더욱 효율적으로 수행할 수 있었다.**
- 이와 같은 구성으로 지사 네트워크에서 **안정성과 관리 효율을 동시에 달성**하며, 보다 견고한 업무 환경을 구축한 의미 있는 경험이었다.

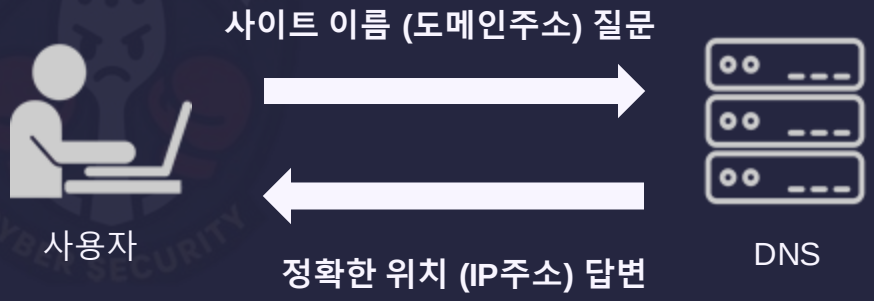
이서진

- 본사, 지사 윈도우 DNS 서버



DNS 란?

- DNS란 **도메인 이름을 IP 주소로 바꿔주는** 인터넷의 주소 변환 시스템
- **사이트 이름 (도메인 주소)로 서비스 접근 가능**
- **www.babhelp.com**



윈도우 DNS 구축

- Zone(영역): DNS가 책임지고 관리하는 도메인 또는 IP 주소 범위의 데이터 저장 영역
- 정방향 영역으로 babhelp.com 생성
- A레코드 www. - 20.0.0.81
- 역방향 영역으로 20.0.0.x 생성

정방향 babhelp.com

이름	종류	데이터
(상위 폴더와 같음)	SOA(권한 시작)	[9], br_dns_sec., hostmast...
(상위 폴더와 같음)	NS(이름 서버)	br_dns_sec.
db	호스트(A)	20.0.0.65
root	호스트(A)	20.0.0.81
root	MX(메일 교환기)	[10] www.babhelp.com.
www	호스트(A)	20.0.0.81

역방향 20.0.0.x

이름	종류	데이터
(상위 폴더와 같음)	SOA(권한 시작)	[2], br_dns_sec., hostmast...
(상위 폴더와 같음)	NS(이름 서버)	br_dns_sec.
20.0.0.81	PTR(포인터)	babhelp.com.

윈도우 DNS 보안 설정

- 윈도우 DNS 보안 설정은 **주요 정보 통신 기반 시설의 윈도우 취약점 보안 기준**에 맞춰 진행

분류	점검 항목	위험도	항목코드
서비스 관리	DNS Zone Transfer 설정	상	W-29
서비스 관리	DNS 서비스 구동 점검	중	W-63
로그 관리	로그의 정기적 검토 및 보고	상	W-34

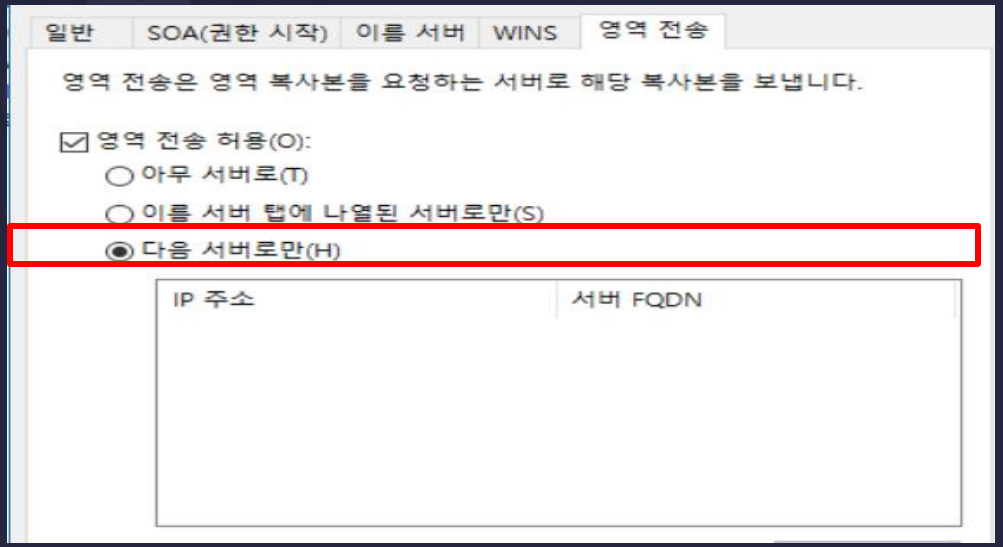
윈도우 DNS 보안 설정

- 영역 전송 : 도메인 구조를 다른 서버에 전달하는 기능
- 지정된 서버만 영역 전송 허용
- 데이터 불법 외부 유출 방지 DNS Recon 공격 차단

※ DNS Recon : DNS를 조사해 서버 구조, 서브도메인, 레코드 정보를 대량 수집하여 이후 공격을 준비하는 정보 수집 정찰 과정

Windows	서비스 관리	DNS Zone Transfer 설정	상	W-29

정방향 babhelp.com



윈도우 DNS 보안 설정

- **동적 업데이트 제거**
- 신뢰할 수 없는 데이터 업데이트 방지
- 비인가 시스템의 **DNS 레코드 생성 · 수정 차단**
- DNS 스푸핑 · 하이재킹 방지

※ DNS 스푸핑 : DNS 서버로 보내는 질문을 가로채서 변조된 결과를 보내주는 것

※ DNS 하이젝킹 : DNS 설정을 공격자가 빼앗아서 사용자가 입력한 도메인을 원래랑 다른 IP로 계속 돌려버리는 공격

Windows	서비스 관리	DNS 서비스 구동 점검	중	W-63

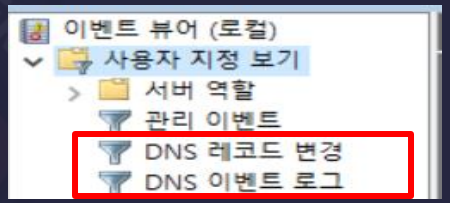
정방향 babhelp.com

윈도우 DNS 보안 설정

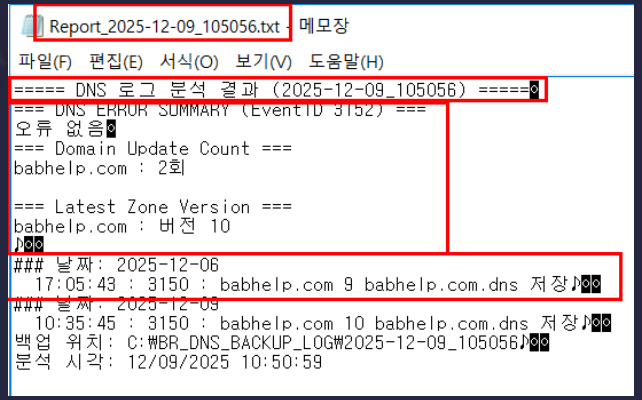
- 공격 식별과 추가조치 필요
- DNS **로그 사용자 지정 보기** 구성
- **매주 로그 분석 보고서** 작성
- 문제 발생 시 **즉시 원인을 추적**할 수 있는 구조로 개선
- 안정적인 시스템 상태 유지

Windows	로그관리	로그의 정기적 검토 및 보고	상	W-34

사용자 지정보기



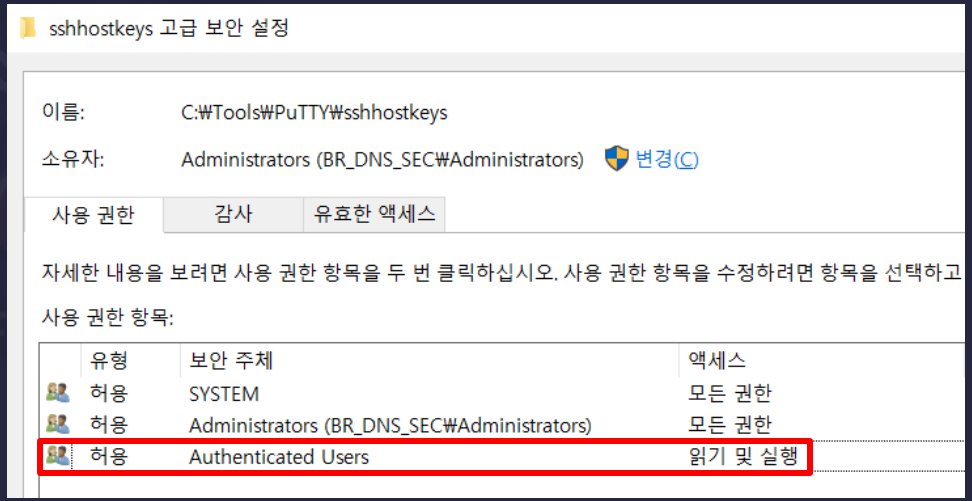
로그 분석 보고서



Trouble Shooting

트러블 슈팅 (윈도우 와 Rocky SSH 접속)

- 키 파일이 권한에 Users가 포함되어 **최소 권한 원칙 위배**
- Rocky의 ssh가 보안 위험으로 판단 하여 **접속 거부**
- 공개키 파일 권한에 **상속과 Users를 제거하여 해결**

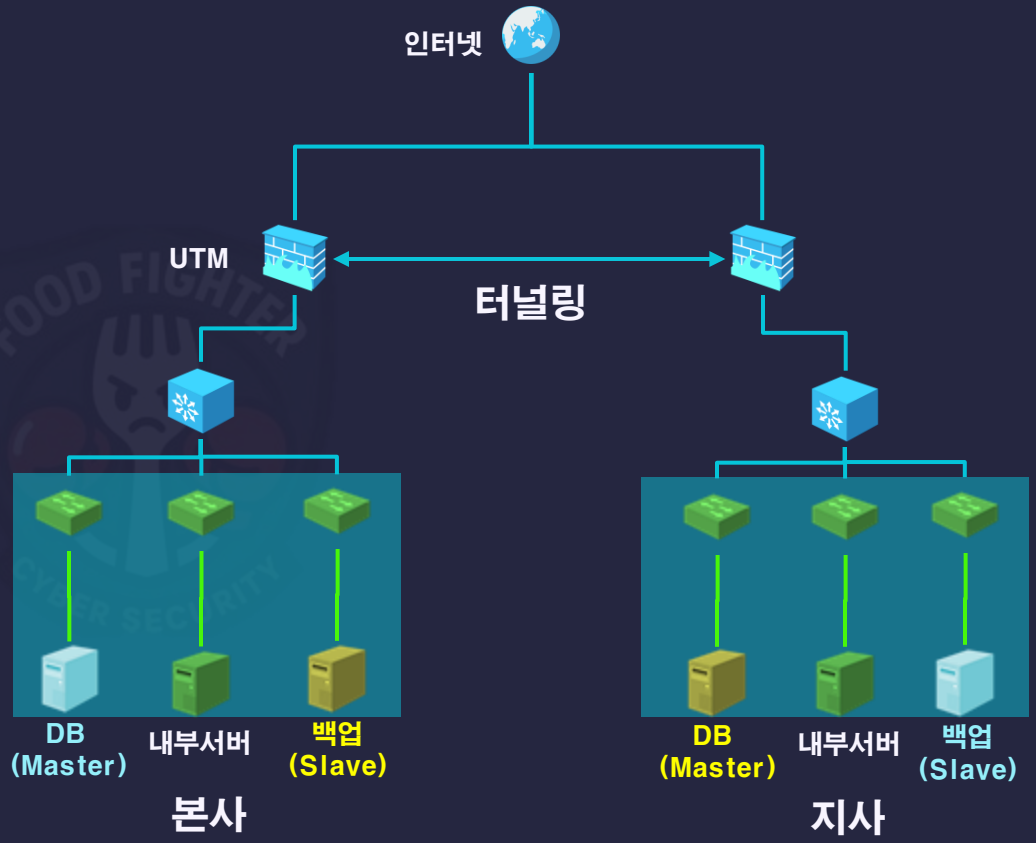


느낀점

- 보안 설정과 로그 필터링을 구성하면서 운영 단계에서 **문제를 발견하고 대응하는 능력**이 구축 과정만큼 중요하다는 사실을 느낄 수 있었다.
- 아울러 권한 관리와 보안 정책의 세부 요소가 시스템 전반에 큰 영향을 미친다는 점을 경험하며, **보안은 무엇보다 사전 예방이 핵심**임을 다시 한 번 확인하게 되었다.

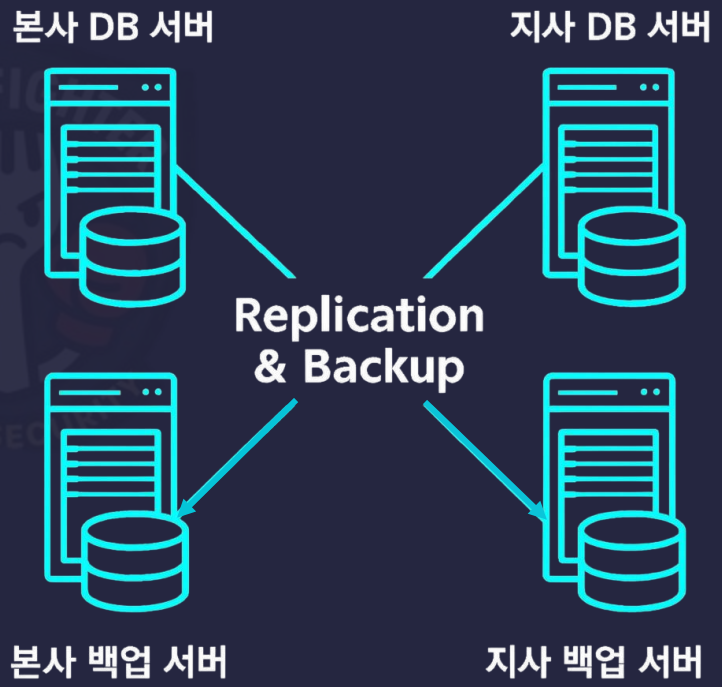
이남혁

- DB 이중화(Master-Slave)
- 백업 서버 구축



본사 · 지사 DB 이중화

- 본사 · 지사 간 **DB 이중화 구조** 구축으로 데이터 안정성 확보
- **Master · Slave** 구조 기반으로 데이터 변경 사항을 **실시간 복제**
- 복제본을 통해 조회 **트래픽 분산** 및 운영 **안정성 강화**



본사 · 지사 DB 이중화 – 동기화

- 덤프로 동일한 데이터 기준을 맞춘 뒤, **Master 변경사항이 Slave로 실시간 전달** 시작
- **Slave의 IO · SQL 동작 상태가 모두 정상으로 표시되어 복제 과정에 오류가 없음**

```
[root@HQ_DB_SEC backup]# mysqldump -u root -p -A > /backup/all_1126.sql
Enter password:
[root@HQ_DB_SEC backup]# scp /backup/all_1126.sql 20.0.0.89:/backup
root@20.0.0.89's password:
all_1126.sql                                  100% 1998KB   1.3MB/s   00:01
[root@HQ_DB_SEC backup]#
```

```
[root@BR_BACKUP_SEC ~]# cd /backup
[root@BR_BACKUP_SEC backup]# ll
합계 4000
-rw-r--r--. 1 root root 2045556 11월  26 23:34 all.sql
-rw-r--r--. 1 root root 2045553 11월  26 23:42 all_1126.sql
[root@BR_BACKUP_SEC backup]#
MariaDB [(none)]> START SLAVE;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> SHOW SLAVE STATUS\G;
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: 10.0.0.73
                  Master_User: slave
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mysql-bin.000004
          Read_Master_Log_Pos: 342
               Relay_Log_File: mariadb-relay-bin.000002
                Relay_Log_Pos: 555
        Relay_Master_Log_File: mysql-bin.000004
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
              Replicate_Do_DB: babseguen
```

본사 · 지사 DB 이중화 – 복제 검증

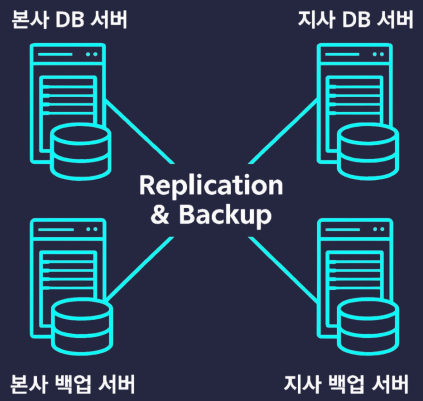
- Master(DB서버) :
  모든 **원본 데이터** 처리 및
  쓰기 연산 담당
- Slave(백업서버) :
  실시간 읽기 전용 복제본 유지
- 서비스 장애 시 Slave를
  활용하여 **데이터 손실 최소화**

```
MariaDB [babseguen]> USE babseguen;
Database changed
MariaDB [babseguen]>
MariaDB [babseguen]> INSERT INTO TBL_MEMBER (email, password, name, phone)
    -> VALUES ('test999@bap.com', '1234', 'replication_test', '010-9999-9999');
Query OK, 1 row affected (0.001 sec)

MariaDB [babseguen]>
```

```
MariaDB [babseguen]> SELECT * FROM TBL_MEMBER WHERE email='test999@bap.com';
+-----------+----------------+----------+------------------+--------------+--------+---
-----------------+---------------------+
| member_id | email          | password | name             | phone        | status | cr
eated_at          | updated_at          |
+-----------+----------------+----------+------------------+--------------+--------+---
-----------------+---------------------+
|         4 | test999@bap.com | 1234     | replication_test | 010-9999-9999 |      1 | 20
25-11-25 04:28:19 | 2025-11-25 04:28:19 |
+-----------+----------------+----------+------------------+--------------+--------+---
-----------------+---------------------+
1 row in set (0.000 sec)

MariaDB [babseguen]>
```

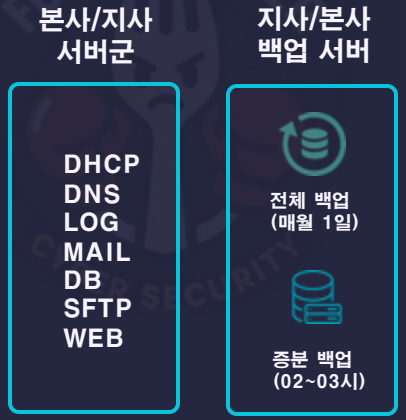
백업 서버 구축

- **본사 · 지사 백업 서버 구축**으로 데이터 보호 체계 강화
- **전체 백업** : 특정 시점의 전체 데이터를 통째로 백업하는 방식
- **증분 백업** : 이전 백업 이후 변경된 데이터만 저장하는 방식



백업 서버 구축

- 서비스별 분리 저장 구조 설계
- DB만 전체 + 증분 백업을 사용하고, 나머지 서버는 파일 단위 전체 백업 방식




```
[root@BR_BACKUP_SEC backup]# ll
합계 32
drwxrwx---. 4 root backup 4096 11월  28 00:00 dhcp
drwxrwx---. 4 root backup 4096 11월  28 00:00 dns
drwxrwx---. 4 root backup 4096 11월  28 00:00 log
drwxrwx---. 4 root backup 4096 11월  28 00:00 mail
drwxrwx---. 4 root backup 4096 11월  27 11:32 mariadb
drwxrwx---. 4 root backup 4096 11월  28 00:00 sftp
drwxrwx---. 2 root backup 4096 11월  27 11:51 tmp
drwxrwx---. 4 root backup 4096 11월  28 00:00 web
```

백업 서버 구축

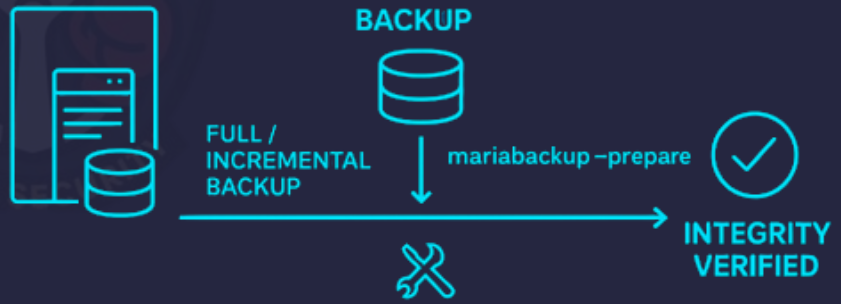
- 백업 서버로 수신된 **전체, 증분 백업**을 일자별로 체계적으로 저장


```
[root@BR_BACKUP_SEC mariadb]# ll
합계 8
drwxr-x---.  4 root backup 4096 12월  9 12:11 full
drwxr-x---. 15 root backup 4096 12월  9 11:53 inc
[root@BR_BACKUP_SEC mariadb]# cd full
[root@BR_BACKUP_SEC full]# ll
합계 8
drwxr-x---. 6 root backup 4096 11월 27 02:00 2025-11-27
drwxr-x---. 6 root backup 4096 12월  1 02:00 2025-12-01
[root@BR_BACKUP_SEC full]# cd ../inc
[root@BR_BACKUP_SEC inc]# ll
합계 52
drwxr-x---. 6 root backup 4096 11월 26 02:10 2025-11-26
drwxr-x---. 6 root backup 4096 11월 27 02:10 2025-11-27
drwxr-x---. 2 root backup 4096 11월 28 02:10 2025-11-28
drwxr-xr-x. 2 root root   4096 11월 29 02:10 2025-11-29
drwxr-xr-x. 2 root root   4096 11월 30 02:10 2025-11-30
drwxr-xr-x. 2 root root   4096 12월  2 02:10 2025-12-02
drwxr-xr-x. 2 root root   4096 12월  3 02:10 2025-12-03
drwxr-xr-x. 2 root root   4096 12월  4 02:10 2025-12-04
drwxr-xr-x. 2 root root   4096 12월  5 02:10 2025-12-05
drwxr-xr-x. 2 root root   4096 12월  6 02:10 2025-12-06
drwxr-xr-x. 2 root root   4096 12월  7 02:10 2025-12-07
drwxr-xr-x. 2 root root   4096 12월  8 02:10 2025-12-08
drwxr-xr-x. 2 root root   4096 12월  9 02:10 2025-12-09
```

Trouble Shooting

백업 무결성 검증 문제

- 증분 백업이 이어져야 할 LSN 구간이 끊겨 발생하는 오류로, **백업 생성 시점 불일치** 또는 **binlog 타임라인 불일치**에서 주로 발생



백업 무결성 검증 문제 해결

- 백업 파일 단위의 해시 비교로 무결성 검증 수행
- 문제가 되었던 LSN 불일치 오류는 --prepare 단계에서 최초로 감지됨
- 모든 서비스 파일을 SHA256 기반으로 검증하여 전체 백업 체계 안정성 확보

```
INC_DIR="$BASE/mariadb/inc"
mkdir -p "$HASH_BASE/mariadb/inc"

for dir in "$INC_DIR"/*; do
    if [[ -d "$dir" ]]; then
        for file in "$dir"/*; do
            if [[ -f "$file" ]]; then
                HASHFILE="$HASH_BASE/mariadb/inc/$(basename $dir)_$(basename $file).sha256"
                check_file_integrity "$file" "$HASHFILE"
            fi
        done
    fi
done
```

```
FULL_DIR="$BASE/mariadb/full"
mkdir -p "$HASH_BASE/mariadb/full"

for dir in "$FULL_DIR"/*; do
    if [[ -d "$dir" ]]; then
        echo "[INFO] FULL 백업 prepare 테스트: $dir" >> "$LOGFILE"
        mariabackup --prepare --target-dir="$dir" >> "$LOGFILE" 2>&1
```

```
SERVICES=("dhcp" "dns" "log" "mail" "sftp" "web")

for svc in "${SERVICES[@]}"; do
    echo "---- [$svc] ----" >> "$LOGFILE"
    mkdir -p "$HASH_BASE/$svc"

    for file in $(find "$BASE/$svc" -type f); do
        HASHFILE="$HASH_BASE/$svc/$(echo $file | sed 's/\//_/g').sha256"
        check_file_integrity "$file" "$HASHFILE"
    done
done
```

백업 무결성 검증 문제 해결

- 전체 백업의 LSN 구조가 정상적으로 기록되어 백업본 자체의 무결성이 확인됨
- 백업 서버에서 필수 파일 (LSN, binlog,데이터파일)이 모두 온전하게 존재함
- 백업 수신 · 무결성 검증 · 로그 정리가 자동 스케줄로 구성된 백업 운영 체계 구축

```
[root@HQ_DB_SEC ~]# cat /backup/db/full-2025-12-03/xtrabackup_checkpoints
backup_type = full-backuped
from_lsn = 0
to_lsn = 1743798
last_lsn = 1743807
[root@HQ_DB_SEC ~]#
[root@BR_BACKUP_SEC full]# ll
합계 8
drwxr-x---. 6 root backup 4096 11월  27 02:00 2025-11-27
drwxr-x---. 6 root backup 4096 12월   1 02:00 2025-12-01
[root@BR_BACKUP_SEC full]# cd 2025-12-01/
[root@BR_BACKUP_SEC 2025-12-01]# ll
합계 12344
-rwxr-x---. 1 root backup    16384 12월   1 02:00 aria_log.00000001
-rwxr-x---. 1 root backup       52 12월   1 02:00 aria_log_control
drwxr-x---. 2 root backup     4096 12월   9 11:52 babseguen
drwxr-x---. 2 root backup     4096 12월   9 11:52 babseservice
-rwxr-x---. 1 root backup      325 12월   1 02:00 backup-my.cnf
-rwxr-x---. 1 root backup     2560 12월   1 02:00 ib_logfile0
-rwxr-x---. 1 root backup 12582912 12월   1 02:00 ibdata1
drwxr-x---. 2 root backup     4096 12월   9 11:52 mysql
drwxr-x---. 2 root backup     4096 12월   9 11:52 performance_schema
-rwxr-x---. 1 root backup       28 12월   1 02:00 xtrabackup_binlog_info
-rwxr-x---. 1 root backup       77 12월   1 02:00 xtrabackup_checkpoints
-rwxr-x---. 1 root backup      540 12월   1 02:00 xtrabackup_info
```

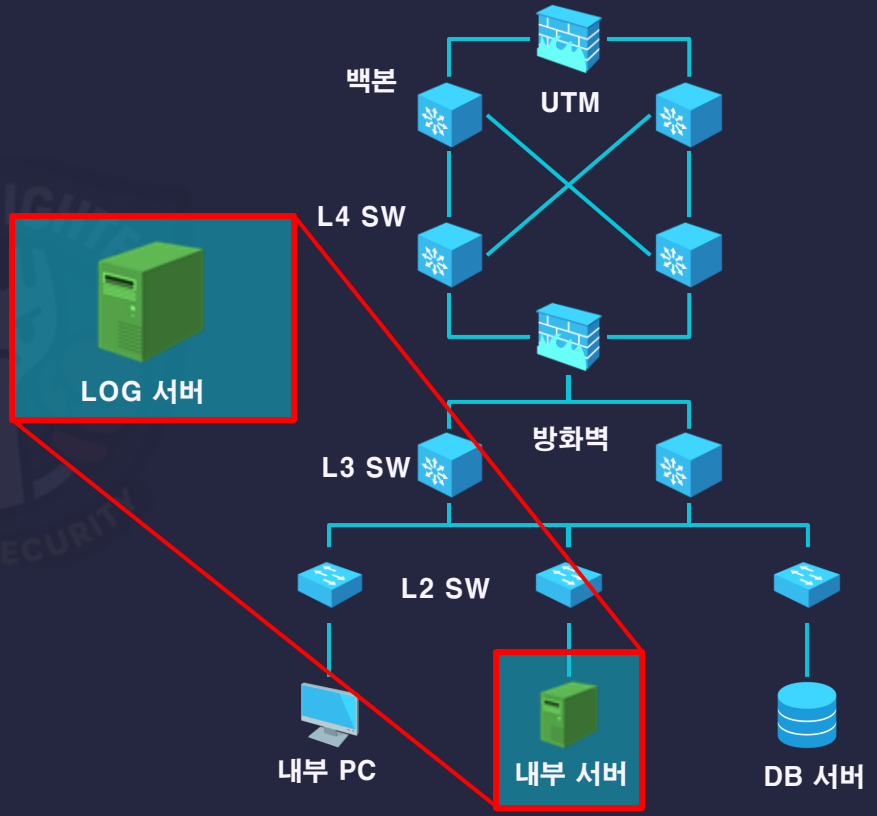
```
root@BR_BACKUP_SEC:/usr/local/bin
# 1시간마다 서버 백업 수신 정리
0 * * * * /usr/local/bin/rsync_receive.sh

# 매일 새벽 05:00 무결성 검사
0 5 * * * /usr/local/bin/check_integrity.sh

# 로그 정리 (매일 새벽 05:10)
10 5 * * * /usr/local/bin/cleanup_integrity.sh
```

느낀점

- 이번 과업을 진행하며 운영 · 백업 · 보안은 분리된 기능이 아니라 하나의 흐름으로 설계될 때 시스템이 비로소 안정화된다는 점을 깊이 체감했다.
- 본사 · 지사 DR 구조를 구축하며, 정확한 시간 관리와 일관된 정책 설계의 중요성을 다시 확인했다.

최장현

- 정책서
- LOG 서버 ELK 스택 기반
  통합 모니터링 시스템 구축



정책서

- 참고근거 법령
- 로그서버 정책

제 2 조(근거 법령)

본 정책은 다음의 법 및 기준을 준수한다

1. 개인정보 보호법 및 시행령
2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 시행령
3. 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드
4. 개인정보의 안전성 확보조치 기준

U-43	SRV-115	상	로그의 정기적 검토 및 보고

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보처리시스템에 접속한 자(다만, 정보주체는 제외한다)의 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다.

1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
3. 개인정보처리자로서 「전기통신사업법」 제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보취급자의 개인정보처리시스템에 대한 접속기록 및 개인정보 다운로드 상황을 확인하고 점검하는 주기·방법·사후조치절차 등을 내부 관리계획으로 정하고 이행하여야 한다.

③ 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

정책서

- 참고근거 법령
- 로그서버 정책

제 10 조(로그 및 모니터링)

로그 및 모니터링 체계를 운영하기 위해 다음 기준을 적용한다.

1. 모든 대상 시스템의 로그를 중앙 서버로 안정적으로 수집하고 데이터 누락을 방지한다.
2. 로그는 위·변조 방지 기능을 적용하여 보관한다.
3. 로그는 1 년 이상 보관하며, 법령에서 요구하는 경우 기간을 확장한다.
4. 이상징후 발생 시 즉시 정보보호책임자(CISO)에 보고한다.

Log(모니터링)

- 기존 문제점
- 문제 발생 시 담당자가 수동으로 확인 필요하여 실시간 대응 어려움

```
drwx------+ 2 root root 4096 11월  27 23:40 BR_LOG_SEC
drwx------+ 2 root root 4096 11월  28 10:41 BR_MAIL_SEC
drwx------+ 2 root root 4096 11월  28 10:37 BR_PHP_SEC
drwx------+ 2 root root 4096 11월  28 09:39 BR_SFTP_SEC
[root@BR_LOG_SEC remote]#
```

```
[root@BR_LOG_SEC remote]# cd BR_MAIL_SEC/
[root@BR_LOG_SEC BR_MAIL_SEC]# ll
합계 16
-rw-r-----+ 1 root root 682 11월  28 10:41 sshd.log
-rw-r-----+ 1 root root 340 11월  28 10:41 unix_chkpwd.log
[root@BR_LOG_SEC BR_MAIL_SEC]# vi sshd.log
[root@BR_LOG_SEC BR_MAIL_SEC]# cat sshd.log
Nov 28 10:41:03 BR_MAIL_SEC sshd[1360]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=
0 tty=ssh ruser= rhost=20.0.0.85  user=root
Nov 28 10:41:05 BR_MAIL_SEC sshd[1360]: Failed password for root from 20.0.0.85 port 55881 ssh2
Nov 28 10:41:10 BR_MAIL_SEC sshd[1360]: Failed password for root from 20.0.0.85 port 55881 ssh2
Nov 28 10:41:03 BR_MAIL_SEC sshd[1360]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=
0 tty=ssh ruser= rhost=20.0.0.85  user=root
Nov 28 10:41:05 BR_MAIL_SEC sshd[1360]: Failed password for root from 20.0.0.85 port 55881 ssh2
Nov 28 10:41:10 BR_MAIL_SEC sshd[1360]: Failed password for root from 20.0.0.85 port 55881 ssh2
```

Log(모니터링)

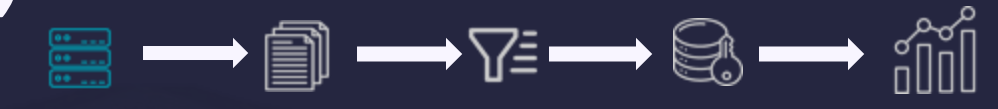
로그 데이터 파이프라인 구축

1. Log 파일 **생성/수집**
2. 파일 **감지 및 전달**
3. 전달 받은 파일 **파싱**
4. 파싱된 파일 저장소에 **저장**
5. 저장된 파일을 **시각화**

Log 서버 설정(1/5)

- Rsyslog 설정

(1) 수신 프로토콜 활성화
(2) 로그 포맷 지정




```
18 # Provides UDP syslog reception
19 # for parameters see http://www.rsyslog.com/doc/imudp.html
20 module(load="imudp")
21 input(type="imudp" port="514")
22
23 # Provides TCP syslog reception
24 # for parameters see http://www.rsyslog.com/doc/imtcp.html
25 module(load="imtcp")
26 input(type="imtcp" port="514")
```

```
template(name="RemoteLogs" type="string"
 string="/var/log/remote/%HOSTNAME%/%PROGRAMNAME%.log")

*.* ?RemoteLogs
```

Log 서버 설정(2/5)

- Filebeat 설정

(1) 로그 실시간 감지(input)
(2) logstash 전달(output)

```
filebeat.inputs:
- type: filestream
  id: all-remote-logs
  enabled: true
  paths:
    - /var/log/remote/*/*.log
  fields_under_root: true
```

```
output.logstash:
  # The Logstash hosts
  hosts: ["20.0.0.65:5044"]
```

Log 서버 설정(3/5)

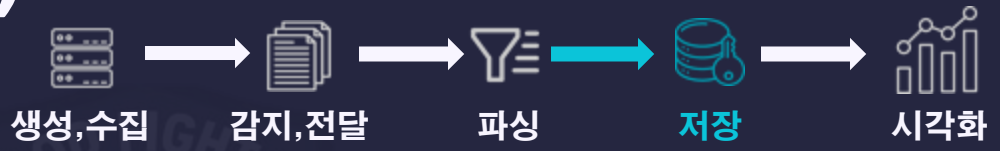
- Logstash 설정

(1) 전달받는 방식(input)
(2) 파싱 후 전달할 방식(output)

```
input {
    beats {
        port => 5044
        codec => "plain"
```

```
output {
    elasticsearch {
        hosts => ["https://20.0.0.65:9200"]
        user => "elastic"
        password => "-A=irjuaEfcnvUML4DQK"

        index => "logstash-tcp-%{+YYYY.MM.dd}"
```

Log 서버 설정(4/5)



- **Elasticsearch 설정**

(1) 네트워크 호스트를 20.0.0.65로 설정하여 내부 접속만 허용

(2) 기본 포트를 9200으로 설정

```
network.host: 20.0.0.65
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
```

Log 서버 설정(5/5)

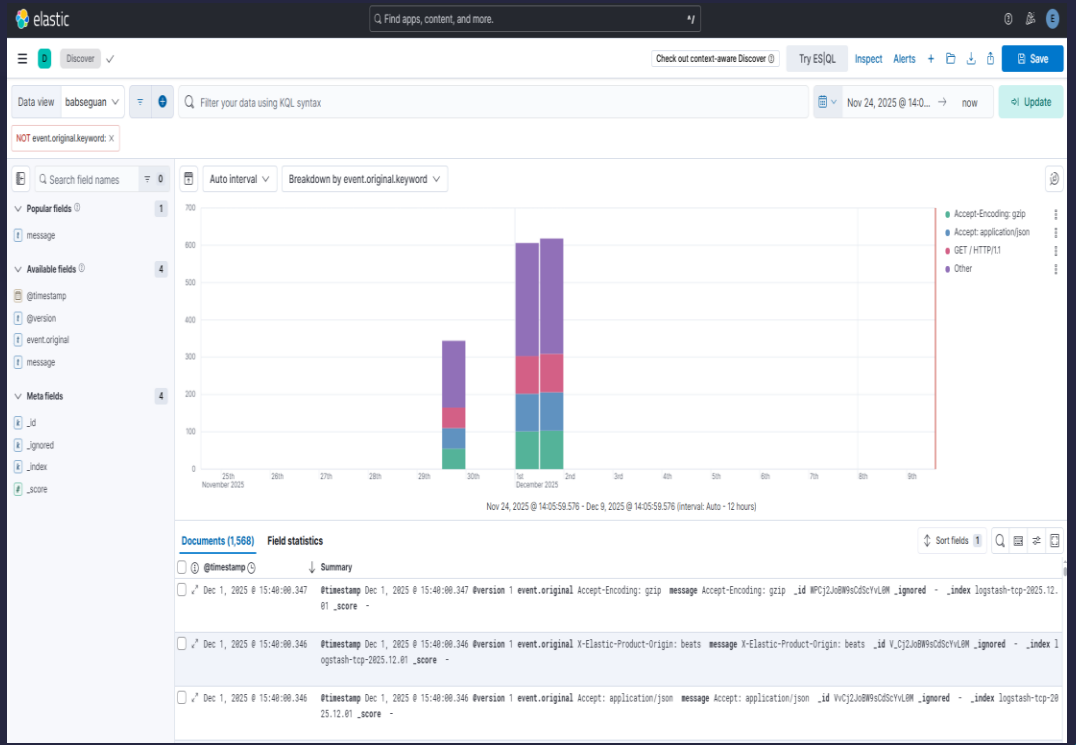
- kibana 설정

(1) 서버의 포트와 외부 접속 여부
(2) 연결을 시도할 IP 지정

```
# This section was automatically generated during setup.
server.port: 5601
server.host: localhost
elasticsearch.hosts: [https://20.0.0.65:9200]
```

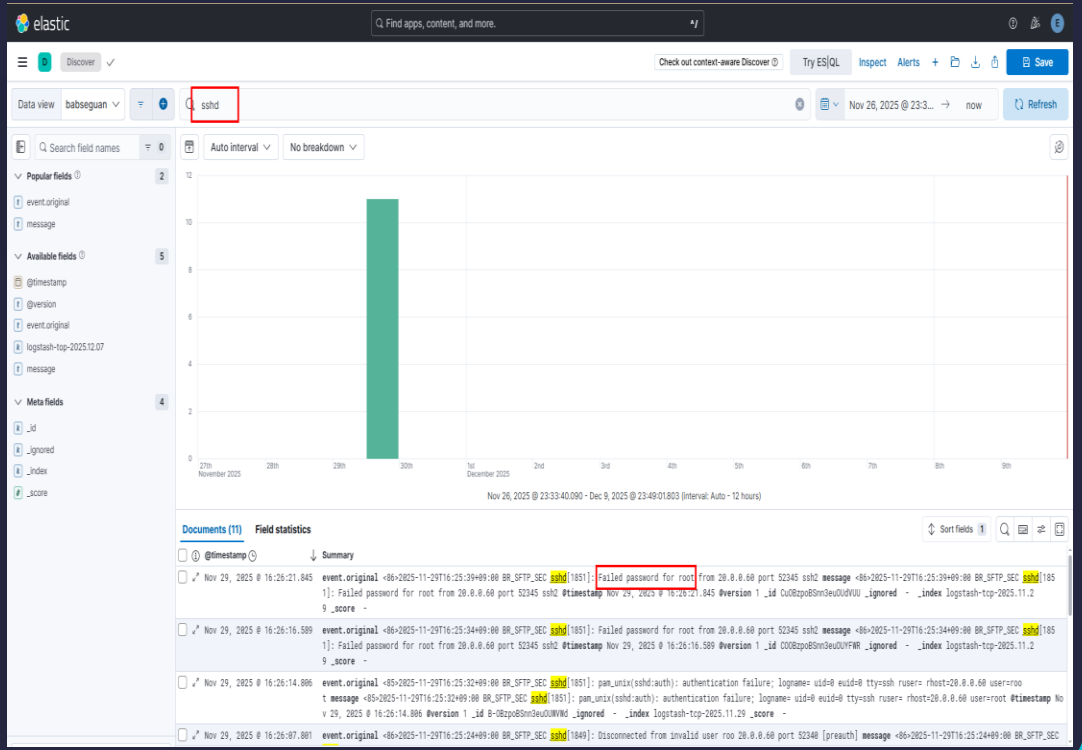
Log(모니터링)

- Kibana Discover 화면을 이용한 실시간 로그 시각화
- 필터링을 통한 상세 검색 (원격 로그인 실패)



Log(모니터링)

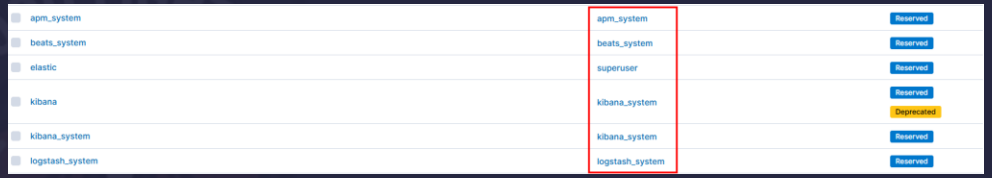
- Kibana Discover 화면을 이용한 실시간 로그 시각화
- 필터링을 통한 상세 검색 (원격 로그인 실패)



Log 서버 보안 조치

- 위 · 변조 방지 기능 적용
- 익명 접속 미설정 확인
- superuser와 시스템 계정 외에 사용자 존재하는지 확인
- 통신 시 암호화 설정 확인

```
[root@BR_LOG_SEC ~]# cat /etc/kibana/kibana.yml | grep xpack.security.authc.anonymous enabled
[root@BR_LOG_SEC ~]#
```

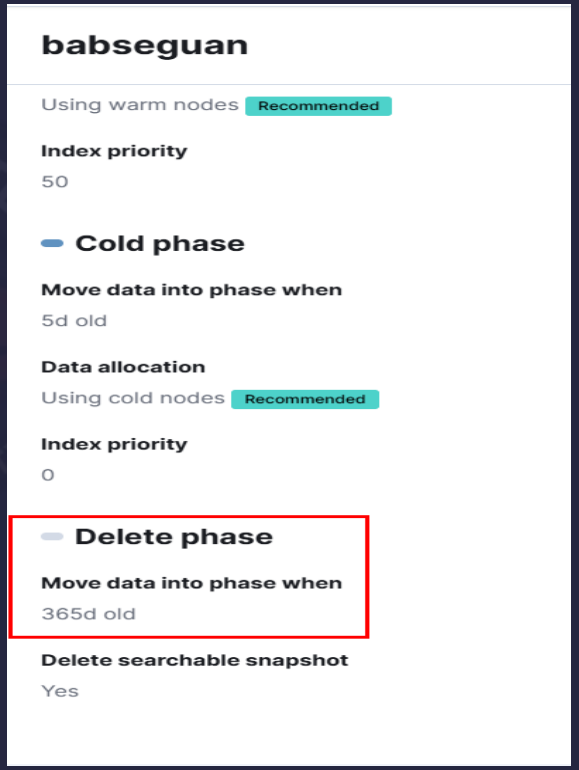



```
output.logstash:
  # The Logstash hosts
  hosts: ["20.0.0.65:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  ssl.certificate_authorities: ["/etc/logstash/certs/ca.crt"]
```

```
input {
    beats {
        port => 5044
        codec => "plain"
        host => "0.0.0.0"
        ssl_enabled => true
        ssl_certificate => "/etc/logstash/certs/logstash.crt"
        ssl_key => "/etc/logstash/certs/logstash.key"
    }
}
```

Log 서버 보안 조치

- 1년 이상 보관 확인
- 키바나 에서 정책으로 정확하게 수립되어 있는지 확인



Trouble Shooting

로그 서버 초기 세팅 시 과부하 문제

- 초기 대량 로그 유입 시 Elasticsearch가 과부하로 인해 status 137로 강제 종료됨
- 환경에 맞춰 Elasticsearch 힙 사이즈를 기본 1GB 이상에서 768MB로 **하향 조정**, 파일의 유입 **속도 제한**을 통해 안정화

```
[root@BR_LOG_SEC ~]# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: failed (Result: exit-code) since Sun 2025-12-07 13:44:51 KST; 2h 13min ago
     Docs: https://www.elastic.co
  Process: 969 ExecStart=/usr/share/elasticsearch/bin/systemd-entrypoint -p ${PID_DIR}/elasticsearch.pid --quiet (code=exited, status=137)
 Main PID: 969 (code=exited, status=137)

12월 07 12:39:35 BR_LOG_SEC systemd[1]: Starting Elasticsearch...
12월 07 12:41:22 BR_LOG_SEC systemd[1]: Started Elasticsearch.
12월 07 13:44:51 BR_LOG_SEC systemd-entrypoint[969]: ERROR: Elasticsearch exited unexpectedly, with exit code 137
12월 07 13:44:51 BR_LOG_SEC systemd[1]: elasticsearch.service: Main process exited, code=exited, status=137/n/a
12월 07 13:44:51 BR_LOG_SEC systemd[1]: elasticsearch.service: Failed with result 'exit-code'.
```

```
################################################################
## IMPORTANT: JVM heap size
################################################################
##
## The heap size is automatically configured by Elasticsearch
## based on the available memory in your system and the roles
## each node is configured to fulfill. If specifying heap is
## required, it should be done through a file in jvm.options.d,
## which should be named with .options suffix, and the min and
## max should be set to the same value. For example, to set the
## heap to 4 GB, create a new
## directory containing these
##
##

-Xms768m
-Xmx768m
```

```
# ------------------------ Output Queue -----------------------

queue.mem:
  events: 2048
```

느낀점

- 이번 과업을 통해 PL 역할을 수행하며 **PM과 팀원들 사이에서 의견을 조율하고 문제를 해결하는 데 집중**했다.
- 지속적인 소통을 통해 서로의 관점을 이해할 수 있었고, 이러한 과정이 구축 단계에서 **통일된 방향성을 유지**하는 데 큰 도움이 되었다.
- 또한 트러블슈팅 과정에서는 과부하 문제 해결을 위해 메모리 증설을 고려했으나 추가 비용이 발생할 수 있어, **비용 효율성을 우선으로 두고 기존 인프라 내에서 대안을 찾고자 노력**했다.
- 이를 통해 운영성과 효율성 사이의 균형을 판단하는 경험을 쌓을 수 있었고, **실무적인 문제 해결 역량도 향상**될 수 있었다.

Q&A

감사합니다