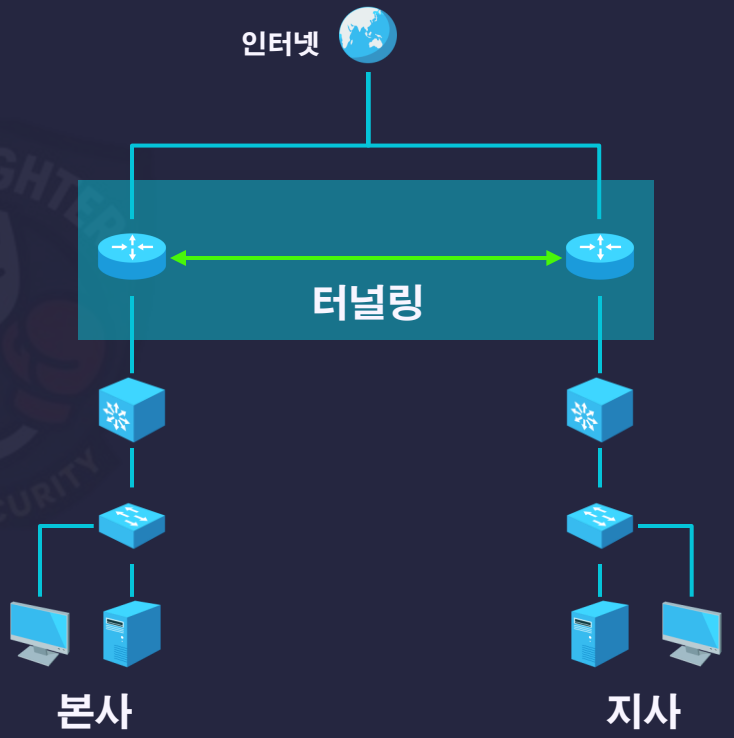
네트워크 엔지니어
강버들 포트폴리오

정보 보호 컨설팅 기반 네트워크 웹 보안 사업
- 네트워크 구축 -

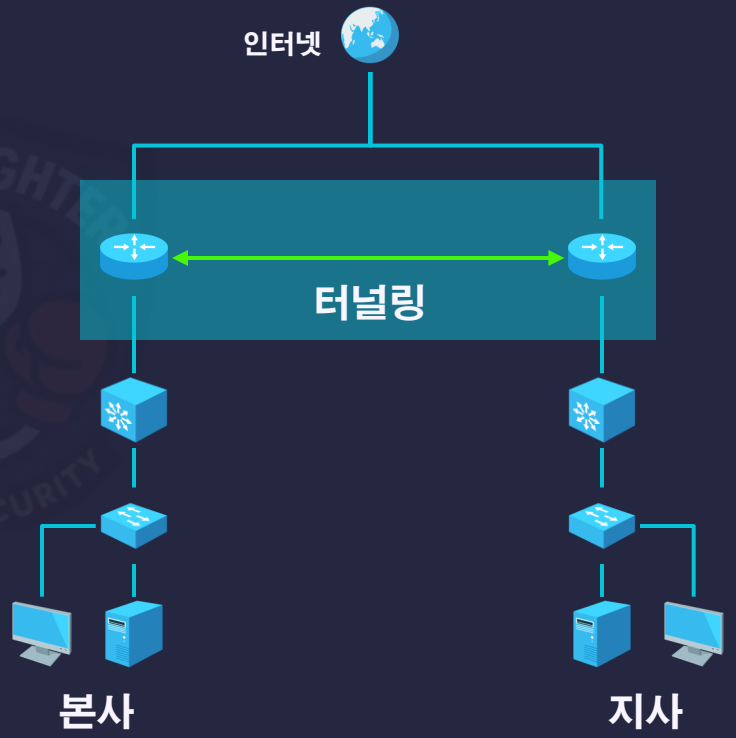
역할

- GRE over IPsec 적용
- OSPF 라우팅
- 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

IPsec 암호화 구조 – Phase 1 ~ 2

- IPsec을 통해 데이터 기밀성 · 무결성 · 인증 확보
- Phase 1: 보안 채널 수립
- Phase 2: 실제 데이터 암호화
- GRE는 내부망을 운반, IPsec은 운반된 트래픽을 보호

ISAKMP Policy (Phase 1)

```
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key sun address 2.2.2.2
!
```

IPsec 암호화 구조 – Phase 1 ~ 2

- IPsec을 통해 데이터 기밀성 · 무결성 · 인증 확보
- Phase 1: 보안 채널 수립
- Phase 2: 실제 데이터 암호화
- GRE는 내부망을 운반, IPsec은 운반된 트래픽을 보호

IPsec Transform-set (Phase 2)

```
!
crypto ipsec transform-set test
!
```

```
esp-3des esp-sha-hmac
```

IPsec 암호화 구조 – Phase 1 ~ 2

- IPsec을 통해 데이터 기밀성 · 무결성 · 인증 확보
- Phase 1: 보안 채널 수립
- Phase 2: 실제 데이터 암호화
- GRE는 내부망을 운반, IPsec은 운반된 트래픽을 보호

Crypto Map

```
!
crypto map sun 10 ipsec-isakmp
 set peer 2.2.2.2
 set transform-set test
 match address VPN_ACL
!
```

MTU / MSS 조정

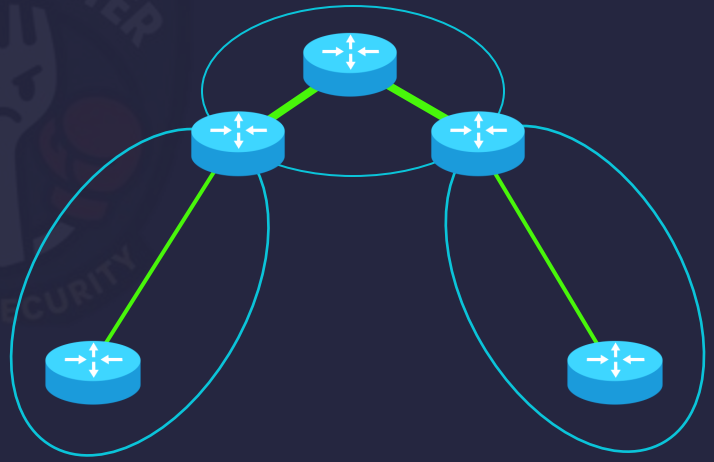
- GRE + Ipsec 오버헤드 고려
  MTU/MSS 값 조정

```
!
interface Tunnel0
 ip address 50.50.50.10 255.255.255.252
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source FastEthernet0/0
 tunnel destination 2.2.2.2
!
```

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 적용으로 라우터 간 경로 정보 자동 교환 · 동기화
- GRE 터널 인터페이스 상에서 Neighbor 관계 정상 성립

```
HQ_UTM#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.0           0   FULL/  -        00:00:39    50.50.50.9      Tunnel0
1.1.1.2           1   FULL/DR         00:00:36    10.0.1.14       FastEthernet2/0
1.1.1.1           1   FULL/DR         00:00:38    10.0.1.10       FastEthernet1/0
HQ_UTM#
```

OSPF Neighbor 형성

- 본사 · 지사 모두 OSPF 기반 동적 라우팅 구성
- OSPF 적용으로 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

- 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

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
!
```

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

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.

결과물

- 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.

푸드파이터 팀 공통
프로젝트 개요

정보 보호 컨설팅 기반 네트워크 웹 보안 사업

목차

1. 팀원 소개

2. 프로젝트 배경
   - 추진 배경
   - 사업 목표

3. 분석 및 점검
   - 기존 인프라 문제점
   - 개선된 인프라 내용

01

팀원 소개

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

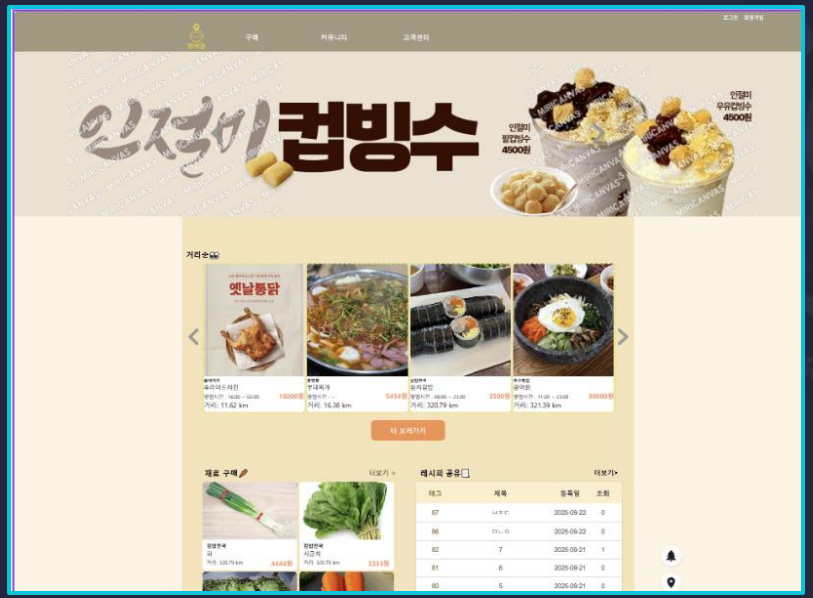
이서진 / 수행원

윈도우 서버 구축,
MariaDB 구축, 모의해킹

02

프로젝트 배경

고객사 설명 (본사)

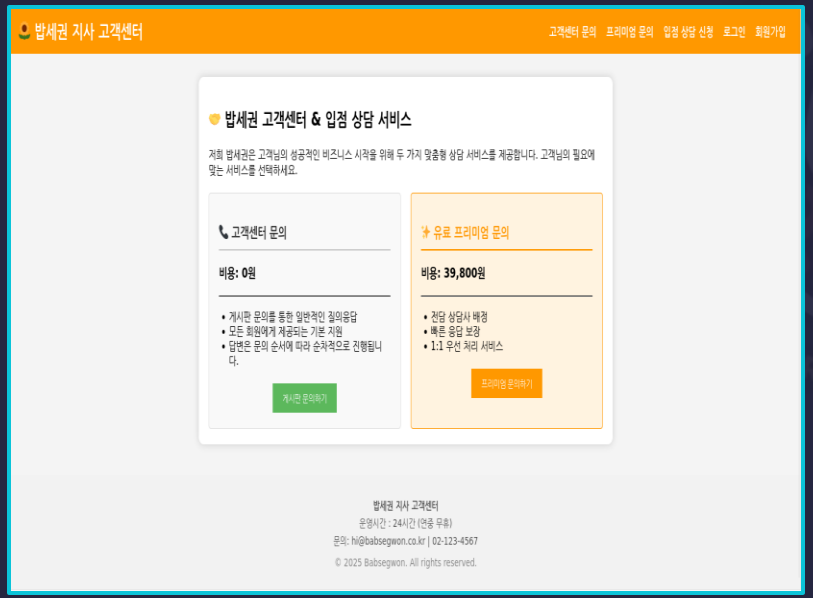


판매자 잉여 재고 판매 저렴한 가격에 구매 가능

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

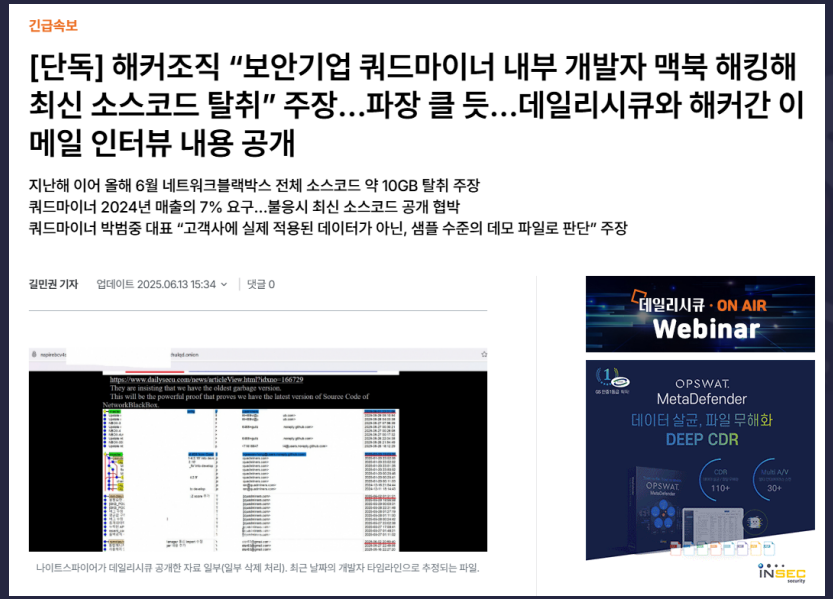
Bjorka • Sat Oct 04 2025 • #Indonesia

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 해킹했다고 밝혔다.

이에 대해 나이트스파이어는
“이번에는 작년처럼 끝내지 않겠다”
며 보복성 공격임을 간접적으로 시사했다.

시나리오 요약

Namhyux Tovalds

고객의 분노 표출

시나리오 요약

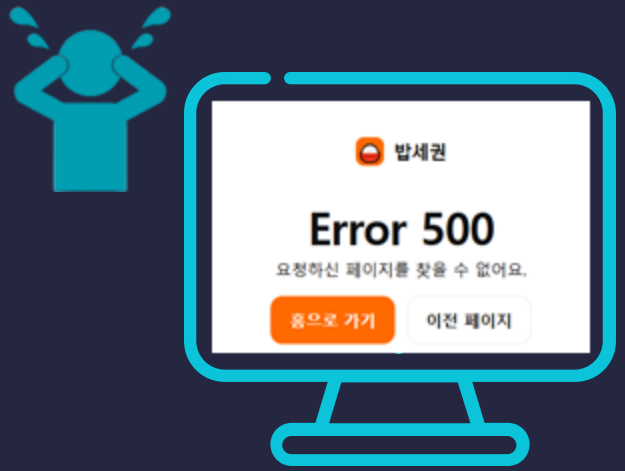
모든 네트워크
보안 설정 비활성화

밥세권 보안팀의
미흡한 초기 대응

DB

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

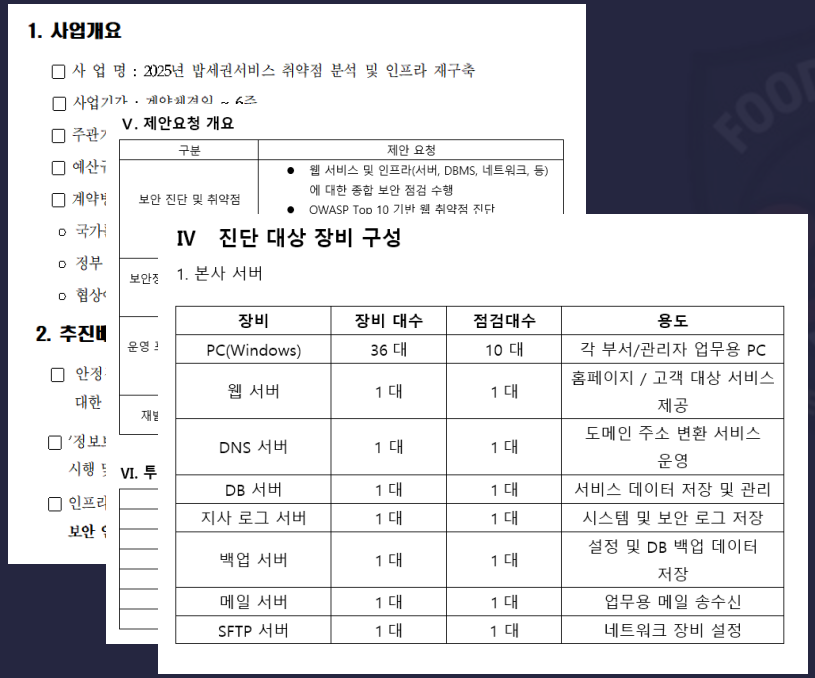
Cisco Router : Cisco 3660 Series 12.4(15)T9
Cisco L3 SW : Cisco 3745 Router 12.4(11)T

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

○ 국가

○ 정부

○ 협상

2. 추진배

☐ 안정

대한

☐ 정보

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

03

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

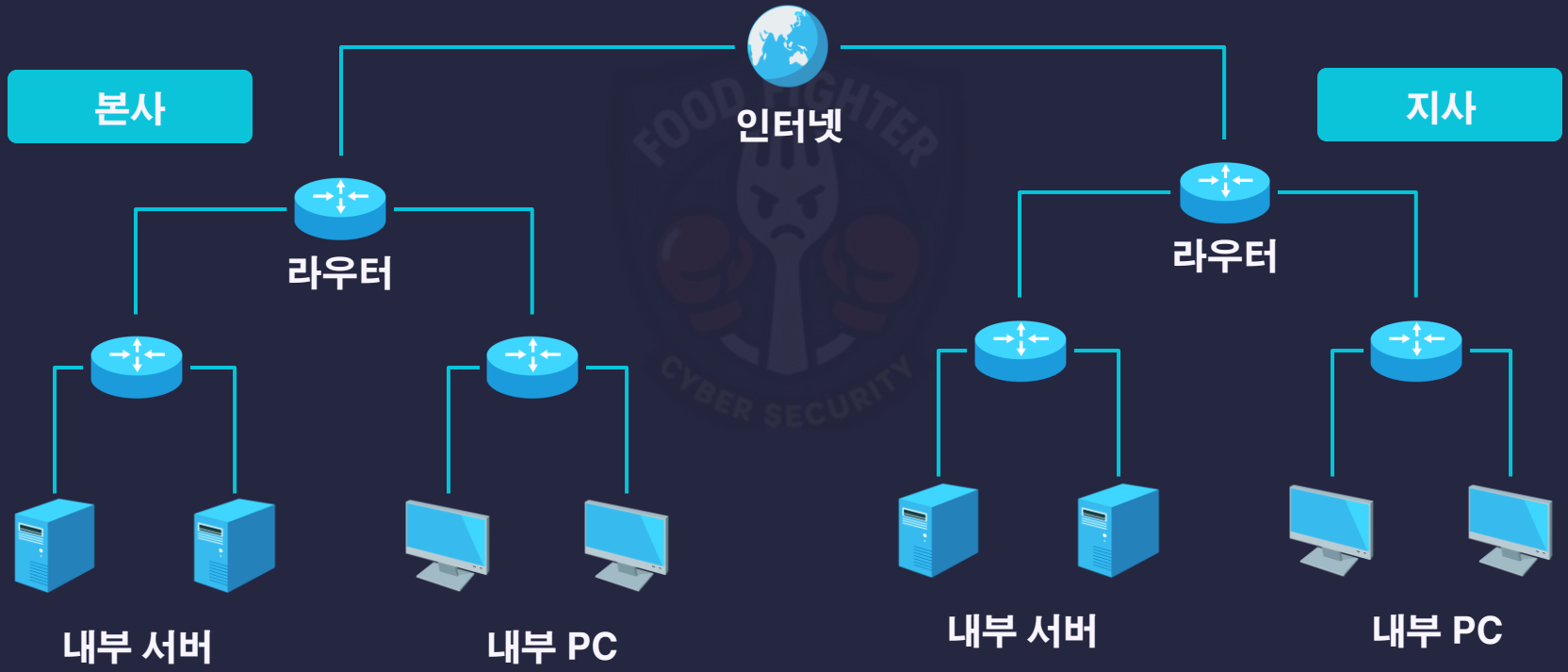
L3 스위치 8대 / 8대

UTM 2대 / 2대

점검 44 대 / 총 104 대

인프라 구성

기존 인프라



기존 인프라 문제점

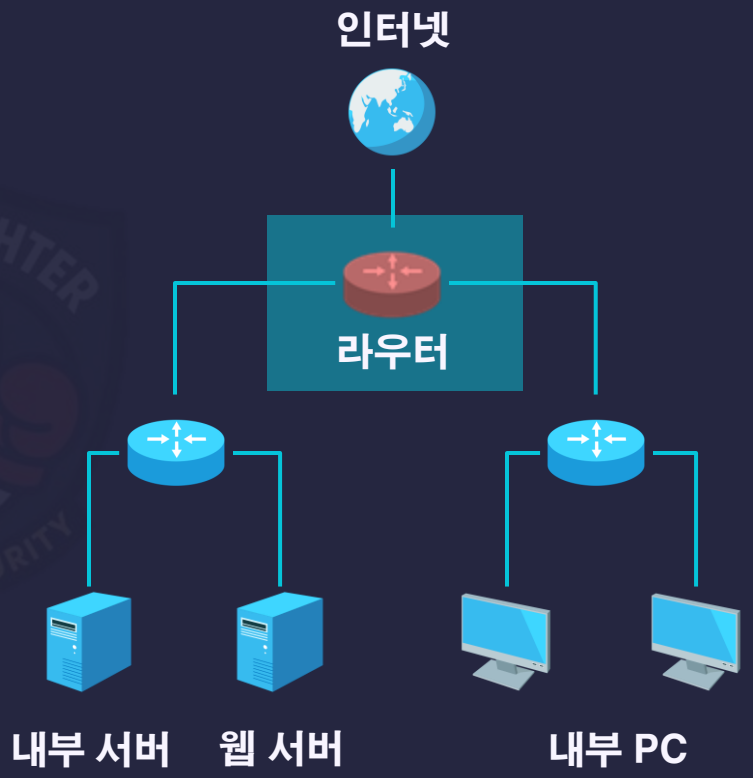
● 장비 이중화 미비
단일 장비 장애 시 전체 서비스 마비

● 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

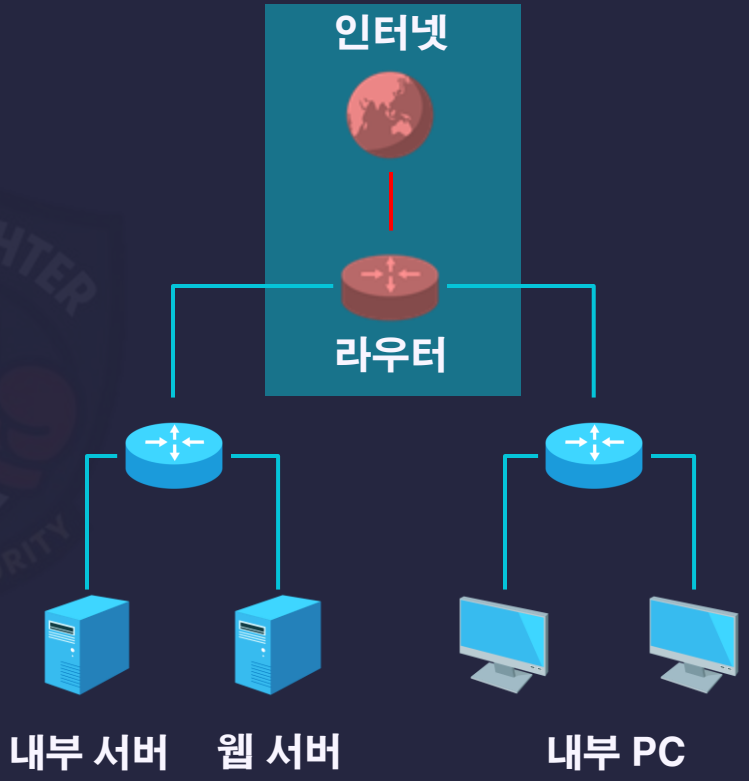
- **장비 이중화 미비**
  단일 장비 장애 시 전체 서비스 마비

- **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

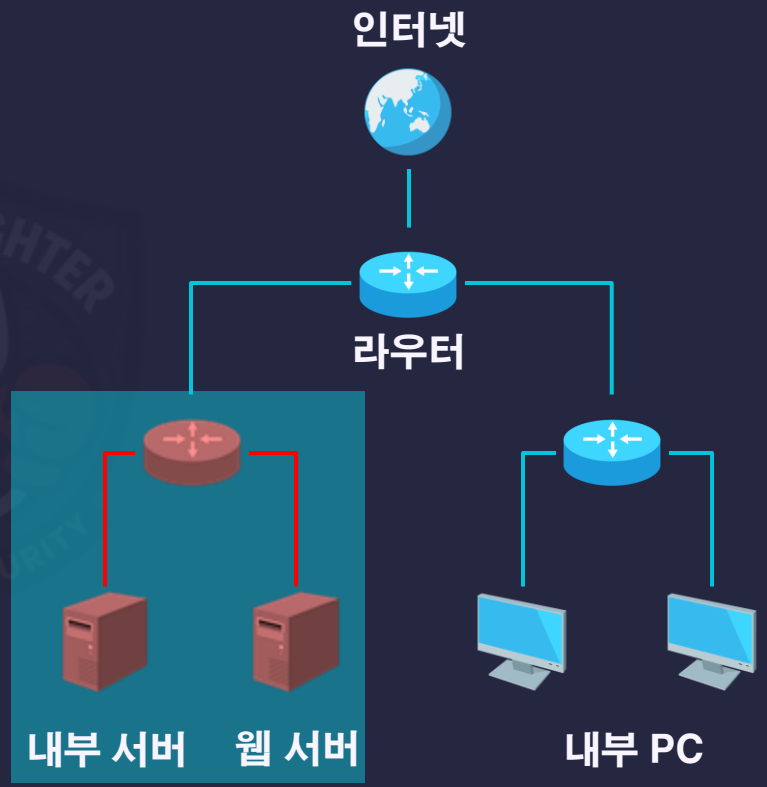
- **장비 이중화 미비**
  단일 장비 장애 시 전체 서비스 마비

- **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

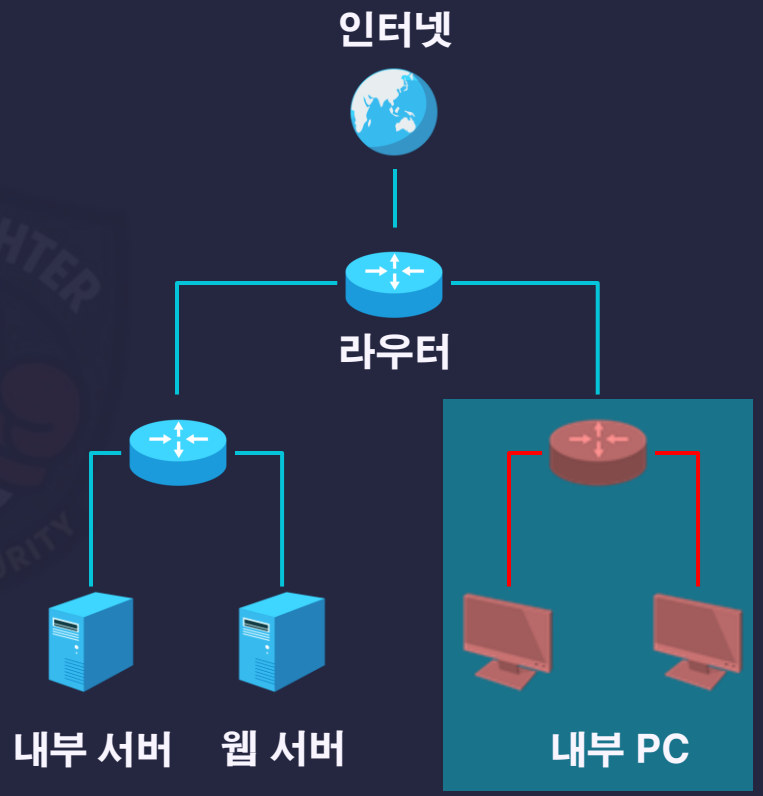
● 장비 이중화 미비
단일 장비 장애 시 전체 서비스 마비

● 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

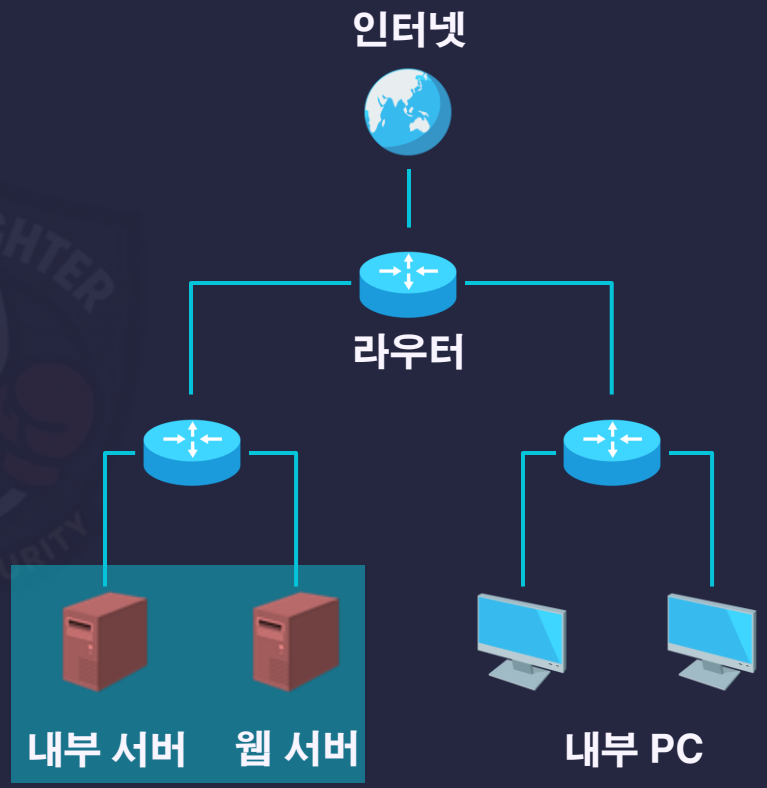
- **장비 이중화 미비**
  단일 장비 장애 시 전체 서비스 마비

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

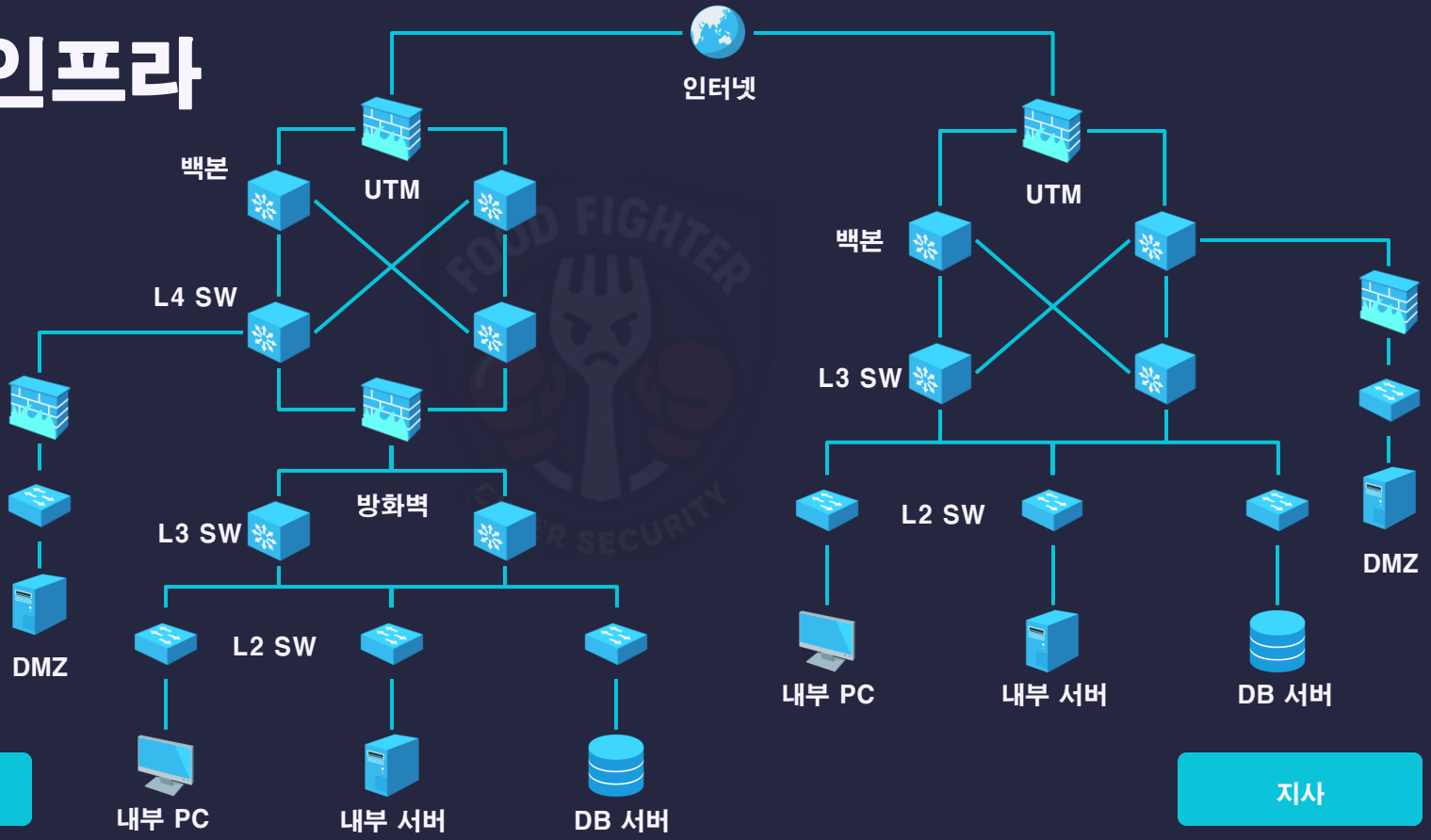
- **DMZ 내부망 구분 없음**
  내부망 직접 노출 및 침투 용이

- **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

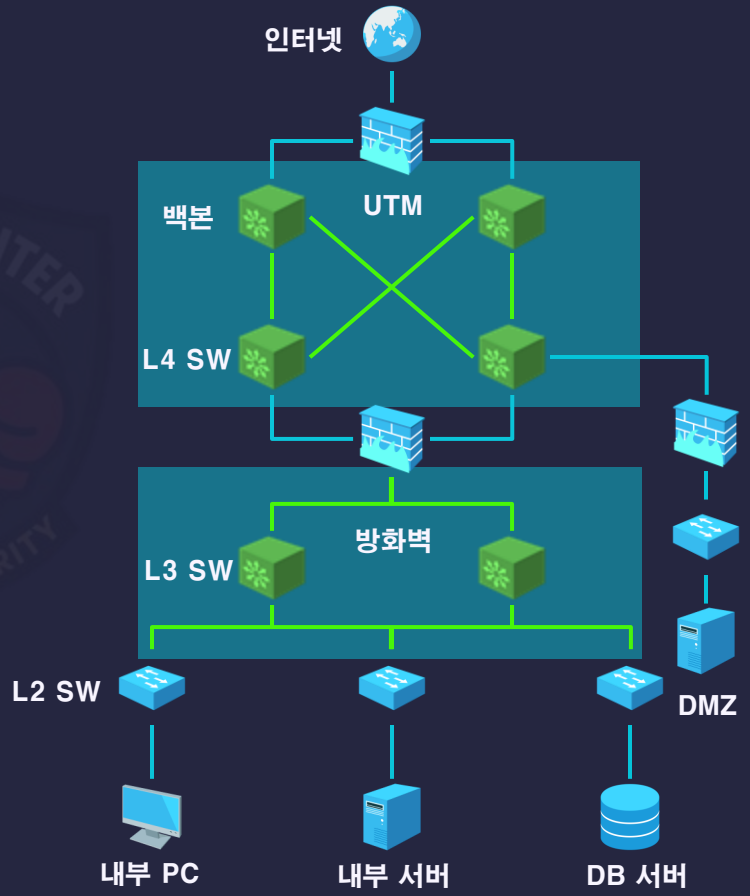
개선된 인프라

● **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



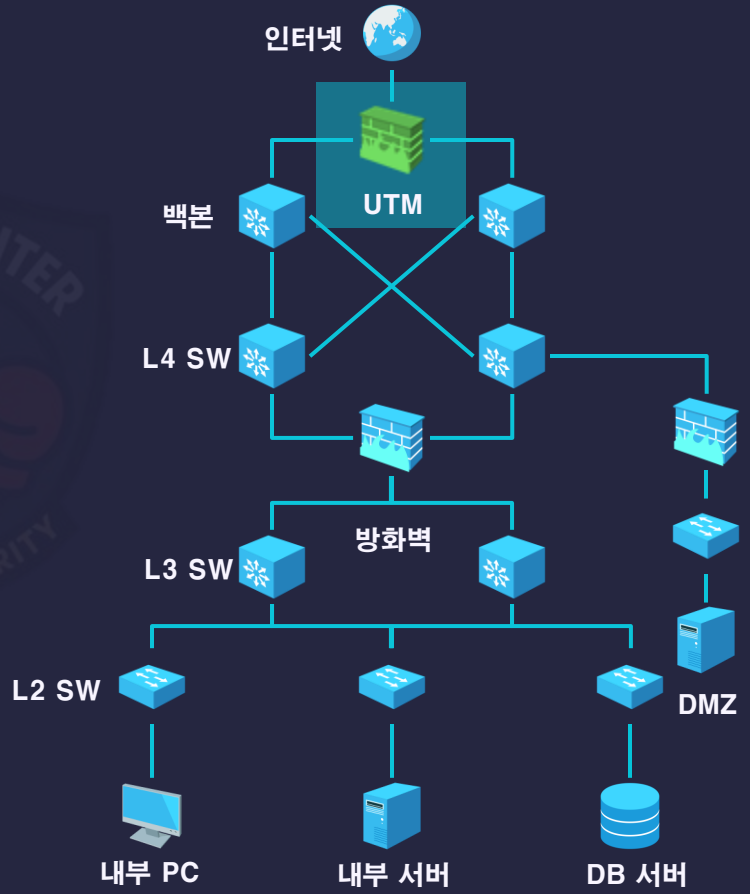
개선된 인프라

● 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



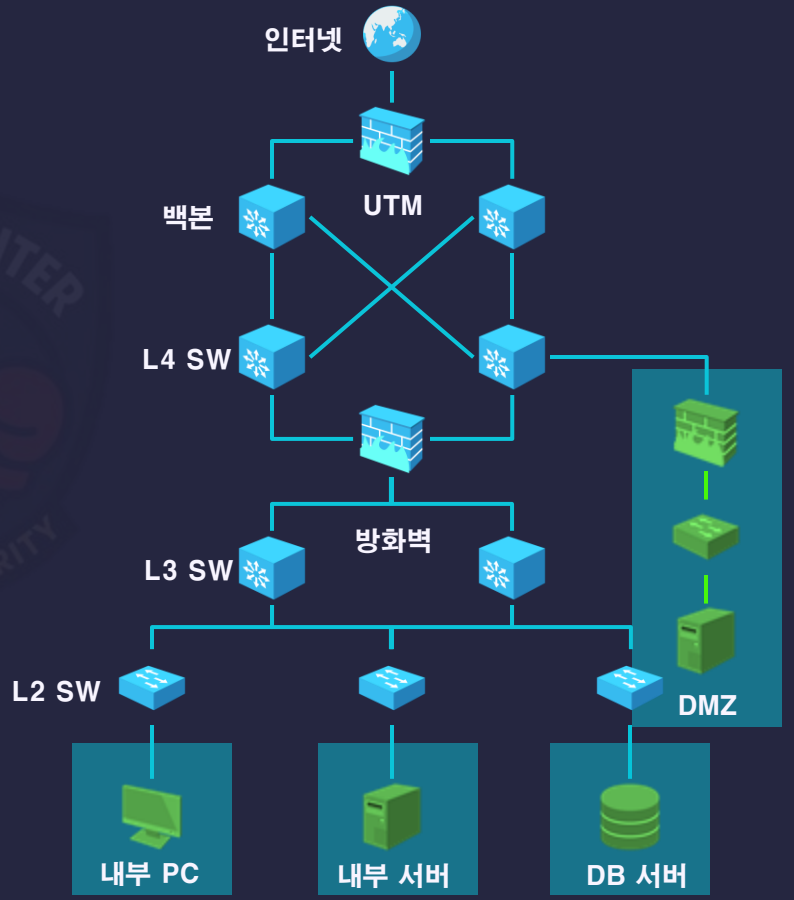
개선된 인프라

● 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



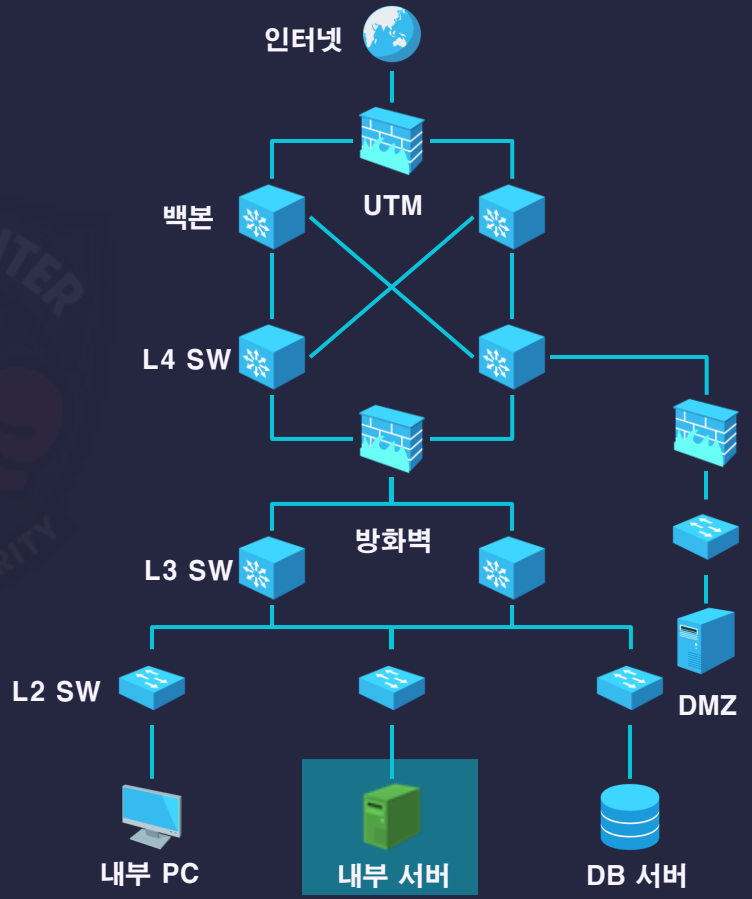
개선된 인프라

● **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

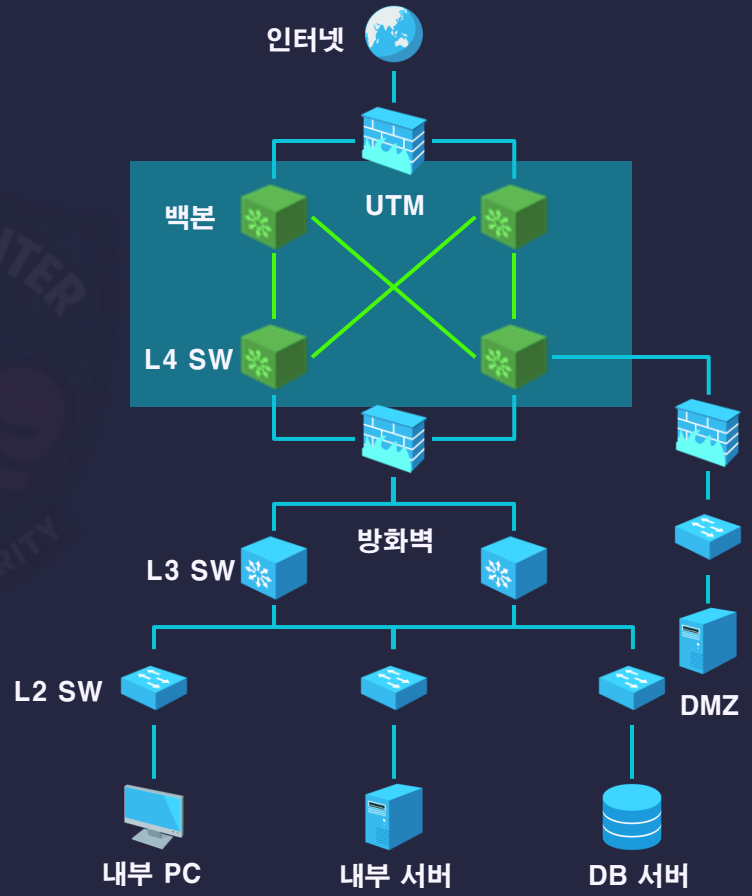
● **로그 및 파일 백업 서버 구성**
파일 손실시 대응 체계 마련



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