

침해사고 대응 기반 인프라 및 정보보호 체계 강화 사업

Security Report.

틈새 걸음

전보라

황승우

백정이

Table Of Contents >

01 프로젝트 배경

- 추진 배경
- 고객사 설명
- 시나리오
- 사업 목표
- 사용 툴
- 프로젝트 기간
- 수행 인력

02 분석 및 점검

- 점검 기준
- 점검 항목
- 자산 목록
- 점검 범위
- 기존 고객사 인프라
- 개선된 인프라

03 개인 발표

- 담당 업무
- 취약점
- 시나리오
- 보안 점검
- 트러블 슈팅
- 프로젝트 후 느낀 점

04 Q & A

01

프로젝트 배경

IT · 과학 / IT일반

KT도 'BPF도어'에 당했다…통신사 전반 확산 우려

 김민수 기자

업데이트 2025.11.09 오전 10:23 ▾

리눅스 서버 노린 백도어 악성코드…BPF 기능 악용해 탐지 회피
보안 장비 우회·은폐 가능한 고도화된 침투 방식



IT·과학

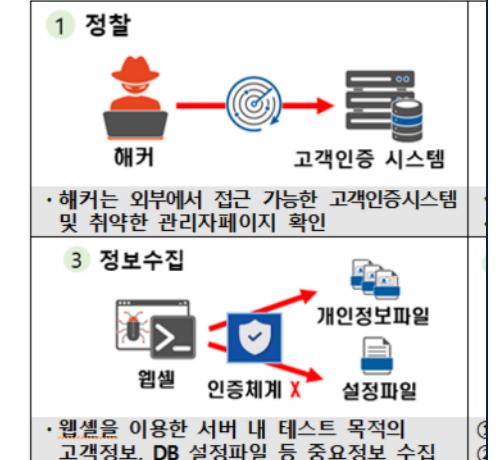
정부, LG유플 해킹피해 29만명 결론…“인증DB 보안 취약”

우수민 기자 rsvp@mk.co.kr

입력 : 2023-04-27 11:30:35 수정 : 2023-04-27 18:19:06

실시간 탐지체계 구축 요구키로

< 고객인증 시스템을 통한



2025년 피싱범죄 피해액 8000억 '역대 최고'

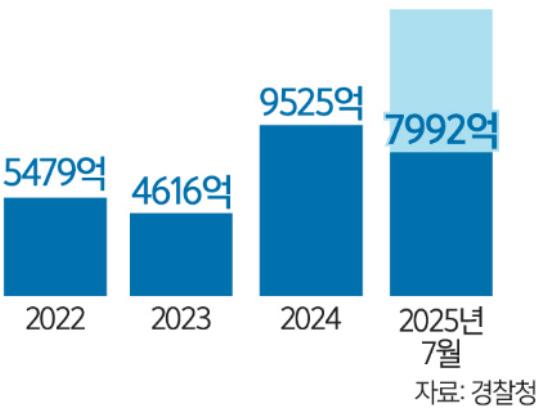
입력 : 2025-08-31 18:59:33 | 수정 : 2025-08-31 21:15:50

김승환 기자 hwan@segye.com

2024년 피해액 육박…연말 1조 넘을듯
경찰, 1일부터 5개월간 특별 단속

올해 보이스피싱 등 피싱범죄 피해액이 7월 기준으로 약 이미 8000억원에 달하며 역대 최고치를 찍은 것으로 나타났다. 올해 말에는 사상 처음으로 1조원을 돌파할 수도 있다는 전망까지 나온다. 지난해부터 이어진 피싱범죄 증가세가 수그러들 기미를 보이지 않자 경찰은 9월1일부터 피싱범죄에 대한 대대적인 특별단속에 착수하기로 했다.

연간 피싱 범죄 피해액 추이 (단위: 원)



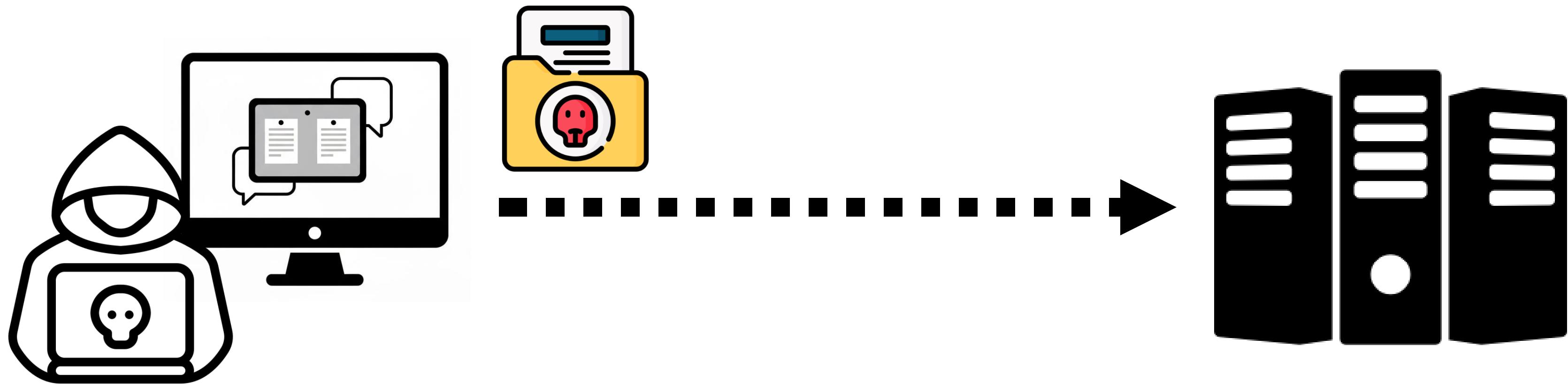
백도어 악성코드 피해, 통신사 전반 확산 우려

29만명 규모의 고객 정보 해킹 피해 발생

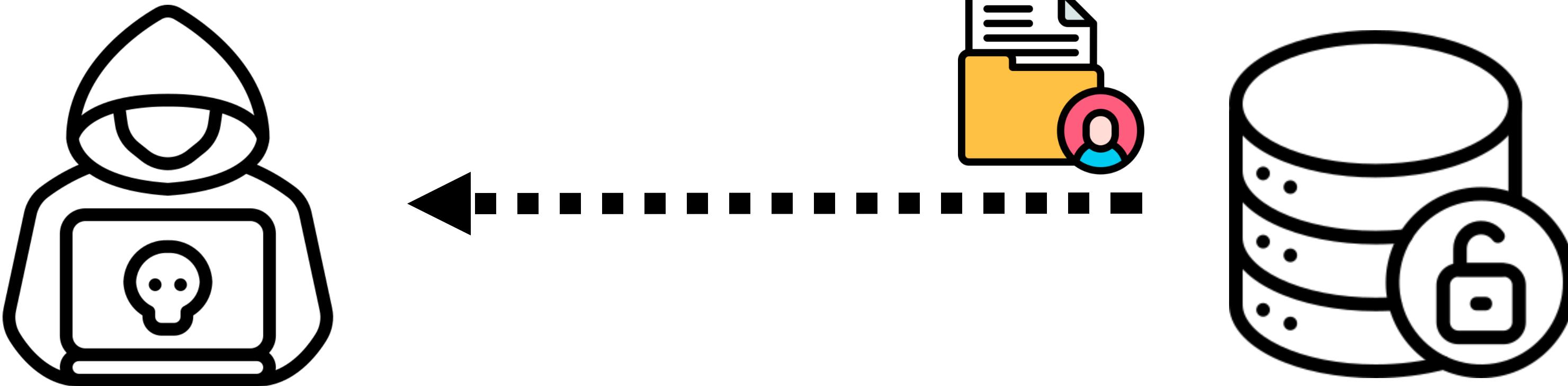
2025년 피싱 범죄 피해액 8000억 '역대 최고'

함께 빛 함께 살아가는 따스한 세상의 빛

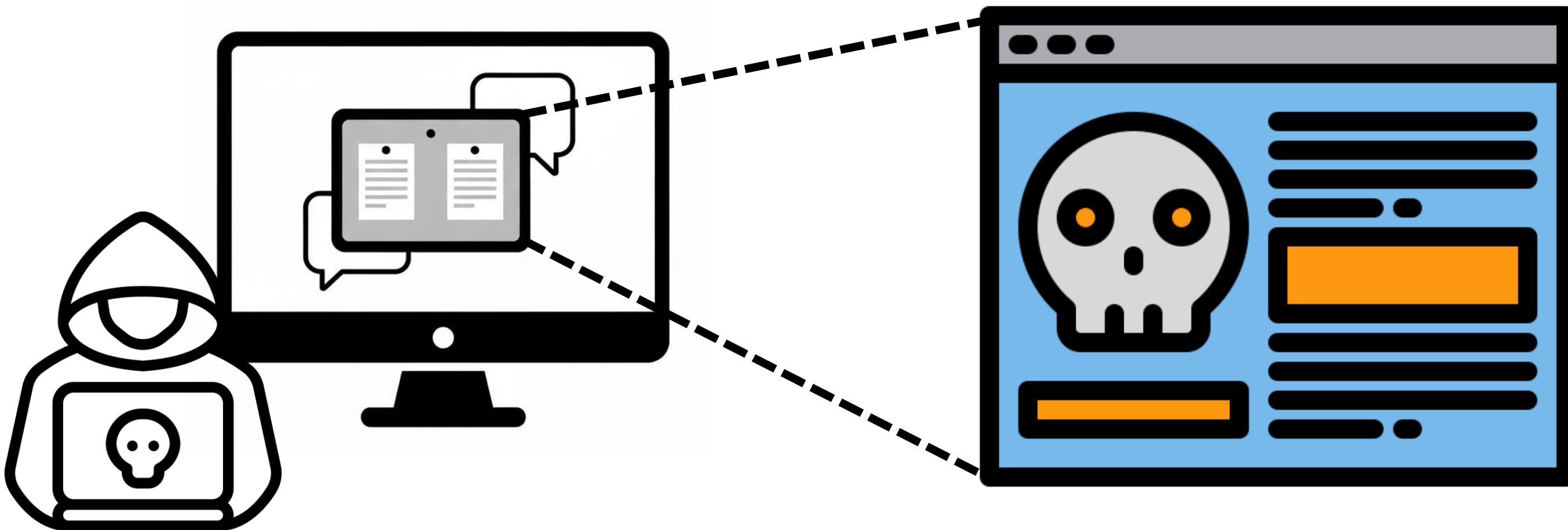
거동 불편자를 위한 "함께 걸음"과 청년들을 위한 "틈새 빛"이 힘을 합쳐 함께하는 세상의 따스한 빛이 되고자 합니다.



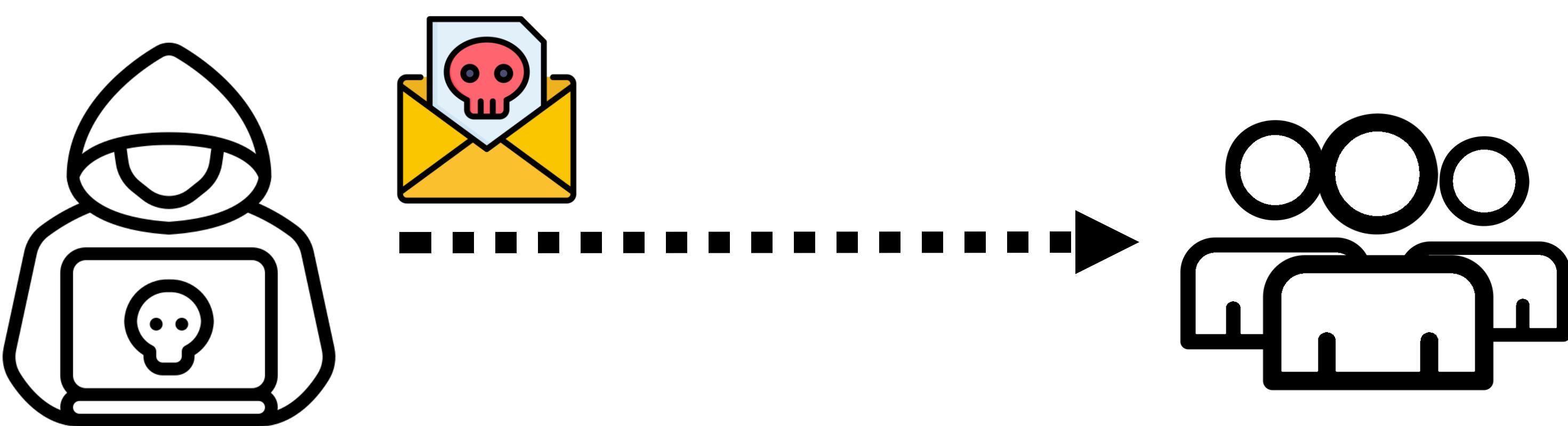
공격자가 파일 업로드 취약점을 통해 내부 서버에 백도어 프로그램 업로드



백도어 프로그램을 통해 DB 서버에서 약 1,000여 명의 개인정보 탈취



관리자 계정을 탈취하여 배너를 변경하여 가짜 공지 사항 등록



탈취한 고객 정보를 통해 메일 송부 후, 피싱 사이트를 통해 결제 유도

취약 사항

- 본사와 지사 간의 사설 통신망 부재
- 중요 내부 서버와 외부 망 분리 부재
- 보안 장비 부재
- 서버 및 장비 보안 설정 미흡
- 네트워크 장비 이중화 부재
- 백업, 로그 서버 부재



개선 사항

- VPN을 통한 사설 통신망 구축 및 보안 강화
- DMZ 및 내부 망을 구축하여 외부 망과 분리
- 보안 장비(WAF, UTM, 방화벽) 도입
- 서버 및 장비 별 보안 설정
- 백본(L3), L4 스위치 이중화
- 백업, 로그 서버 구축

사용 도구



Packet Tracer
8.2.2.400



GNS3
1.5.3.0



VMWare
17.6.2



PuTTY
putty
0.83.0.0



Metasploit
6.4.34-dev



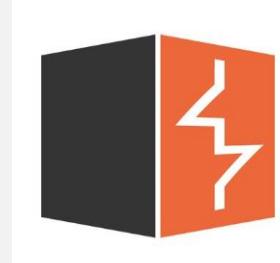
Wireshark
4.4.9



nmap
7.94 SVN



Hydra
v9.5



Burp Suite
v2024.9.4

협업 도구



Discord



Google
Drive



Notion



Kali
2024.4



Rocky
8.10



modsecurity
2.9.6



php
7.2.24



Windows
Server 2016



Sophos
9.723

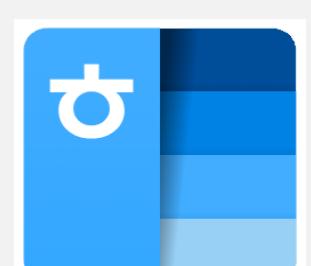


MariaDB
3.1.11



Windows
10

문서화 도구



총 수행 기간 : 25/11/03 – 25/12/12 (총 30일)

	Task	Star	End	1w	2w	3w	4w	5w	6w
프로젝트 관리	제안서 작성	11/03	11/04	2d					
	일정 수립	11/05	11/05		1d				
	킥 오프 미팅	11/05	11/05		1d				
취약점 분석 및 평가	취약점 점검 대상 식별 및 분류	11/06	11/07		2d				
	취약점 본 점검 수행	11/10	11/12			3d			
	취약점 위험 분석/평가 수행	11/12	11/13			2d			
보안대책 수립 및 조치 지원	취약점 개선 방안 도출	11/13	11/14			2d			
	인프라 구성 및 시스템 구축(보안설정)	11/17	11/19				3d		
	인프라 취약점 이행점검 수행	11/20	11/24				3d		
모의해킹	모의해킹	11/21	11/24				2d		
	모의해킹 보안설정	11/25	11/28					4d	
	모의해킹 이행점검 수행	12/01	12/03					3d	
문서화 및 보고	문서화 작업	12/04	12/08					3d	
	최종 보고	12/09	12/12						4d

수행 인력



전보라 (PM)

총괄
PC 점검, 보안 설정
모의해킹 수행, 보안 설정
리눅스 서버 점검, 보안 설정



황승우 (PL)

본사 네트워크 점검, 보안 설정
모의해킹 수행
보안장비 점검, 보안 설정
리눅스 서버 점검, 보안 설정



백정이

지사 네트워크 점검, 보안 설정
DBMS 서버 점검, 보안 설정
모의해킹 수행
리눅스 서버 점검, 보안 설정

02

분석 및 점검



> 취약점 점검 기준 문서

한국 인터넷 진흥원(KISA)에서 발행한
주요정보통신기반시설
기술적 취약점 분석·평가 방법
상세 가이드
+
금융보안원에서 발행한
전자금융기반시설 보안 취약점 평가기준 안내서

 Linux 서버

분류	점검 항목	항목 중요도	항목 코드
계정 관리	패스워드 복잡성 설정	상	U-02
	계정 잠금 임계 값 설정	상	U-03
파일 및 디렉터리 관리	/etc/hosts 파일 소유자 및 권한 설정	상	U-09
	SUID, SGID, Sticky bit 설정 파일 점검	상	U-13
	/dev에 존재하지 않는 device 파일 점검	상	U-16
서비스 관리	cron 파일 소유자 및 권한 설정	상	U-22
	웹서비스 웹 프로세스 권한 제한	상	U-36
	웹서비스 상위 디렉토리 접근 금지	상	U-37
	웹서비스 파일 업로드 및 다운로드 제한	상	U-40
로그 관리	로그의 정기적 검토 및 보고	상	U-43

 Windows 서버

분류	점검 항목	항목 중요도	항목 코드
계정 관리	Administrator 계정 이름 변경 또는 보안성 강화	상	W-01
	Guest 계정 비활성화	상	W-02
서비스 관리	공유 권한 및 사용자 그룹 설정	상	W-07
	하드디스크 기본 공유 제거	상	W-08
로그 관리	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검	중	W-68
	원격으로 액세스 할 수 있는 레지스트리 경로	상	W-35
보안 관리	보안감사를 로그할 수 없는 경우 즉시 시스템 종료 해제	상	W-41
	Autologon 기능 제어	상	W-43
	디스크 볼륨 암호화 설정	상	W-45
	시작 프로그램 목록 분석	중	W-81

 DBMS

분류	점검 항목	항목 중요도	항목 코드
계정 관리	데이터베이스의 불필요 계정을 제거하거나, 잠금설정 후 사용	상	D-02
	패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정	상	D-03
	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용	상	D-04
	DB 사용자 계정을 개별적으로 부여하여 사용	중	D-13
접근 관리	원격에서 DB 서버로의 접속 제한	상	D-05
	DBA 이외의 인가되지 않은 사용자 시스템 테이블에 접근할 수 없도록 설정	상	D-06
패치 관리	데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용	상	D-10
	데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정	상	D-11
접근 관리	일정 횟수의 로그인 실패 시 이에 대한 잠금정책이 설정	상	D-15
	데이터베이스의 주요 설정파일, 패스워드 파일 등과 같은 주요 파일들의 접근 권한이 적절하게 설정	상	D-17

 네트워크

분류	점검 항목	항목 중요도	항목 코드
계정 관리	패스워드 복잡성 설정	상	N-02
	암호화된 패스워드 사용	상	N-03
	사용자·명령어별 권한 수준 설정	중	N-15
접근 관리	Session Timeout 설정	상	N-05
	VTY 접속 시 안전한 프로토콜 사용	중	N-16
	불필요한 보조 입·출력 포트 사용 금지	중	N-17
기능 관리	사용하지 않는 인터페이스의 Shutdown 설정	상	N-14
	Proxy ARP 차단	중	N-32
패치 관리	ICMP unreachable, Redirect 차단	중	N-33
	최신 보안 패치 및 벤더 권고사항 적용	상	N-06

 보안장비

분류	점검 항목	항목 중요도	항목 코드
계정 관리	보안장비 Default 계정 변경	상	S-01
	보안장비 Default 패스워드 변경	상	S-02
	보안장비 계정별 권한 설정	상	S-03
	로그인 실패횟수 제한	중	S-17
접근 관리	보안장비 원격 관리 접근 통제	상	S-05
	보안장비 보안 접속	상	S-06
	Session timeout 설정	상	S-07
기능 관리	DMZ 설정	상	S-11
	이상징후 탐지 모니터링 수행	상	S-13
	유해 트래픽 차단 정책 설정	중	S-25

 PC

분류	점검 항목	항목 중요도	항목 코드
계정 관리	패스워드의 주기적 변경	상	PC-01
	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상	PC-02
서비스 관리	공유 폴더 제거	상	PC-03
	항목의 불필요한 서비스 제거	상	PC-04
보안 관리	바이러스 백신 프로그램 설치 및 주기적 업데이트	상	PC-09
	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상	PC-10
	OS에서 제공하는 침입차단 기능 활성화	상	PC-11
	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상	PC-12
	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지등 이동식 미디어에 대한 보안대책 수립	상	PC-13
	PC 내부의 미사용(3개월) ActiveX 제거	상	PC-14

> Web

점검 항목	항목 중요도	항목 코드
운영체제 명령 실행	상	OC
SQL 인젝션	상	SI
정보 누출	상	IL
크로스사이트 스크립팅	상	XS
크로스사이트 리퀘스트 변조(CSRF)	상	CF
파일 업로드	상	FU
디렉터리 인덱싱	상	DI
관리자 페이지 노출	상	AE
데이터 평문 전송	상	SN
쿠키 변조	상	CC

> 본사 자산 목록(총 33/83식)

분류	장비	장비 대 수	점검 대 수	용도
리눅스 서버	PC	55	16	각 부서 별 직원 PC
	웹 서버	2	2	틈새 빛, 함께 걸음 웹 서비스 제공
	DNS 서버	1	1	DNS 서버
	DB 서버	1	1	데이터 베이스 저장 처리
	TFTP 서버	1	1	장비 정보 백업
	DB 백업 서버	1	1	DB 서버 백업 수행
	로그 서버	1	1	로그 저장
윈도우 서버	Mail 서버	1	1	메일 송수신(내부 사용자 용)
	DHCP 서버	1	1	본사 직원 PC IP 할당
네트워크 장비	L2 스위치	11	0	팀 별 PC 연결
	L3 스위치	2	2	백본 스위치
	L4 스위치	2	2	로드 밸런싱 가능
	라우터	1	1	GRE 설정
보안 장비	보안 장비	3	3	UTM, 방화벽, WAF

 지사 자산 목록(총 23/46식)

분류	장비	장비 대 수	점검 대 수	용도
리눅스 서버	PC	25	10	각 부서 별 직원 PC
	웹 서버	1	1	따뜻한 공동체 웹 서비스 제공
	DNS 서버	1	1	DNS 서버
	DB 서버	1	1	데이터 베이스 저장 처리
	TFTP 서버	1	1	장비 정보 백업
	DB 백업 서버	1	1	DB 서버 백업 수행
윈도우 서버	DHCP 서버	1	1	지사 직원 PC IP 할당
네트워크 장비	L2 스위치	8	0	팀 별 PC 연결
	L3 스위치	2	2	백본 스위치
	L4 스위치	2	2	로드 밸런싱 가능
	라우터	1	1	GRE 설정
보안 장비	보안 장비	2	2	UTM, 방화벽

> 지사 WEB 페이지(5/17 페이지)

The screenshot displays a series of five web pages illustrating the user flow:

- 1. 로그인**: The login screen features a header with "환영합니다, 손님!" and buttons for "회원가입" and "로그인".
- 2. 소모임 게시글 작성**: The "새 모임 만들기" (Create Event) screen. A sidebar on the left shows "사용" and "비밀" sections. Step 2 is highlighted on the sidebar.
- 3. 소모임 게시글 상세**: The event detail screen for "hello" (작성자: boradori). Step 3 is highlighted on the sidebar.
- 4. 후원**: The contribution page showing a total amount of 1,068,021원. Step 4 is highlighted on the sidebar.
- 5. 관리자페이지 (users 관리)**: The manager page for users, showing a list of users including ID 1 (관리자), ID 2 (boradori), ID 3 (boradori), and ID 4 (boradori). Step 5 is highlighted on the sidebar.

1 로그인

2 소모임 게시글 작성

3 소모임 게시글 상세

4 후원

5 관리자페이지

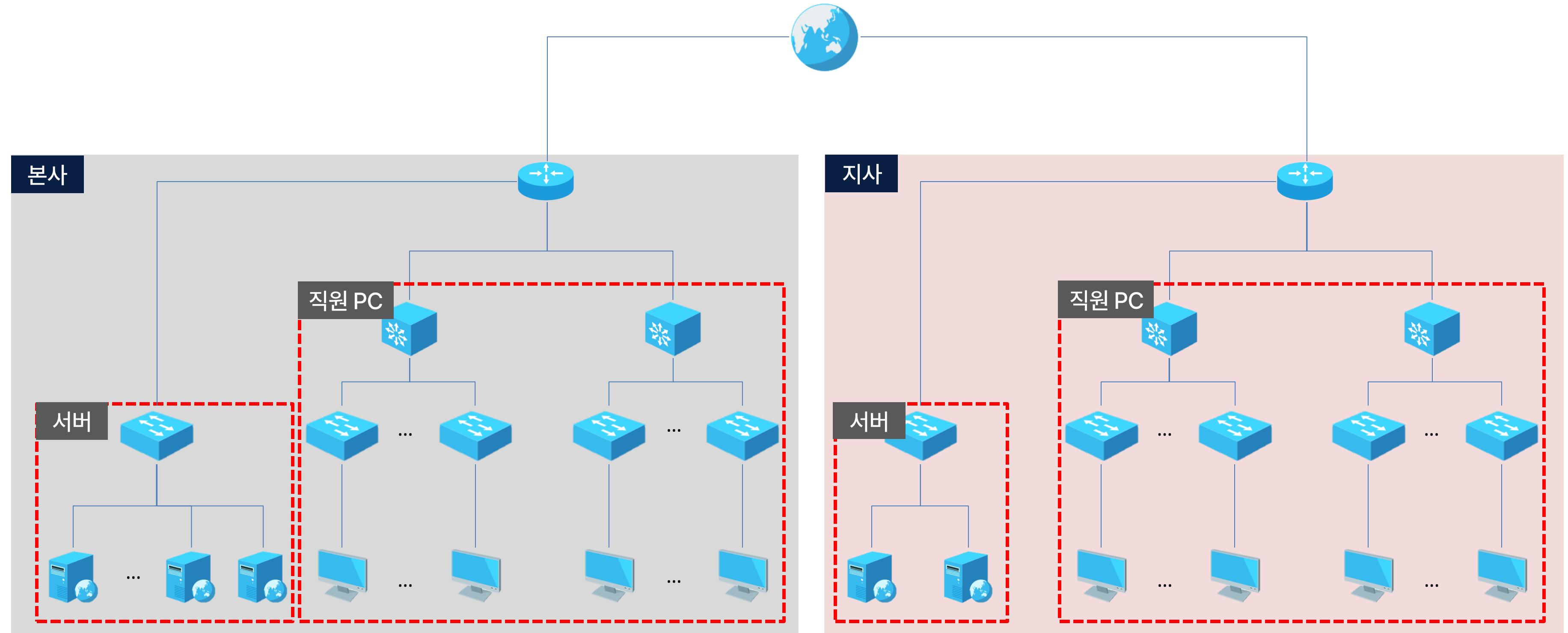
 점검 범위

구분	제안 요청
보안취약점 점검 (인프라, 웹페이지)	<ul style="list-style-type: none">○ 보안취약점 점검 수행○ 보안취약점 점검 보고서 작성○ 보안취약점 점검 및 기술이전
보안취약점 가이드라인 제작	<ul style="list-style-type: none">○ 당사 운영장비 가이드라인 작성<ul style="list-style-type: none">- 서버, DBMS, 보안장비, 네트워크, 웹 서버○ 어플리케이션 보안취약점 가이드라인 작성<ul style="list-style-type: none">- SQL 인젝션, XSS, CSRF 취약점 등

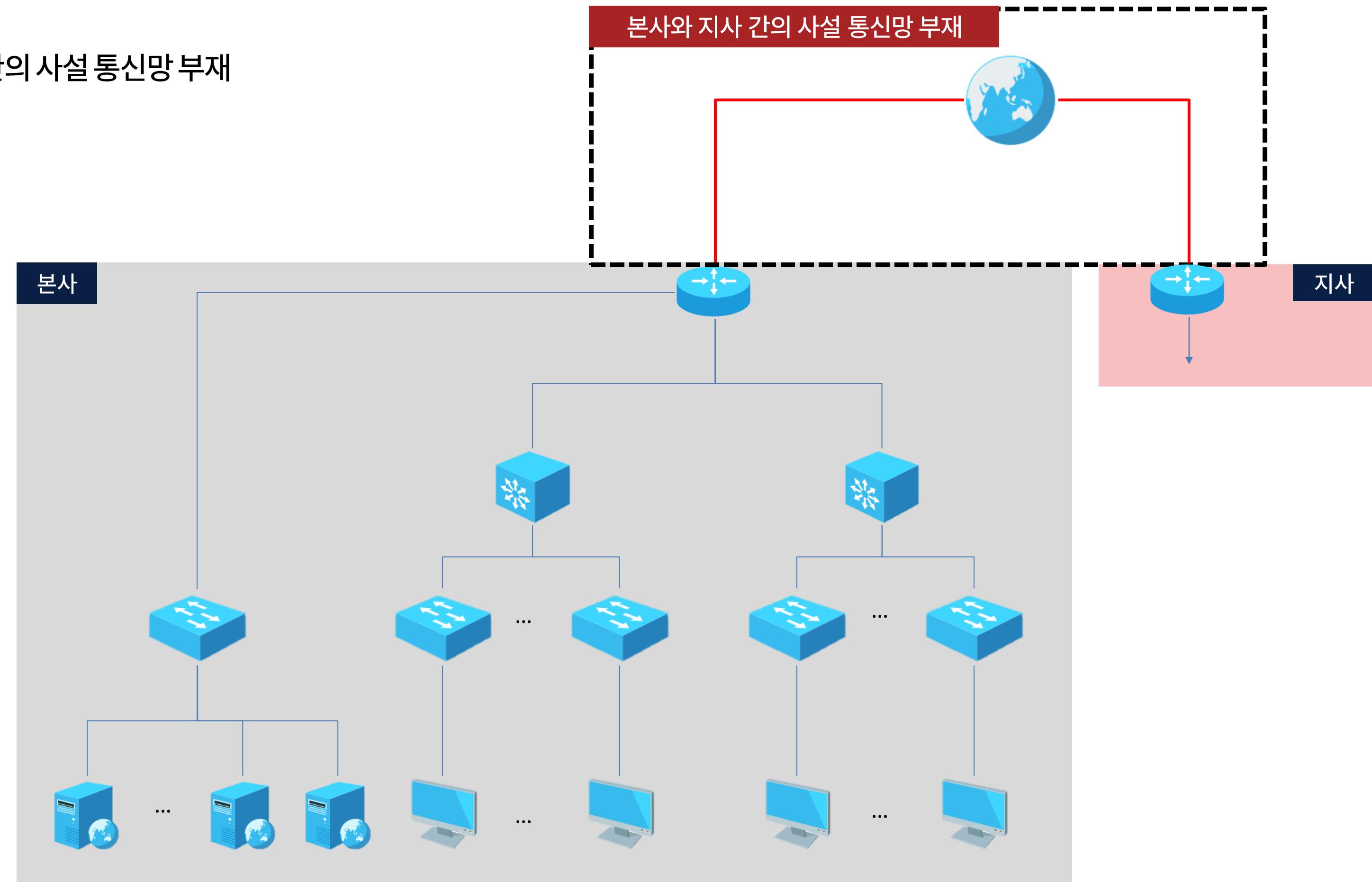
02

분석 및 점검

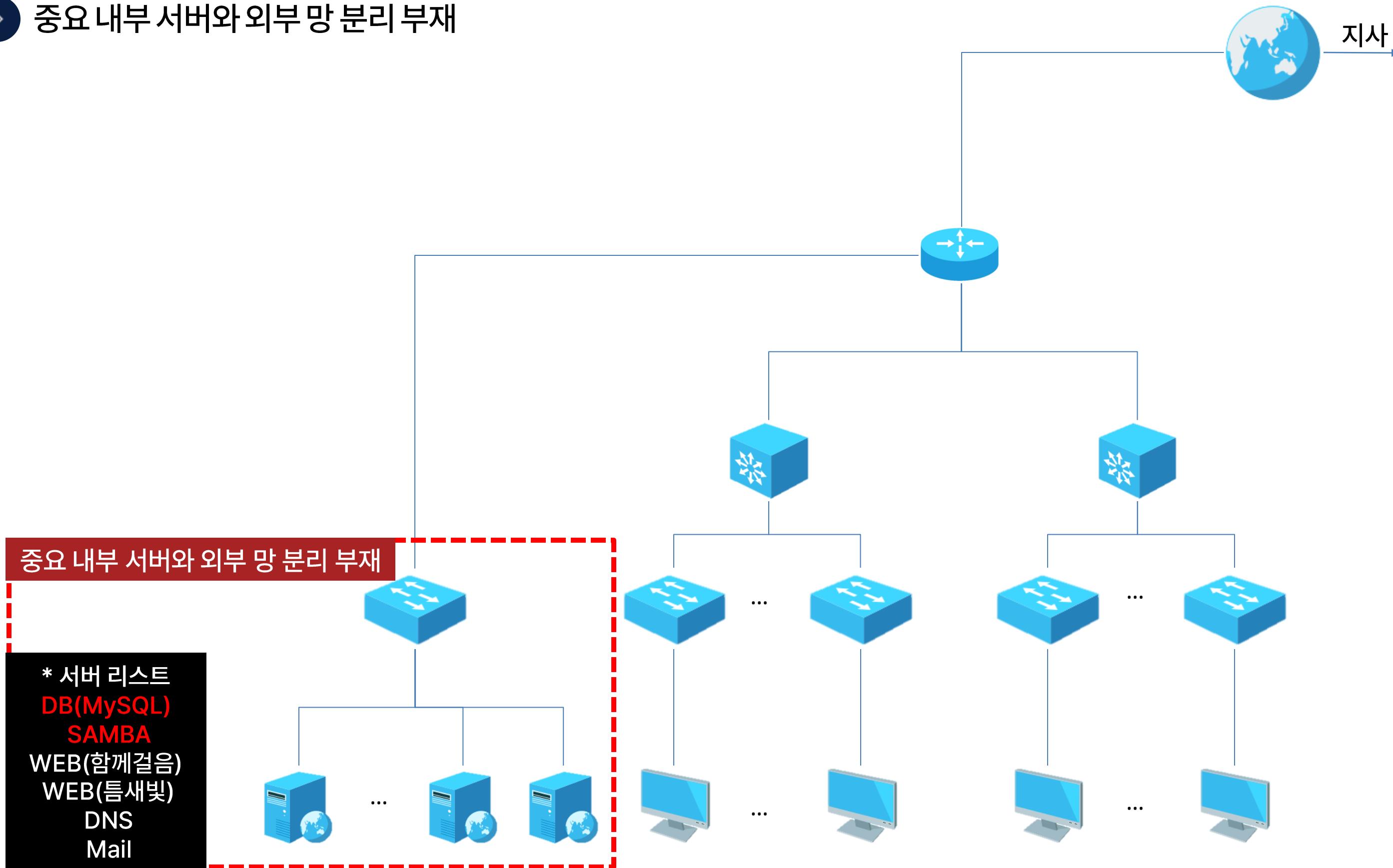
기존 고객사 인프라



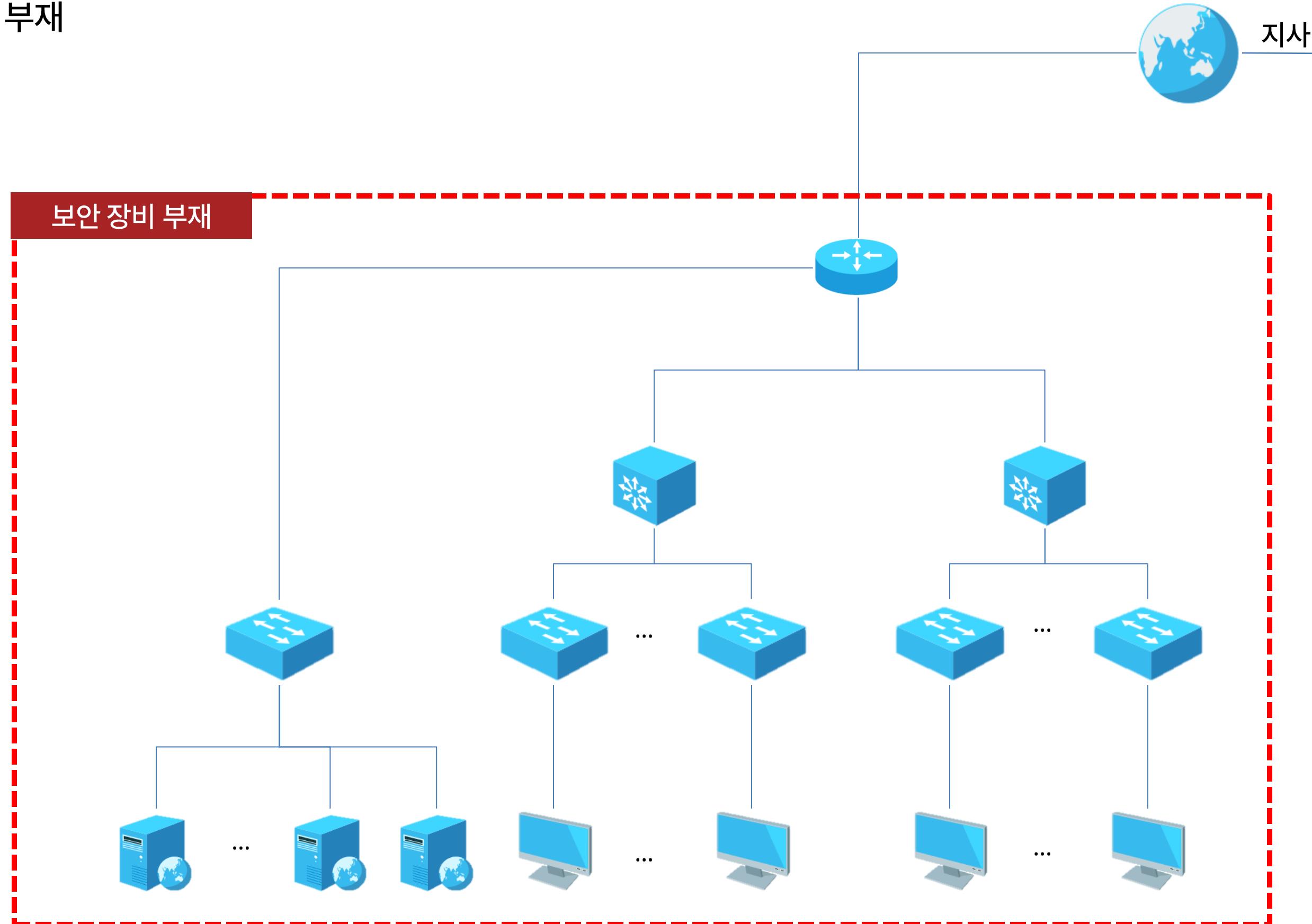
> 본사와 지사 간의 사설 통신망 부재



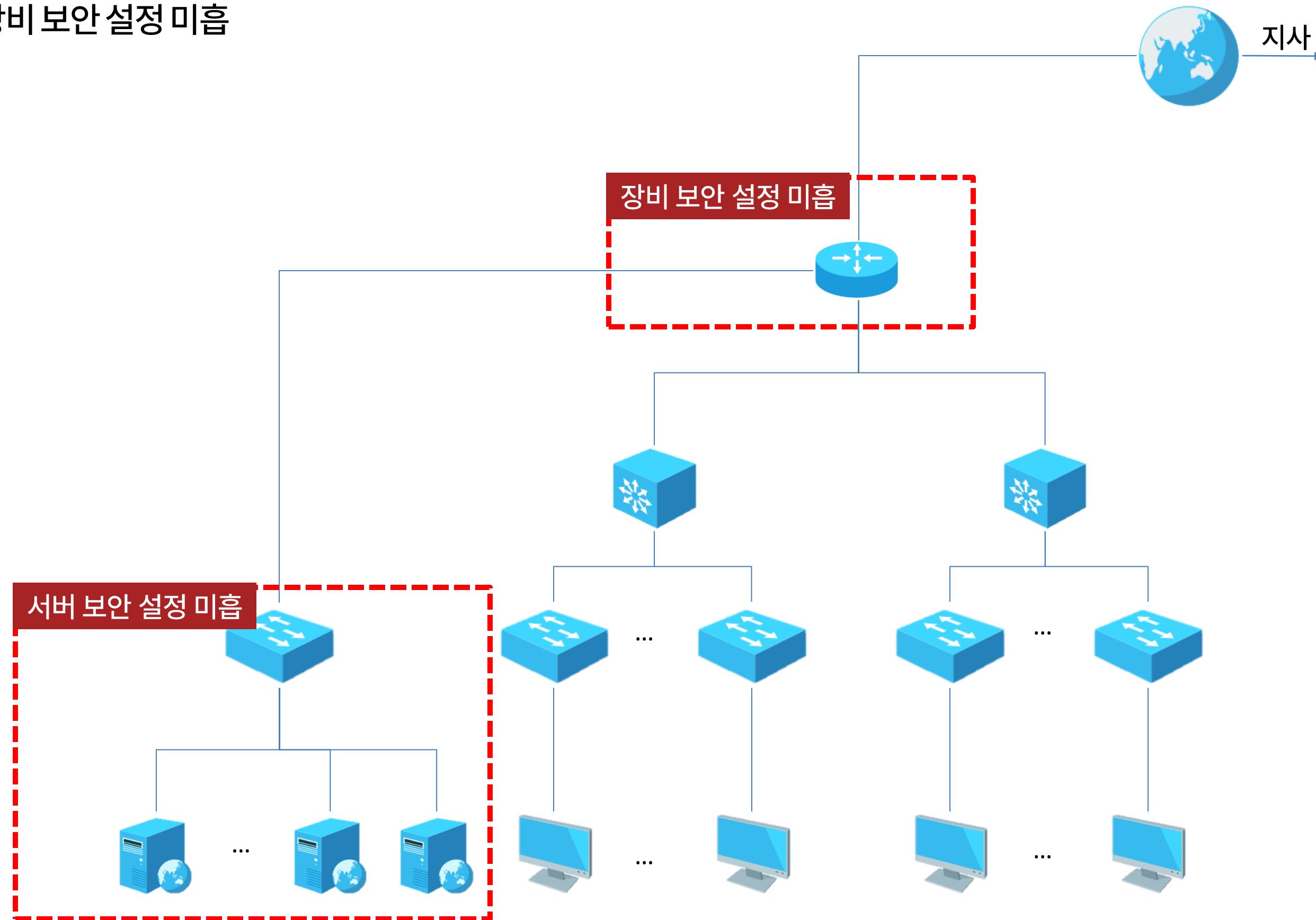
> 중요 내부 서버와 외부 망 분리 부재



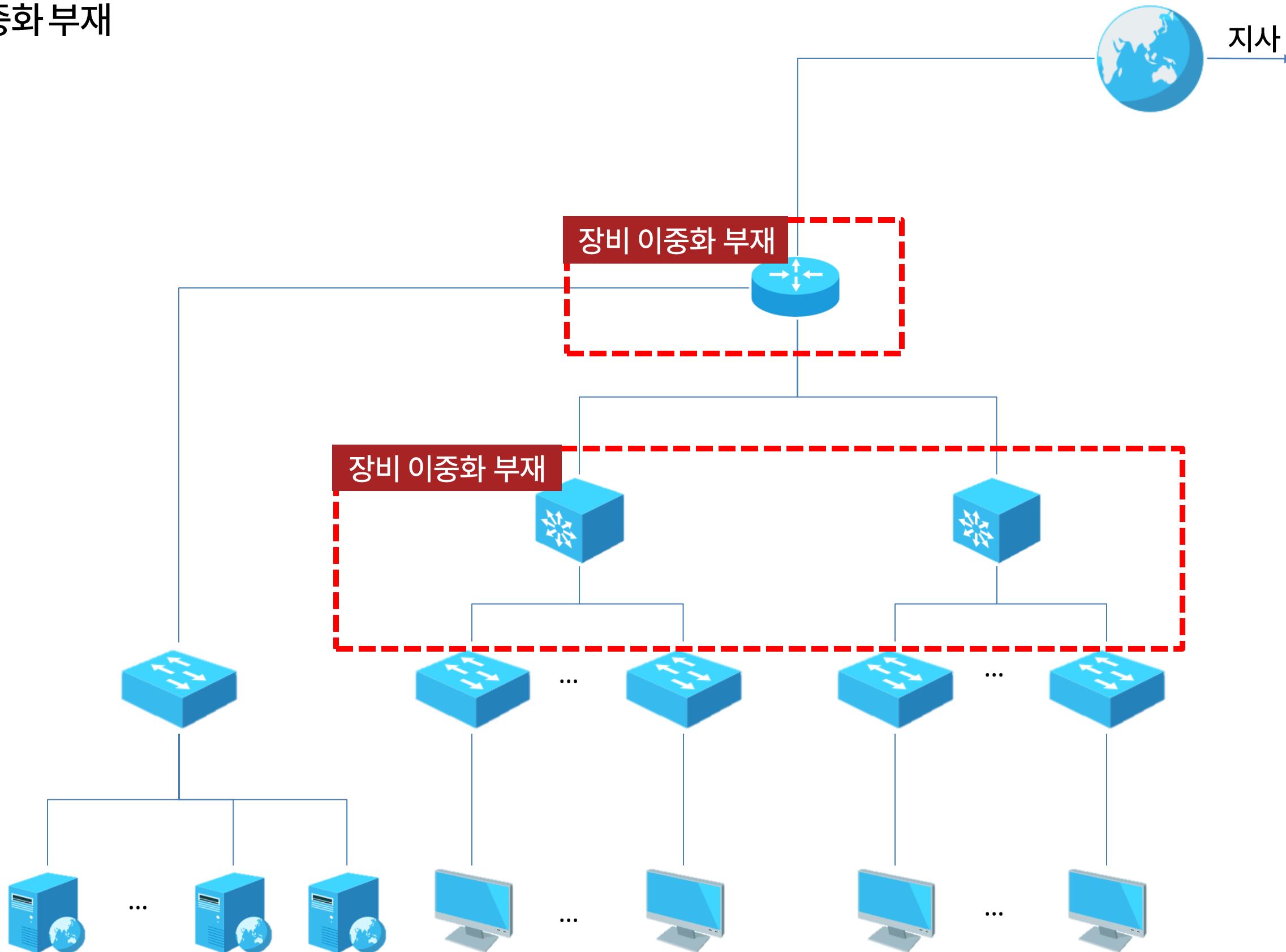
> 보안 장비 부재



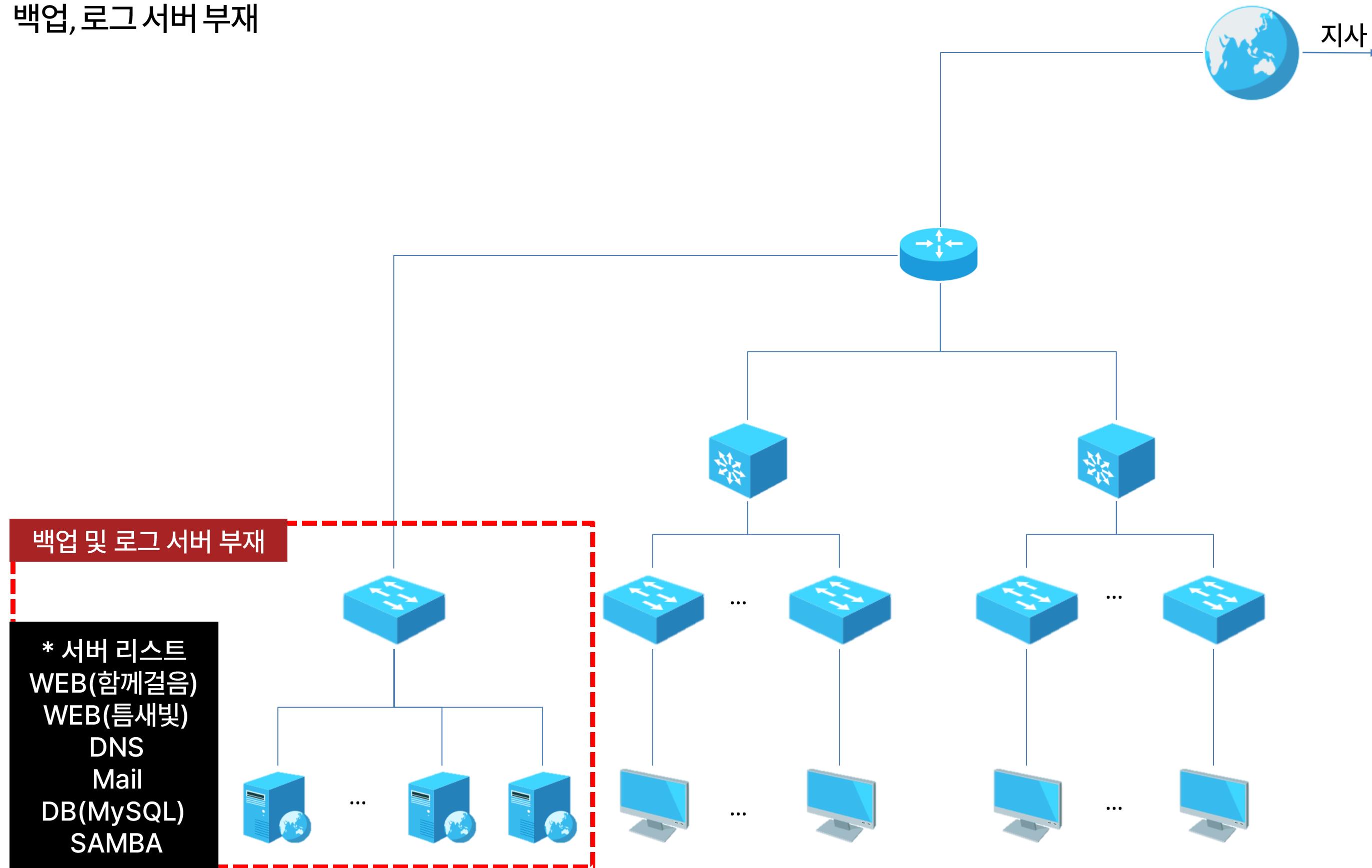
> 서버 및 장비 보안 설정 미흡



> 네트워크 장비 이중화 부재



> 백업,로그 서버 부재

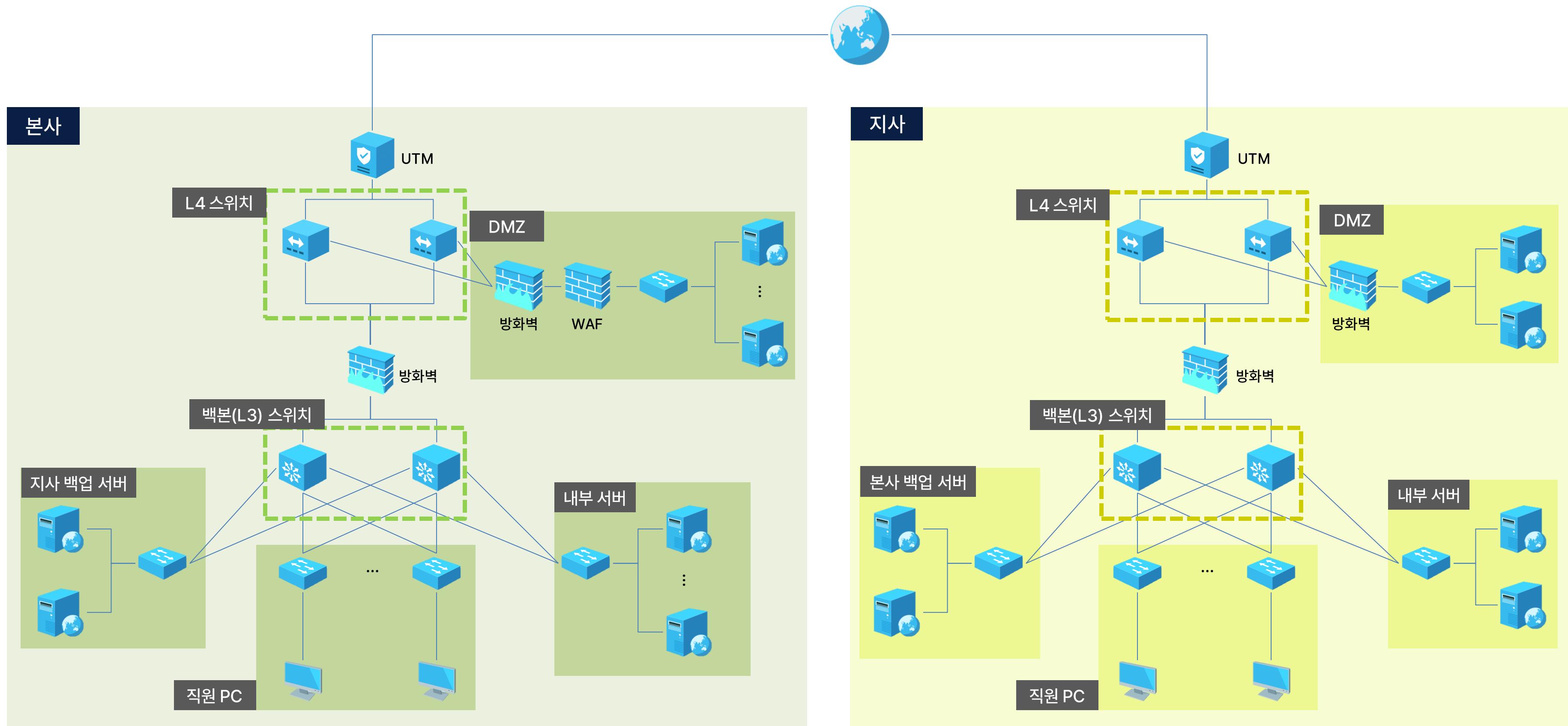


취약점	발생 가능한 위험
본사와 지사 간의 사설 통신망 부재	본사와 지사 간의 사설 통신 설정 부재 및 보안 미흡
중요 내부 서버와 외부 망 분리 부재	외부 네트워크에서 중요 서버 접근 가능
보안 장비 부재	네트워크 계층 별 보안 설정 부재
서버 및 장비 보안 설정 미흡	각종 위협에 대하여 취약점 노출
네트워크 장비 이중화 부재	네트워크 장비 장애 발생 시 가용성 침해
백업, 로그 서버 부재	보안 사고 대응 미흡

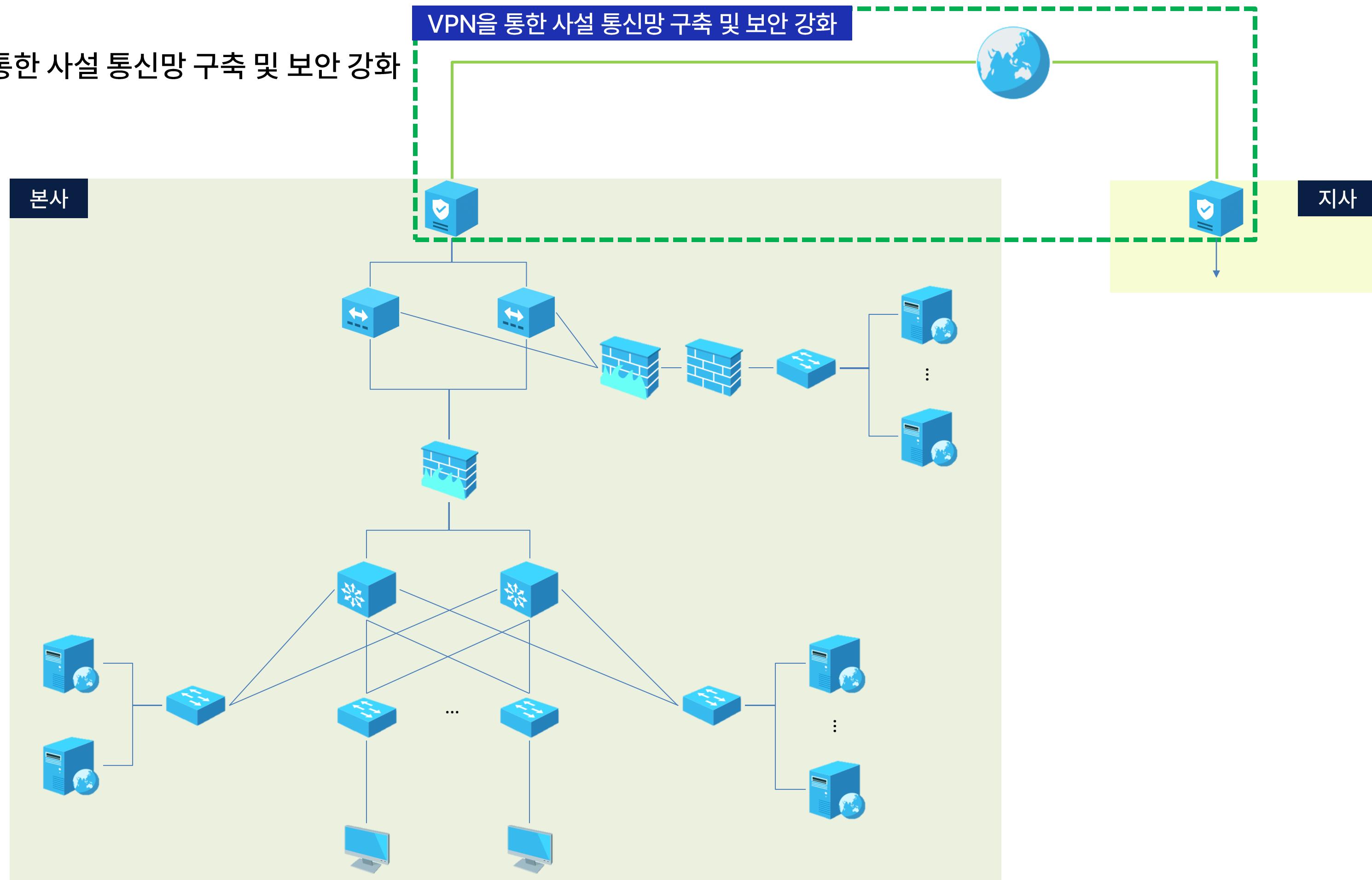
02

분석 및 점검

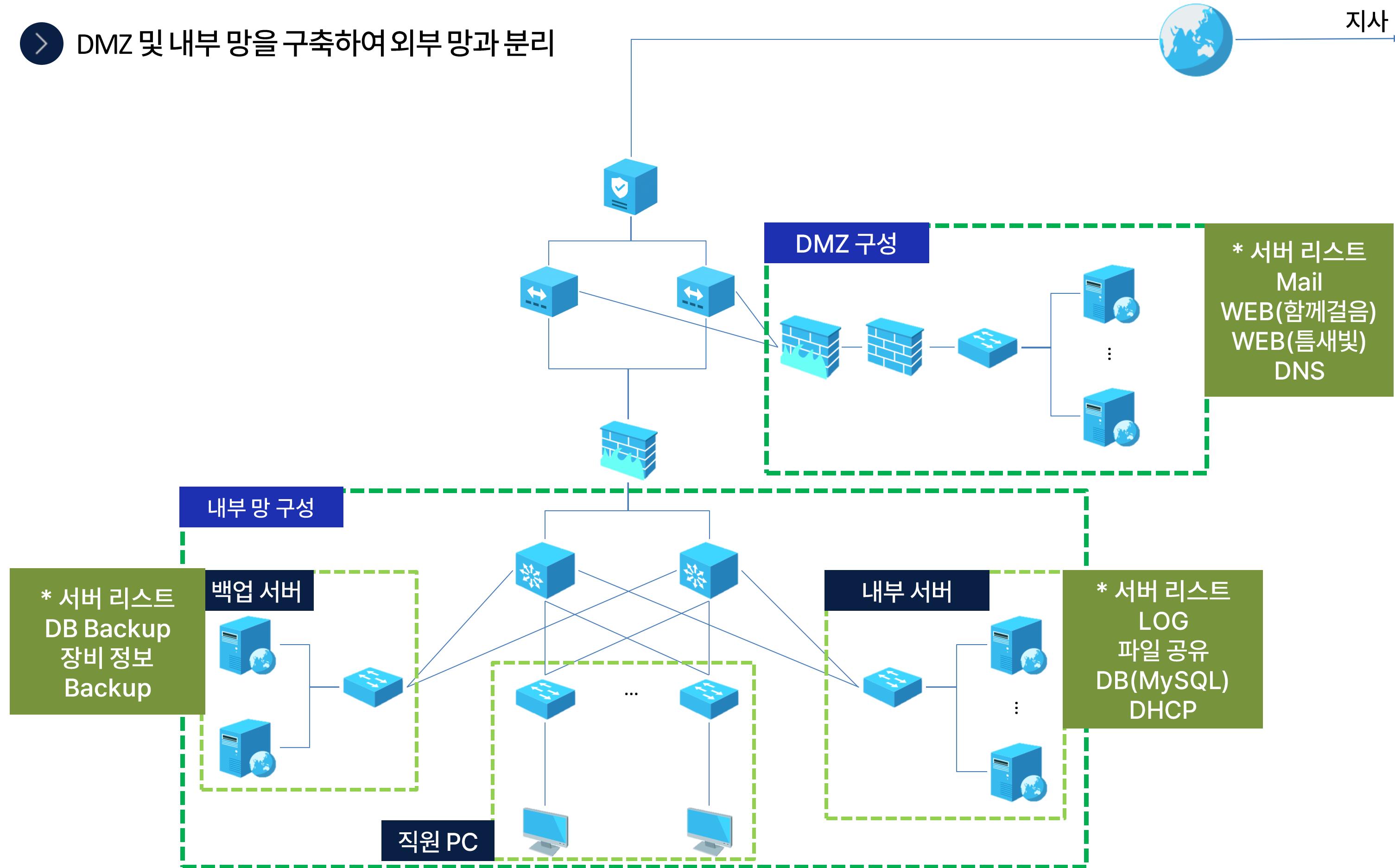
개선된 인프라



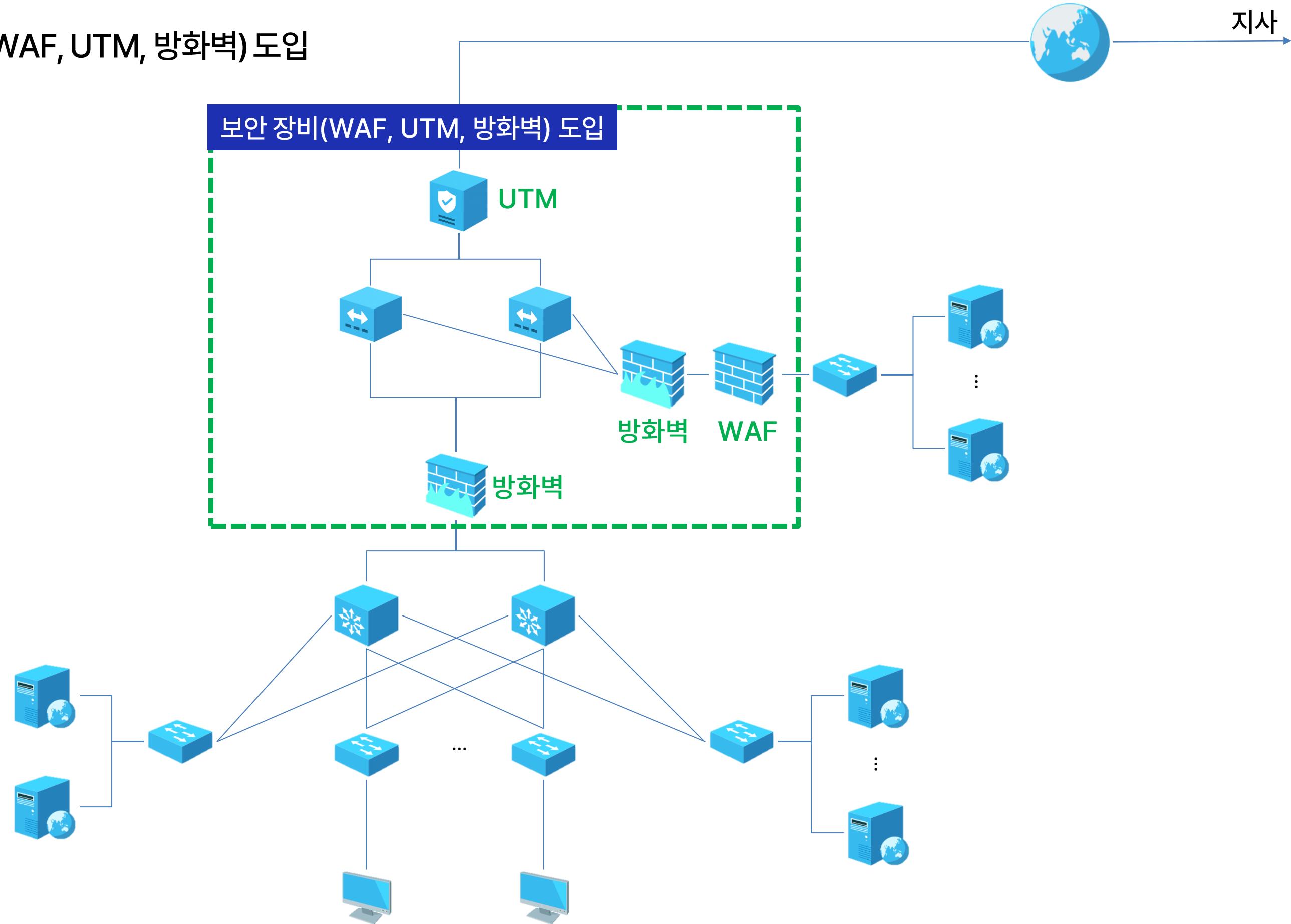
> VPN을 통한 사설 통신망 구축 및 보안 강화



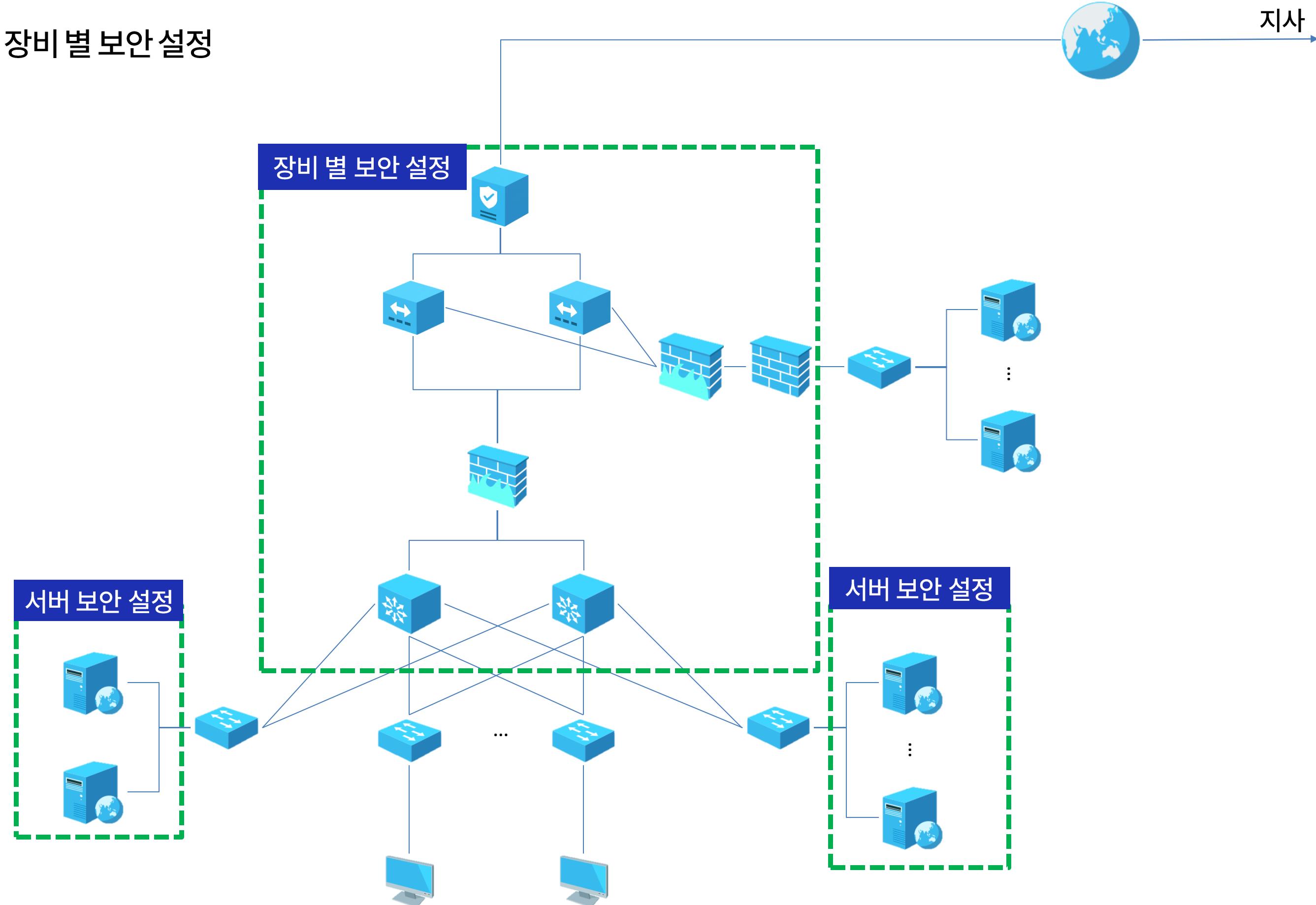
> DMZ 및 내부 망을 구축하여 외부 망과 분리



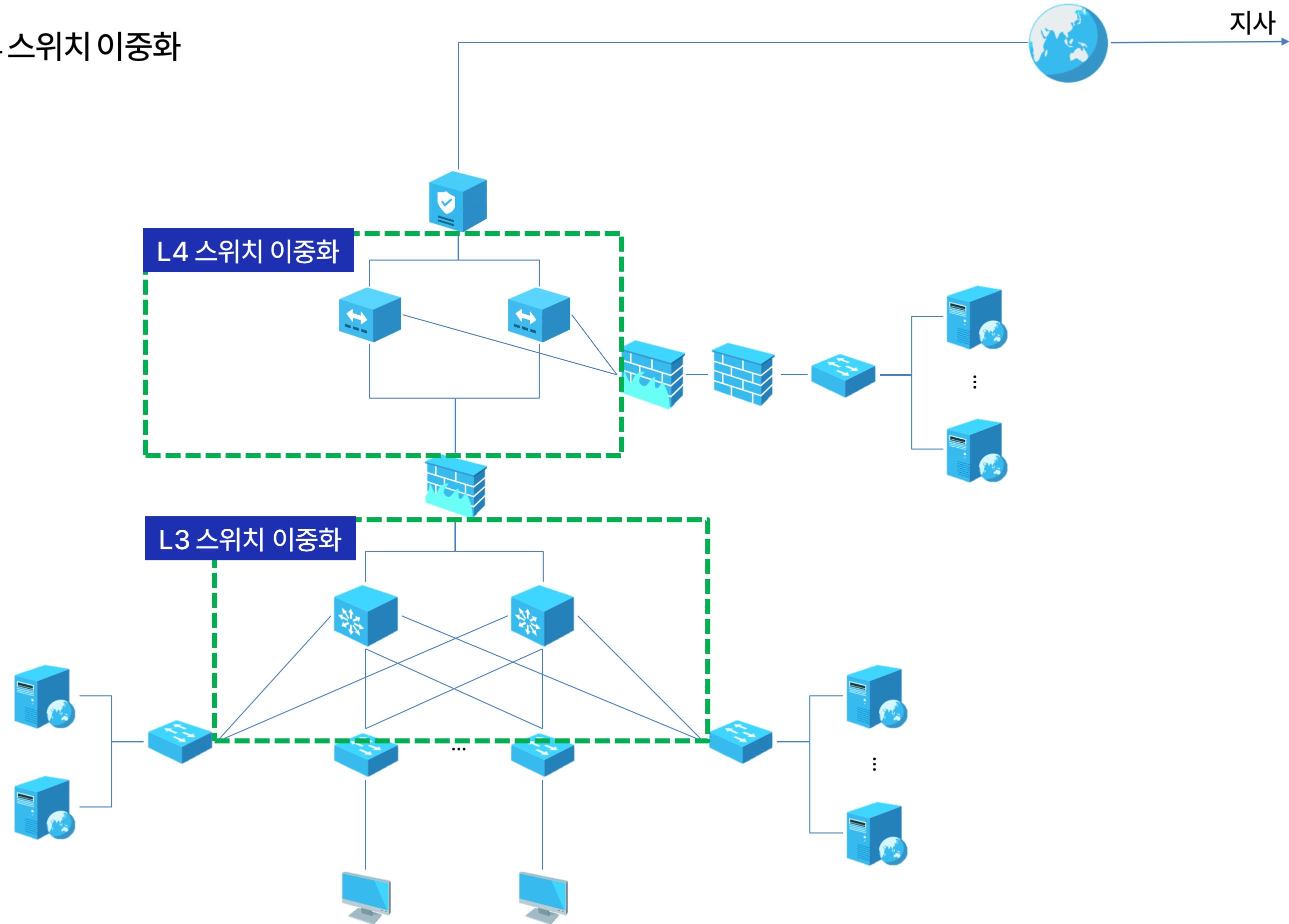
> 보안 장비(WAF, UTM, 방화벽) 도입



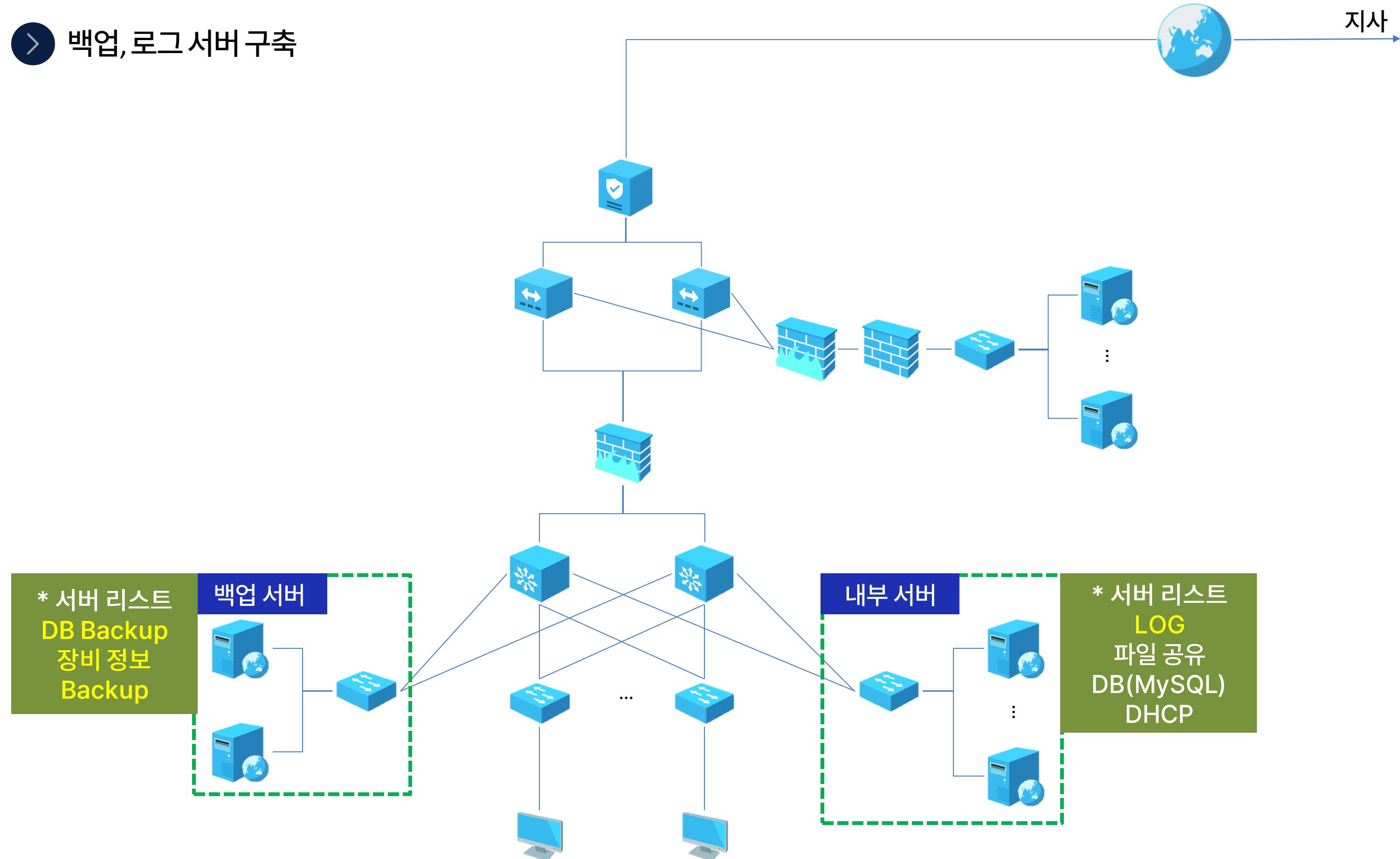
> 서버 및 장비 별 보안 설정



> 백본(L3), L4 스위치 이중화



> 백업,로그 서버 구축



취약점	개선 사항
본사와 지사 간의 사설 통신망 부재	GRE over IPSec를 통한 사설 통신망 구축 및 보안 강화
중요 내부 서버와 외부 망 분리 부재	DMZ 및 내부 망을 구축하여 외부 망과 분리 → 중요 서버 외부 네트워크 접근 차단
보안 장비 부재	보안 장비(WAF, UTM, 방화벽) 도입
서버 및 장비 보안 설정 미흡	주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세 가이드 기준 서버 및 장비 보안 설정
네트워크 장비 이중화 부재	L4 스위치, 백본(L3) 스위치 이중화로 네트워크 장비 장애 발생 상황 대응
백업, 로그 서버 부재	백업 및 로그 서버 구축으로 보안 사고 시 대응 조치

황승우

(PL)

담당 업무

- 본사 네트워크 점검, 보안 설정
- 보안장비 점검, 보안 설정
- 모의 해킹 수행

03

개인 발표

네트워크 인프라 점검

> 접근관리 개선

```
line con 0
  exec-timeout 5 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 1
  privilege level 15
  logging synchronous
  no exec
line vty 0 4
  access-class 2 in
  exec-timeout 5 0
  login
  transport input ssh2
```

```
line con 0
  exec-timeout 5 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 1
  privilege level 15
  logging synchronous
  no exec
line vty 0 4
  access-class 2 in
  exec-timeout 5 0
  login
  transport input ssh1
```

접근 관리

1	Session Timeout 설정	상	N-05
2	VTY 접속 시 안전한 프로토콜 사용	중	N-16
3	불필요한 보조 입·출력 포트 사용 금지	중	N-17

> 기능관리 개선

```

interface FastEthernet1/0
ip address 10.0.35.1 255.255.255.252
1 ip access-group 150 in
ip virtual-reassembly
duplex auto
speed auto
access-list 150 deny ip 0.0.0.0 0.255.255.255 any
access-list 150 deny ip 127.0.0.0 0.255.255.255 any
access-list 150 deny ip 169.254.0.0 0.0.255.255 any
access-list 150 deny ip 172.16.0.0 0.15.255.255 any
access-list 150 deny ip 192.0.2.0 0.0.0.255 any
access-list 150 deny ip 224.0.0.0 15.255.255.255 any
access-list 150 permit ip any any

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet0/1	unassigned	YES	NVRAM	administratively down	down
FastEthernet1/0	unassigned	YES	unset	administratively down	down
2 FastEthernet1/1	unassigned	YES	unset	up	up
FastEthernet1/2	unassigned	YES	unset	administratively down	down
FastEthernet1/3	10.0.35.18	YES	NVRAM	up	up
FastEthernet1/4	unassigned	YES	unset	administratively down	down
FastEthernet1/5	unassigned	YES	unset	up	down
FastEthernet1/6	unassigned	YES	unset	administratively down	down
FastEthernet1/7	unassigned	YES	unset	administratively down	down
FastEthernet1/8	unassigned	YES	unset	administratively down	down
FastEthernet1/9	unassigned	YES	unset	administratively down	down
FastEthernet1/10	unassigned	YES	unset	administratively down	down
FastEthernet1/11	unassigned	YES	unset	administratively down	down
FastEthernet1/12	unassigned	YES	unset	administratively down	down
FastEthernet1/13	unassigned	YES	unset	administratively down	down
FastEthernet1/14	unassigned	YES	unset	administratively down	down

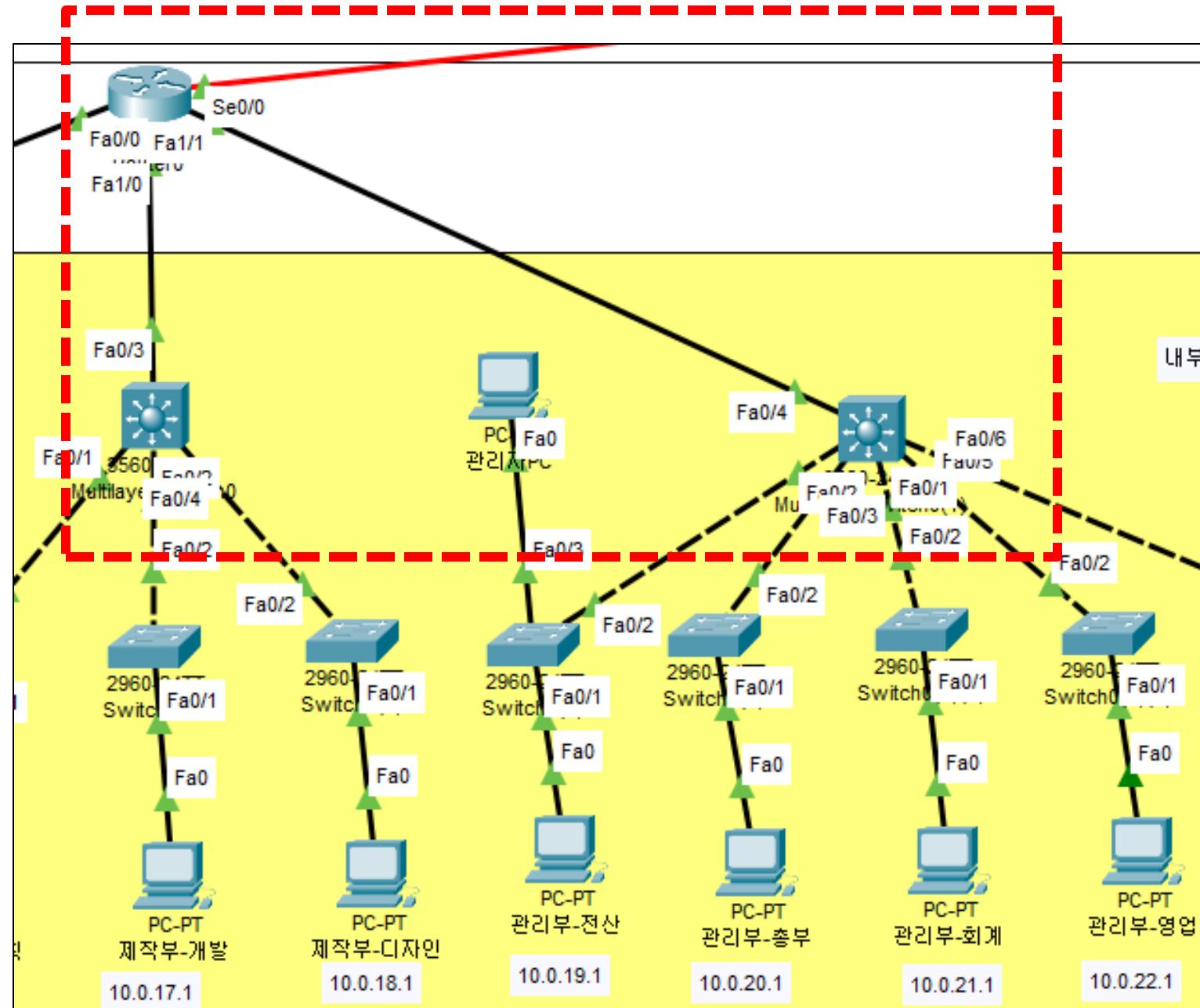
```

interface Vlan10
ip address 10.0.16.254 255.255.255.0
no ip redirects
3 no ip unreachables
no ip proxy-arp
4 vrrp 10 ip 10.0.16.252
vrrp 10 timers learn
vrrp 10 priority 120
vrrp 10 track 10 decrement 30

```

기능 관리	1 Spoofing 방지 필터링 적용 또는 보안장비 사용	상	N-12
	2 사용하지 않는 인터페이스의 Shutdown 설정	상	N-14
	3 Proxy ARP 차단	중	N-32
	4 ICMP unreachable, Redirect 차단	중	N-33

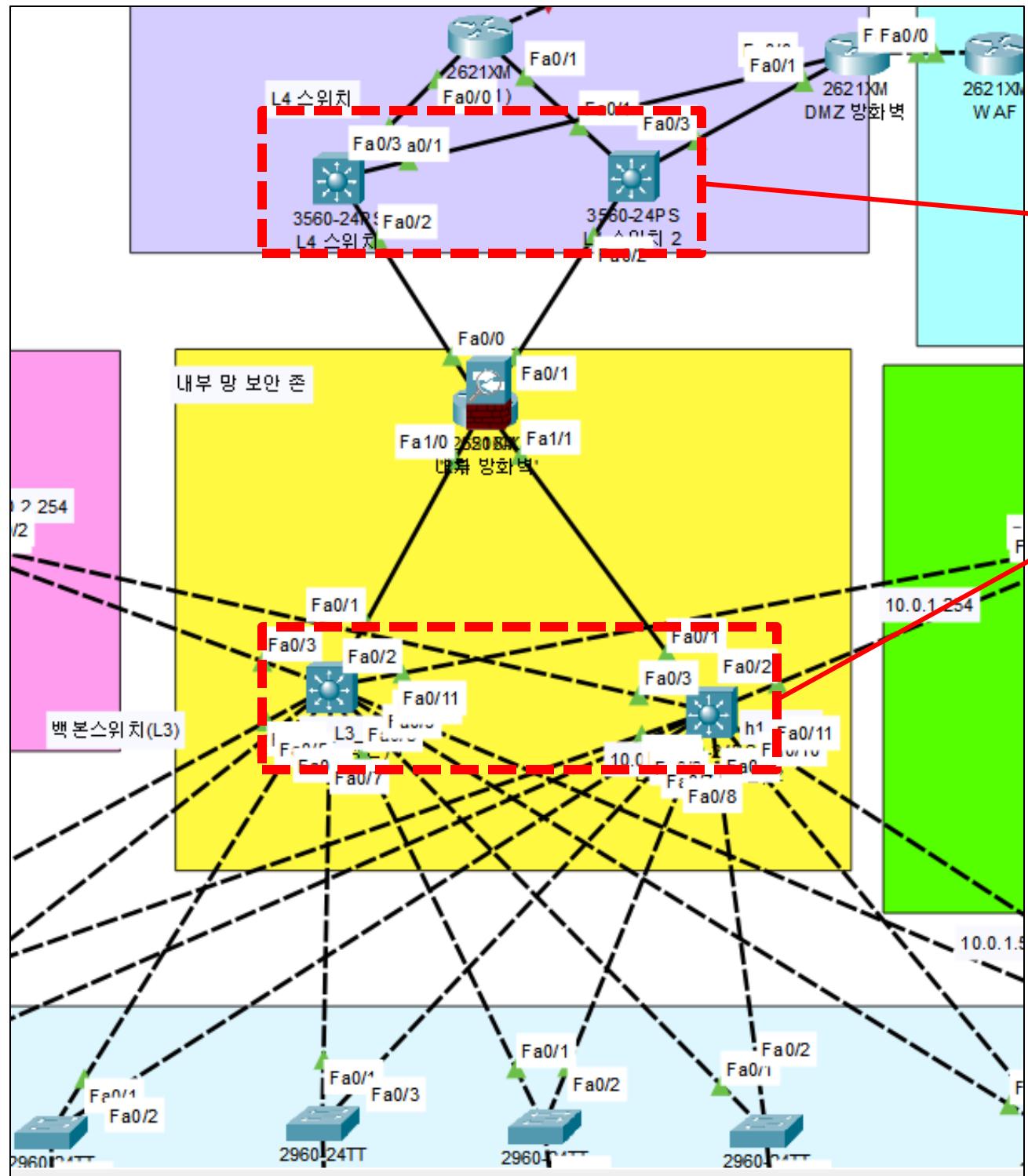
> 개선 전 문제점



> 단일 장애 지점(SPOF) 존재

- 1 단일 장비 장애시 전체 네트워크 서비스 중단
- 2 장애 동안 서비스 제공 불가 및 장애 복구 시간 증가
- 3 유지보수·업데이트 시 서비스 중단
- 4 공격 또는 장애시 우회 경로 부재

> 개선 후

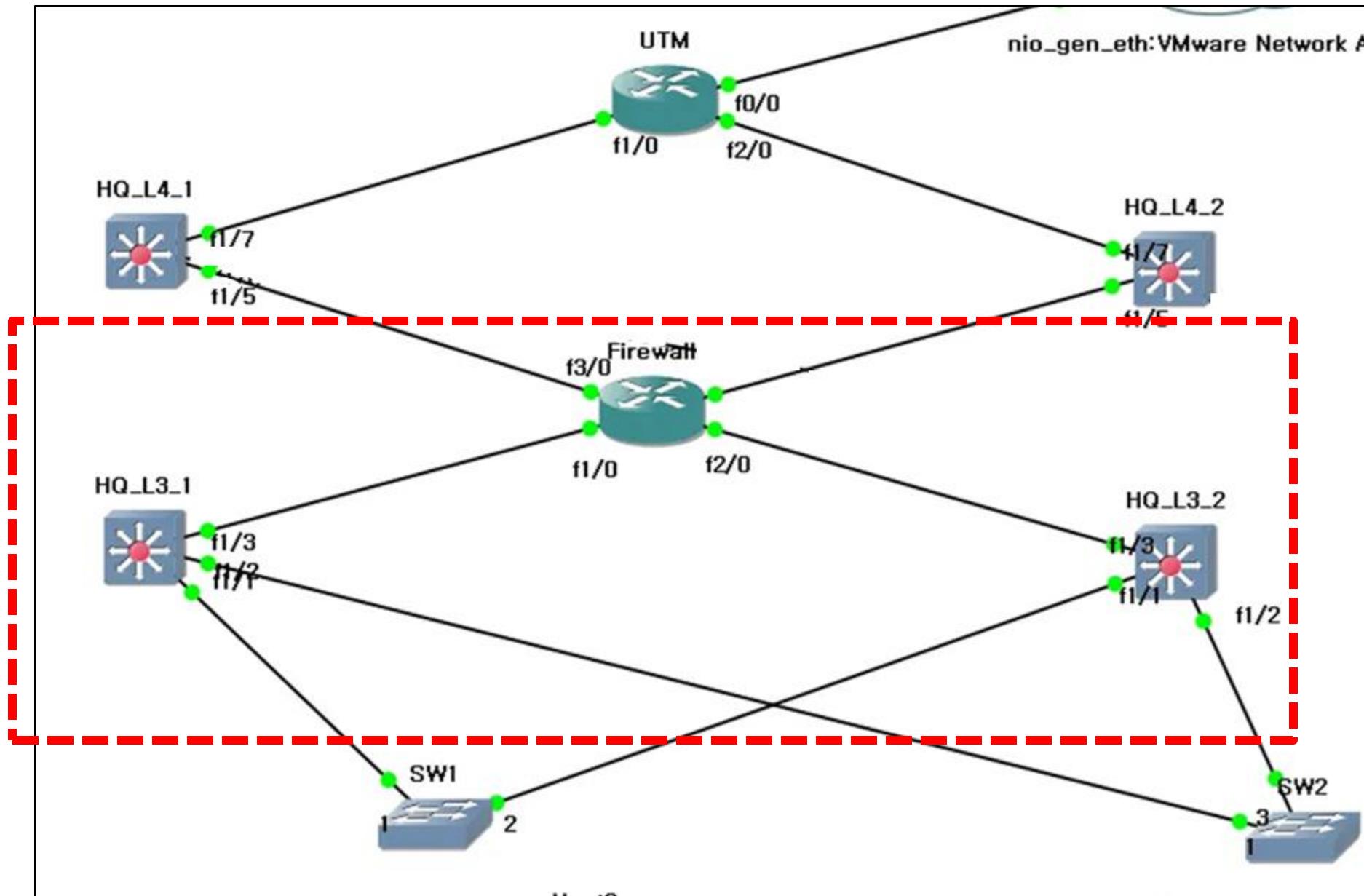


L3, L4 장비 이중화

1 장애 발생 시 서비스 중단 문제 해결

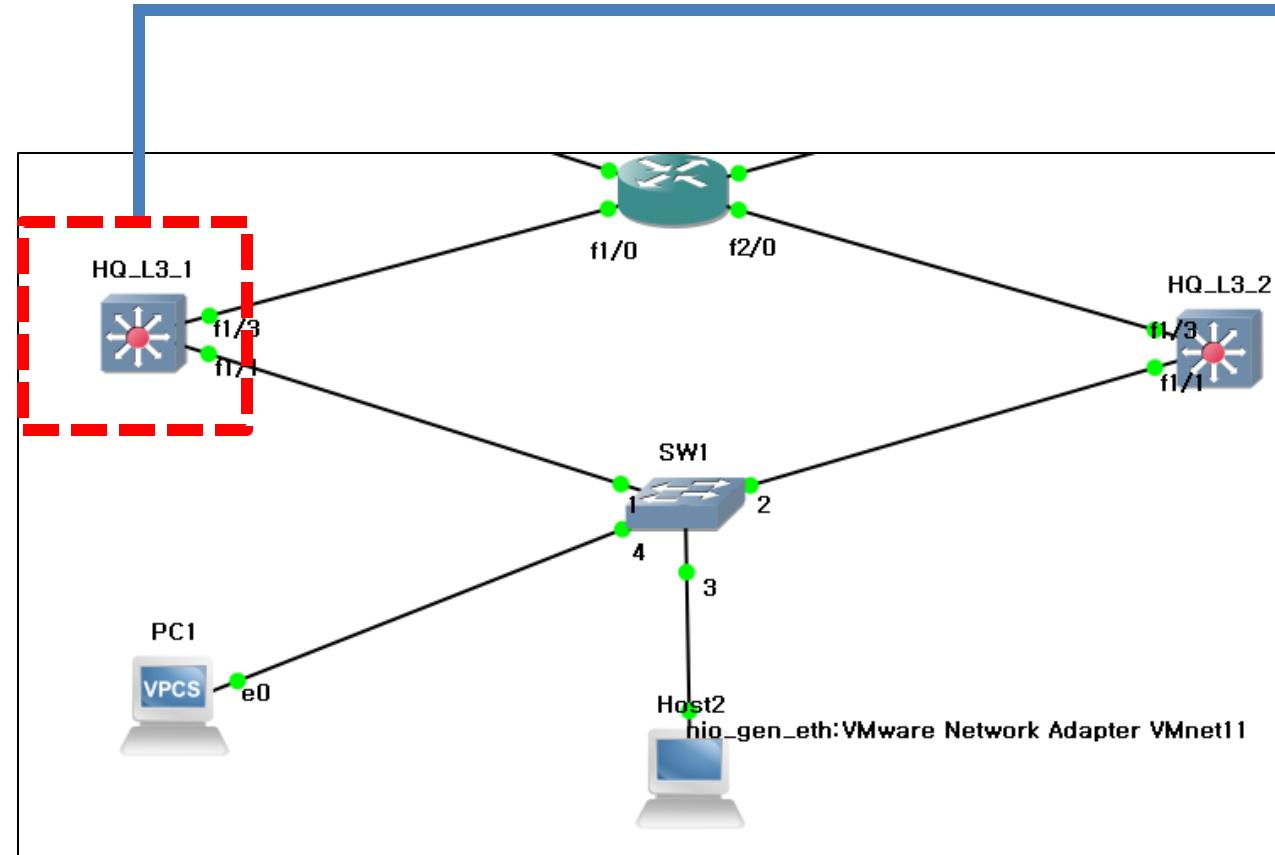
2 비즈니스 연속성 저하 문제 완화

> VRRP 설정



- 1 가용성 증가
- 2 호환성 확보
- 3 확장성 보장

> HQ_L3_1 VRRP 설정

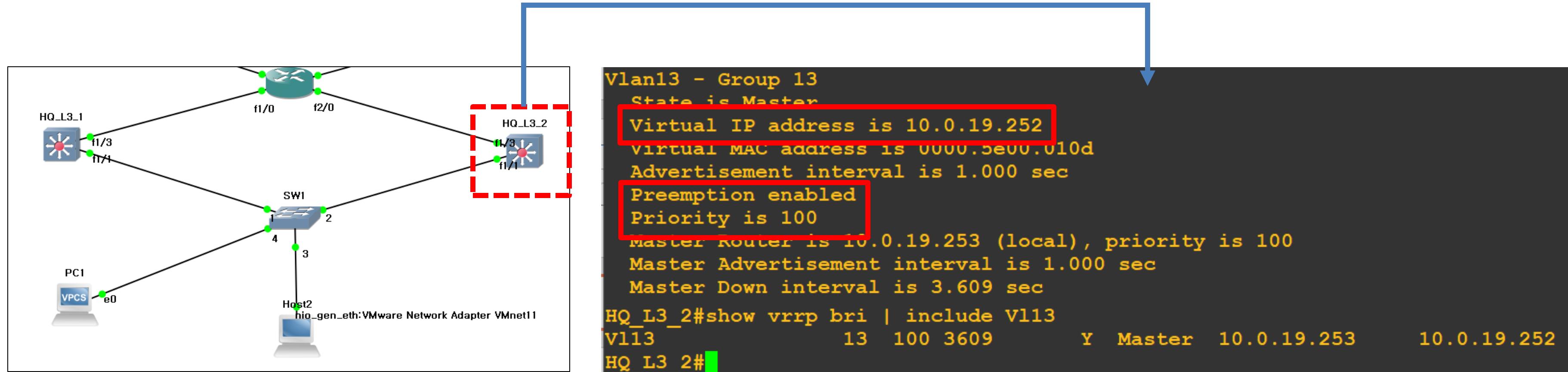


```
Vlan13 - Group 13
  State is Backup
  Virtual IP address is 10.0.19.252
  Virtual MAC address is 0000.5e00.010d
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 90 (cfgd 120)
    Track object 13 state Down decrement 30
  Master Router is 10.0.19.253, priority is 100
  Master Advertisement interval is 1.000 sec

HQ_L3_1#show vrrp bri | include Vl13
Vl13           13  90  3531      Y  Backup  10.0.19.253      10.0.19.252
```

- 1 VirtualIP 10.0.X.252
- 2 Priority값 120
- 3 Preempt 설정

> HQ_L3_2 VRRP 설정



1 VirtualIP 10.0.X.252

2 Priority 값 100

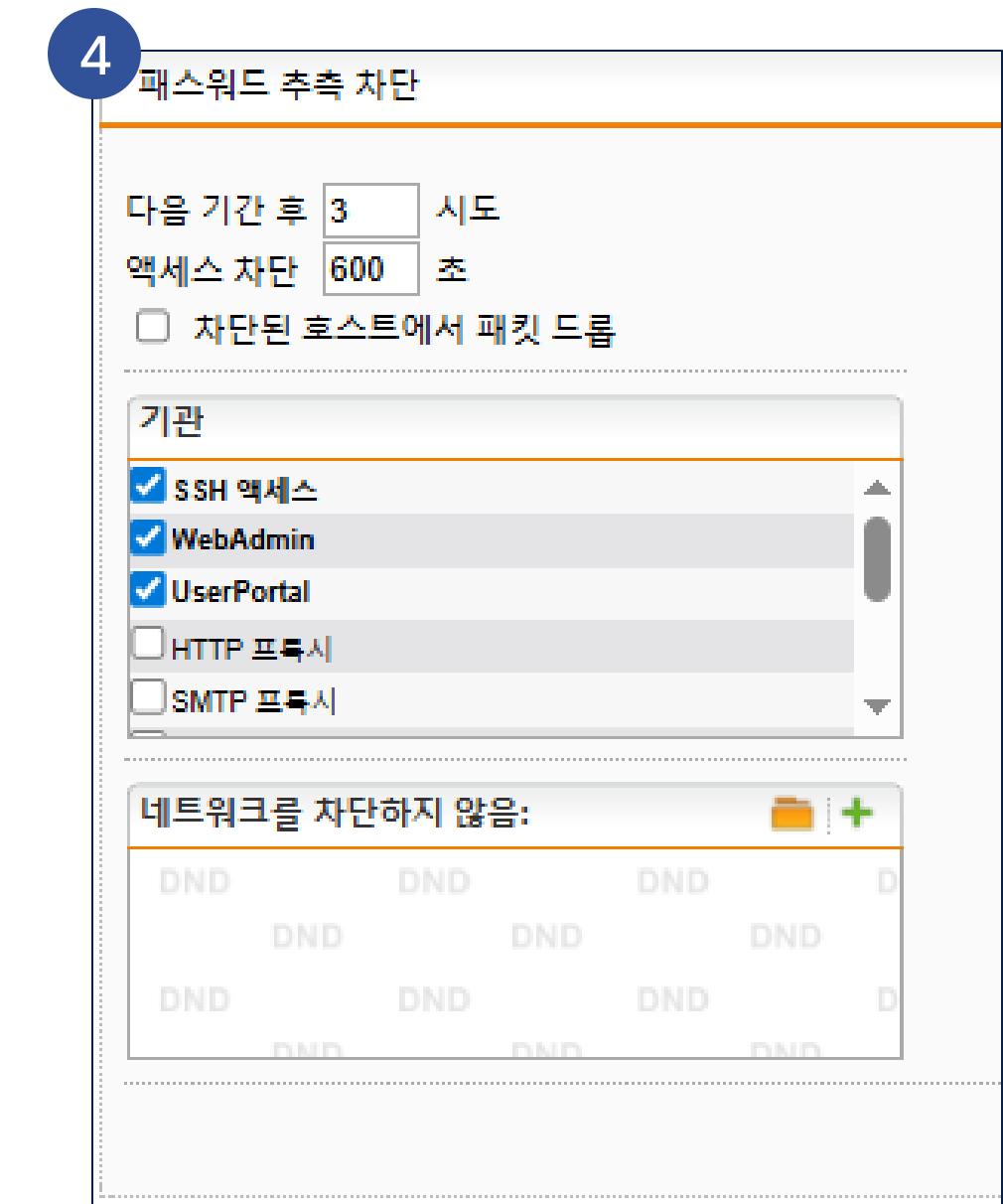
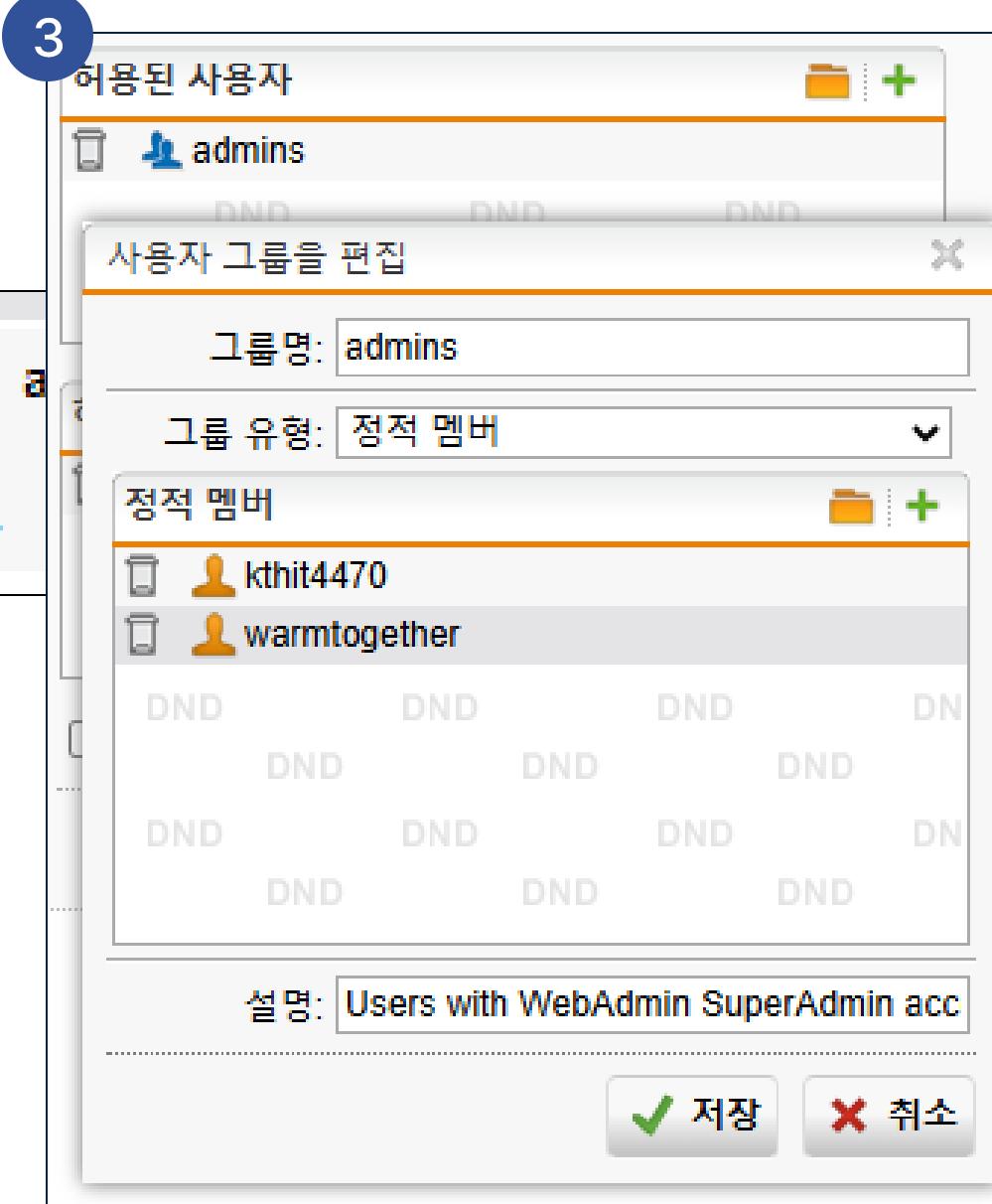
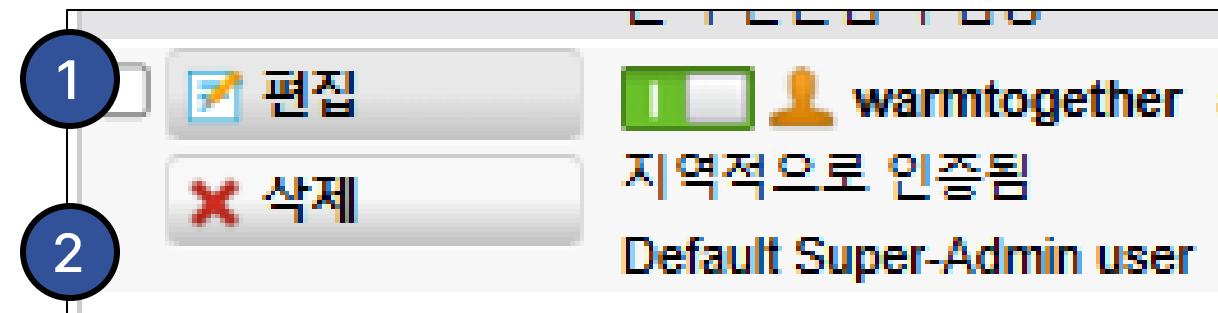
3 Preempt 설정

03

개인 발표

UTM

계정 관리 설정



계정 관리

1 보안장비 Default 계정 변경

상 S-01

2 보안장비 Default 패스워드 변경

상 S-02

3 보안장비 계정별 권한 설정

상 S-03

4 로그인 실패횟수 제한

중 S-17

> 접근 관리 설정

1

WebAdmin 액세스 구성

허용된 사용자

admins	DND	DND	DND
DND	DND	DND	DND
DND	DND	DND	DND

허용된 네트워크

본사 전산팀 네트워크

네트워크 정의 편집

이름: 본사 전산팀 네트워크
유형: 네트워크
IPv4 주소: 10.0.19.0
네트마스크 /24 (255.255.255.0)
설명:
 고급

저장 취소

2

허용된 네트워크

본사 전산팀 네트워크

DND	DND	DND
DND	DND	DND
DND	DND	DND

SSH 허용 네트워크가 성공적으로 설정되었습니다.

3

WebAdmin 유회 시간 제한

후에 로그 아웃 600 초
 대시보드에서 로그아웃합니다.

WebAdmin 시간 제한을 성공적으로 변경했습니다.

접근 관리

1 보안장비 원격 관리 접근 통제

상

S-05

2 보안장비 보안 접속

상

S-06

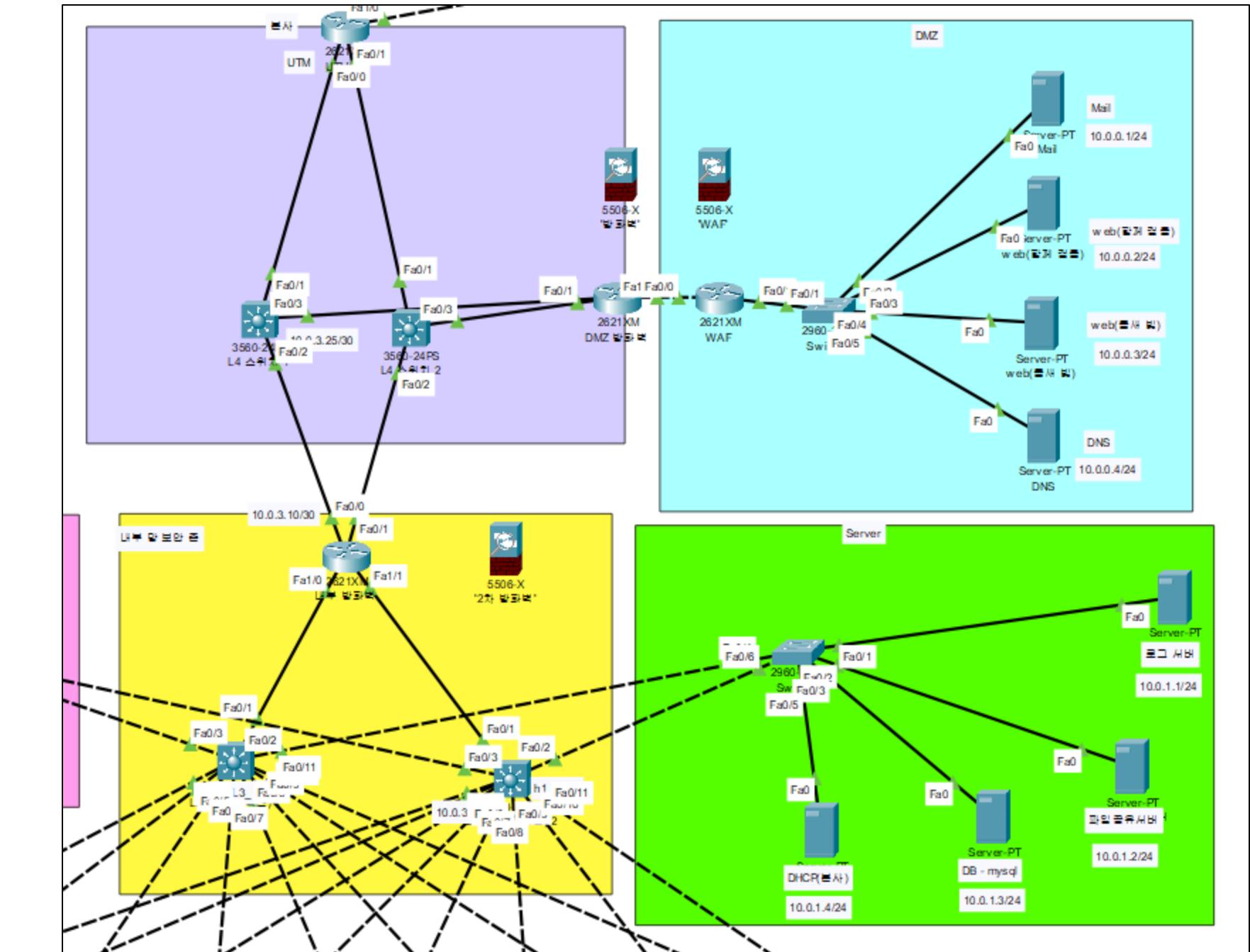
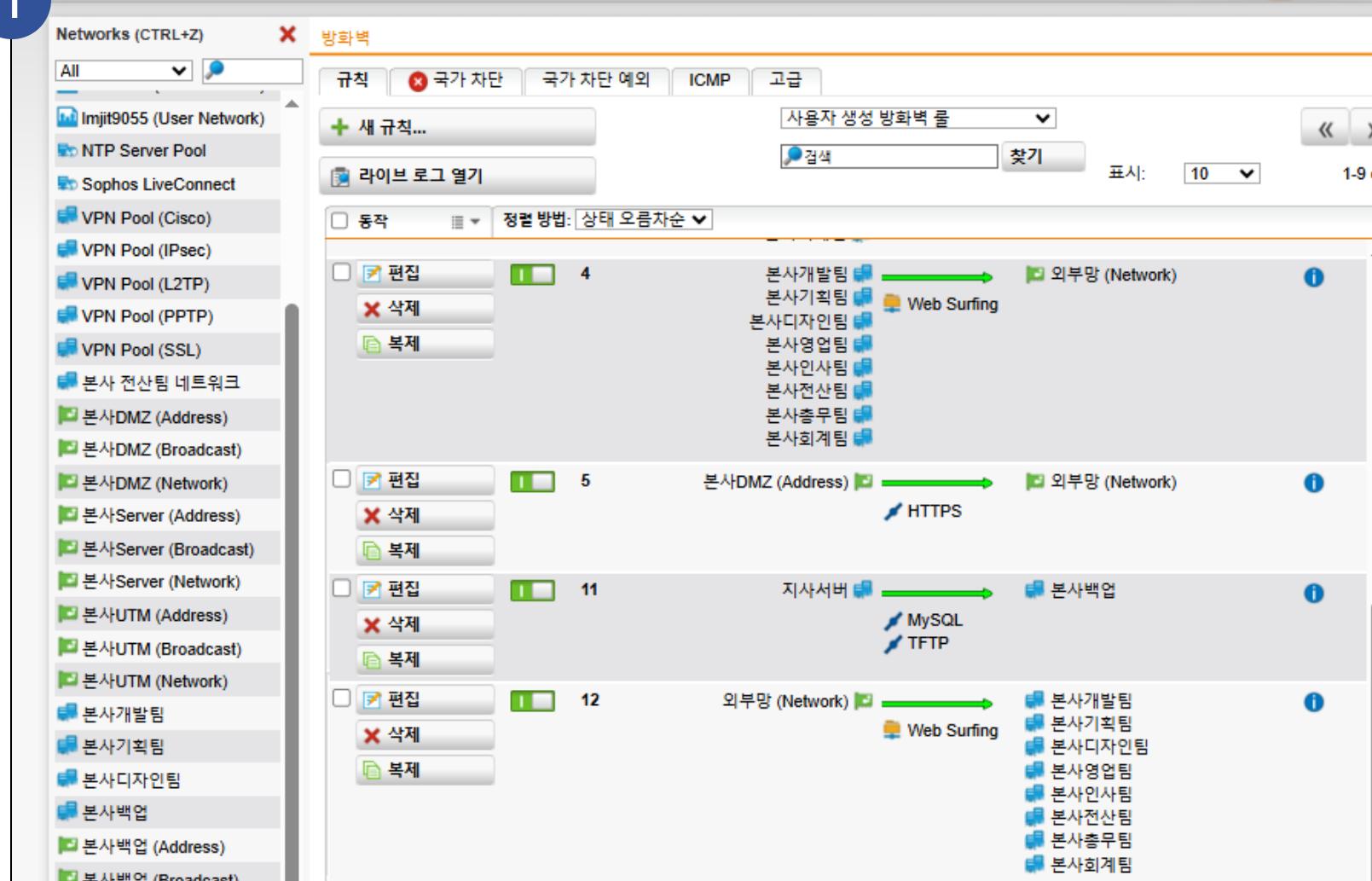
3 Session timeout 설정

상

S-07

> 기능 관리 설정

1



1 DMZ 설정

기능 관리

이상징후 탐지 모니터링 수행

유해 트래픽 차단 정책 설정

상

S-11

상

S-13

중

S-25

기능 관리 설정

2

기능/보고

<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	INFO-700	Daily log file archive
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	INFO-710	Log file partition is filling up
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	INFO-726	VPN connection using Site-to-Site is up again
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	INFO-727	RED connection is up again
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	INFO-728	Access Point is online again
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	INFO-729	Mesh Access Point is online again
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	WARN-711	Log files have been deleted
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	WARN-715	Remote log file storage failed
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	WARN-726	VPN connection using Site-to-Site is down
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	WARN-727	RED connection is down
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	WARN-728	Access Point is offline
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	WARN-729	Mesh Access Point is offline
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	CRIT-712	System shut down due to full log file partition
<input checked="" type="checkbox"/> 이메일	<input checked="" type="checkbox"/> SNMP	모두 전환	

공지

발신자: do-not-reply@fw-notify.net

알림 수신자들:

- root@wamtogther.com
- kthit4470@wamtogther.com
- lmj9055@wamtogther.com

제한 통고

알림 설정을 성공적으로 저장했습니다.

3

터 동작 추가

카테고리 웹사이트 다운로드 안티바이러스 추가 옵션

이름: 기본 트래픽 규칙

아래에 지정된 항목을 제외한 모든 콘텐츠 허용
아래 지정 항목을 제외한 모든 콘텐츠 차단

스파이웨어 감염 및 통신 차단

범주	동작
IT	차단
Locomotion	차단
개인 홈 페이지	차단
게임/도박	차단
극단적 사이트들	차단
금융/투자	차단
라이프 스타일	차단
무기	차단
범죄 행위	차단
신체 노출	차단
악품	차단
오락 / 문화	차단
의심스러운	차단
의학	차단
작업 검색	차단
정보와 통신	차단
주문	차단
커뮤니티/교육/종교	차단
분류되지 않은 웹 사이트	차단

신뢰도가 다음 임계값 미만인 웹 사이트 차단: 확인되지 않음

« 뒤로 » 다음 ✓ 저장 ✖ 취소

기본 정책 일의 항상 기본 트래픽 규칙

기능 관리

DMZ 설정

- 2 이상징후 탐지 모니터링 수행
- 3 유해 트래픽 차단 정책 설정

상

S-11

상

S-13

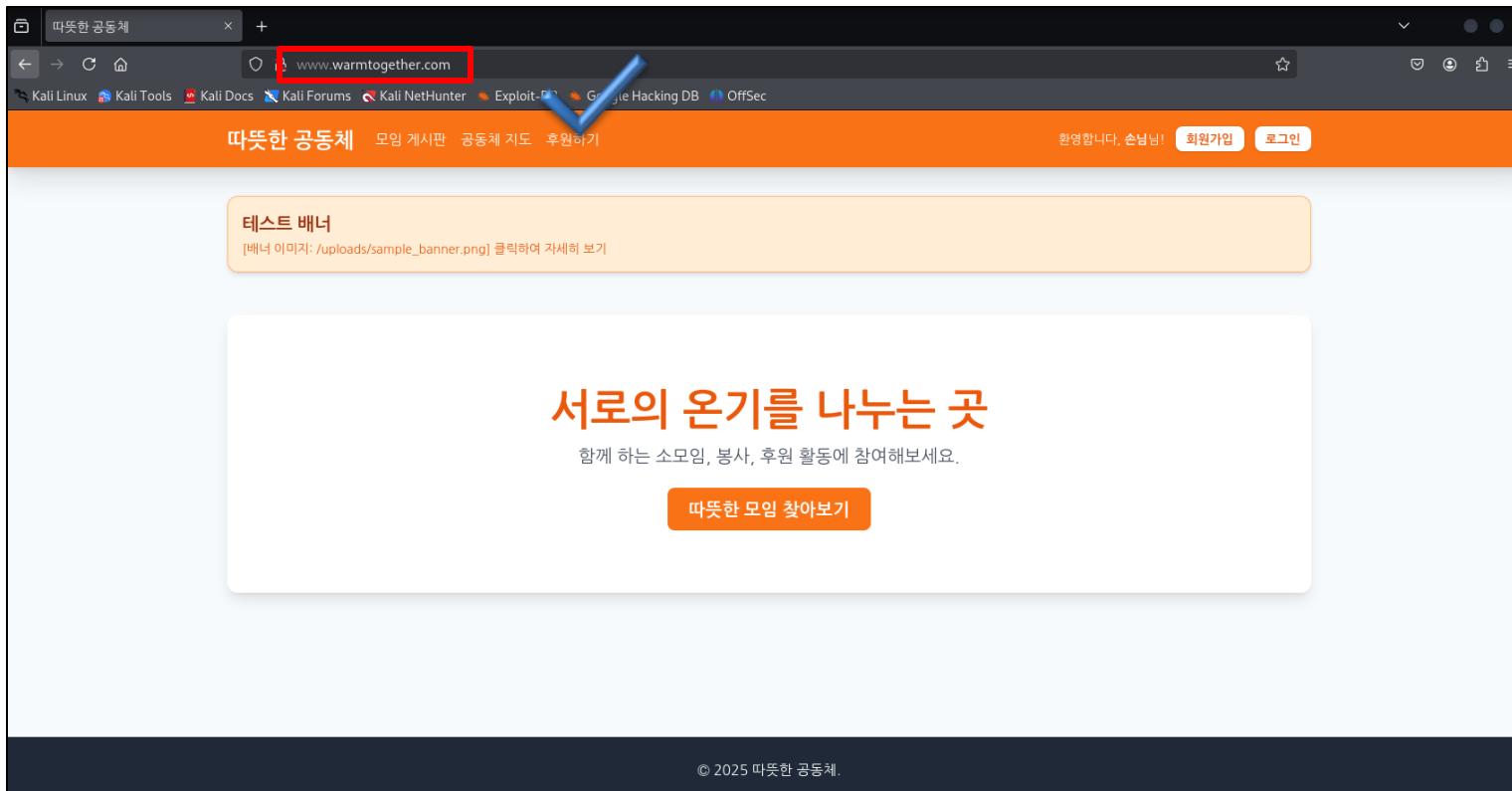
중

S-25

03

개인 발표

WEB 취약점

 후원 페이지

www.warmtogether.com

따뜻한 공동체 모임 게시판 공동체 지도 후원하기

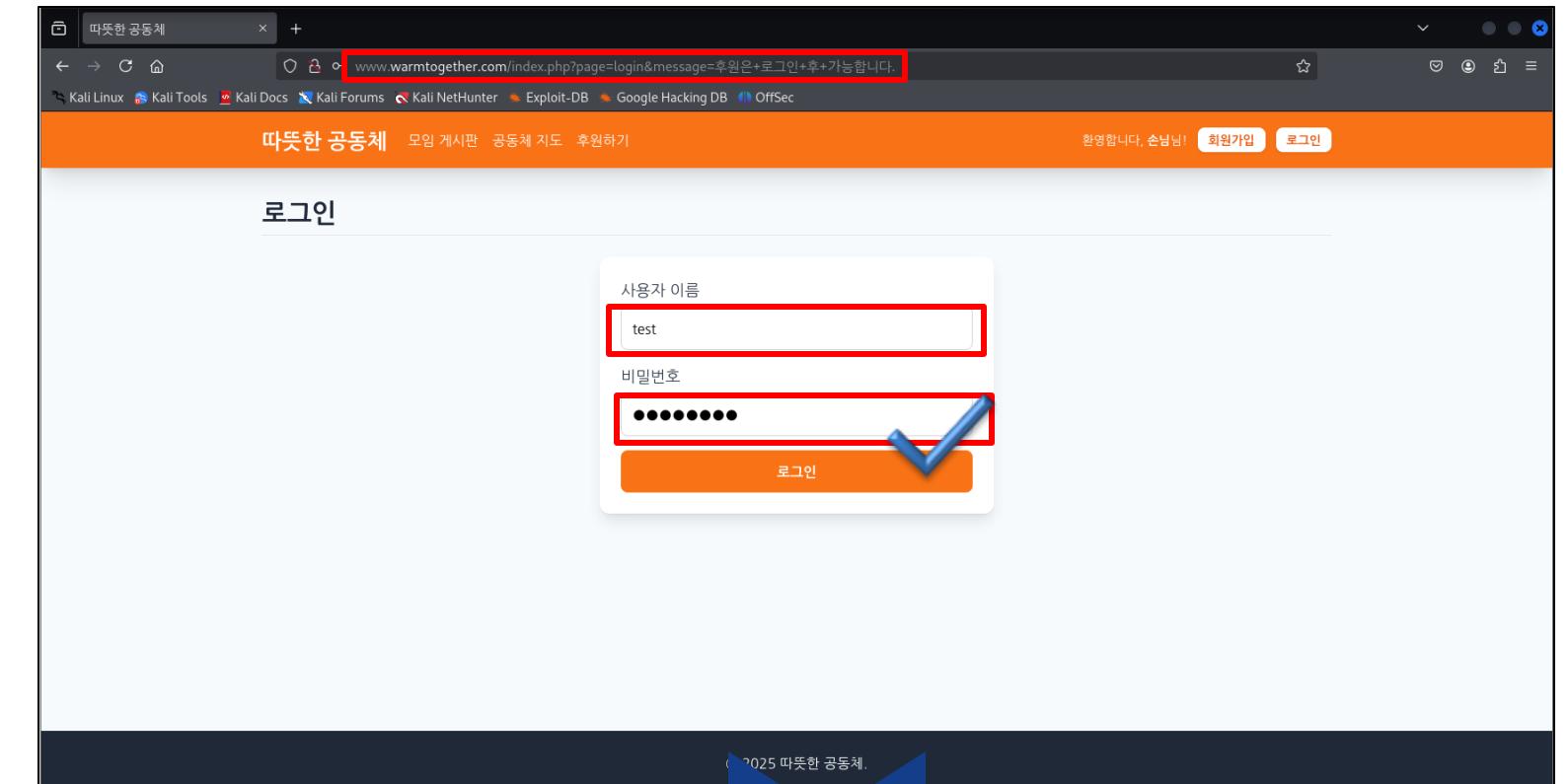
환영합니다, 손님! 회원가입 로그인

테스트 배너 [배너 이미지: /uploads/sample_banner.png] 클릭하여 자세히 보기

서로의 온기를 나누는 곳 함께 하는 소모임, 봉사, 후원 활동에 참여해보세요.

따뜻한 모임 찾아보기

© 2025 따뜻한 공동체.



www.warmtogether.com/index.php?page=login&message=후원은+로그인+후+가능합니다.

따뜻한 공동체 모임 게시판 공동체 지도 후원하기

환영합니다, 손님! 회원가입 로그인

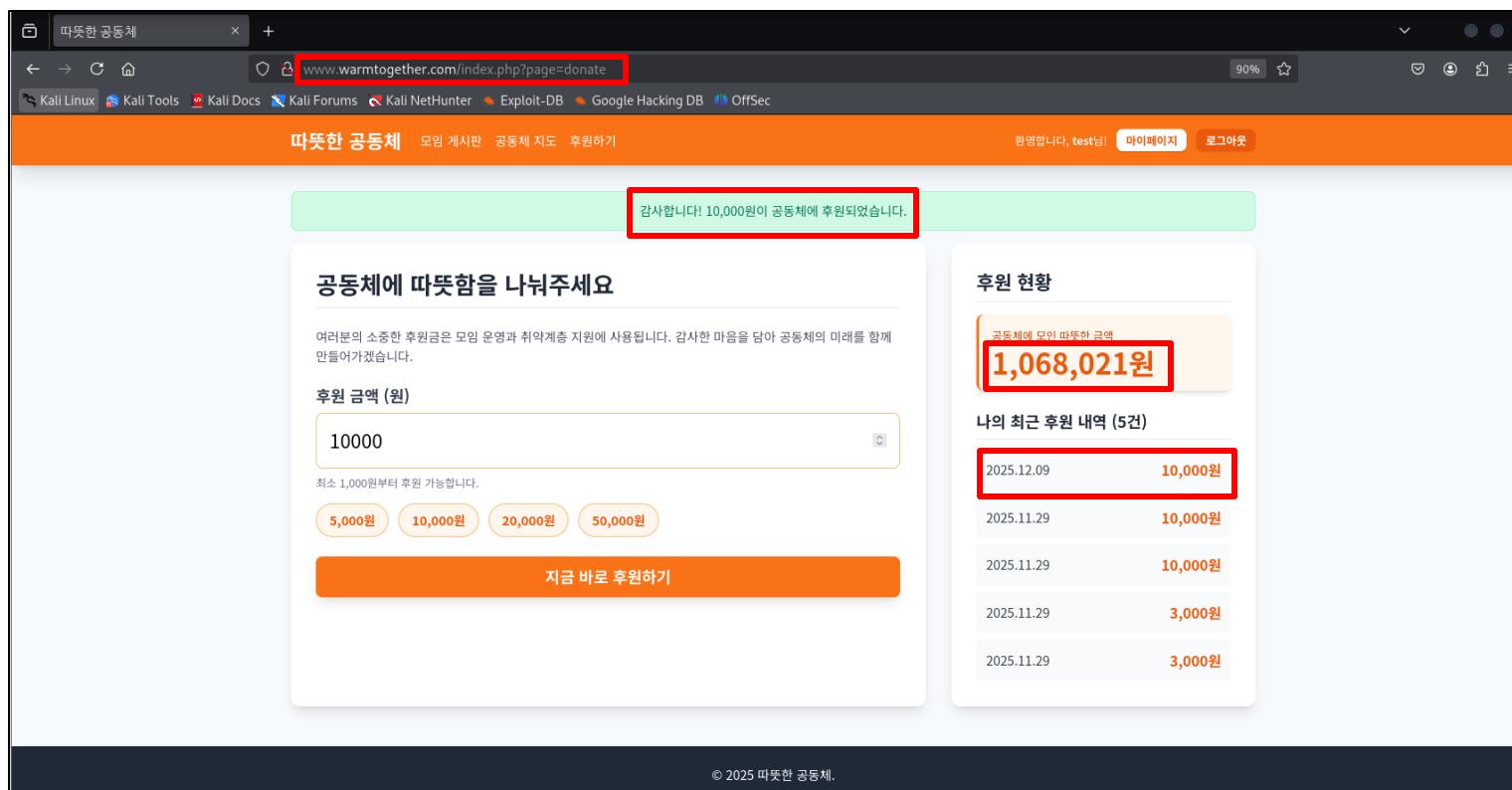
로그인

사용자 이름 test

비밀번호 *****

로그인

© 2025 따뜻한 공동체.



www.warmtogether.com/index.php?page=donate

따뜻한 공동체 모임 게시판 공동체 지도 후원하기

환영합니다, test! 마이페이지 로그아웃

감사합니다! 10,000원이 공동체에 후원되었습니다.

공동체에 따뜻함을 나눠주세요

여러분의 소중한 후원금은 모임 운영과 취약계층 지원에 사용됩니다. 감사한 마음을 담아 공동체의 미래를 함께 만들어가겠습니다.

후원 현황

공동체에 모인 따뜻한 금액 **1,068,021원**

나의 최근 후원 내역 (5건)

날짜	금액
2025.12.09	10,000원
2025.11.29	10,000원
2025.11.29	10,000원
2025.11.29	3,000원
2025.11.29	3,000원

후원 금액 (원)

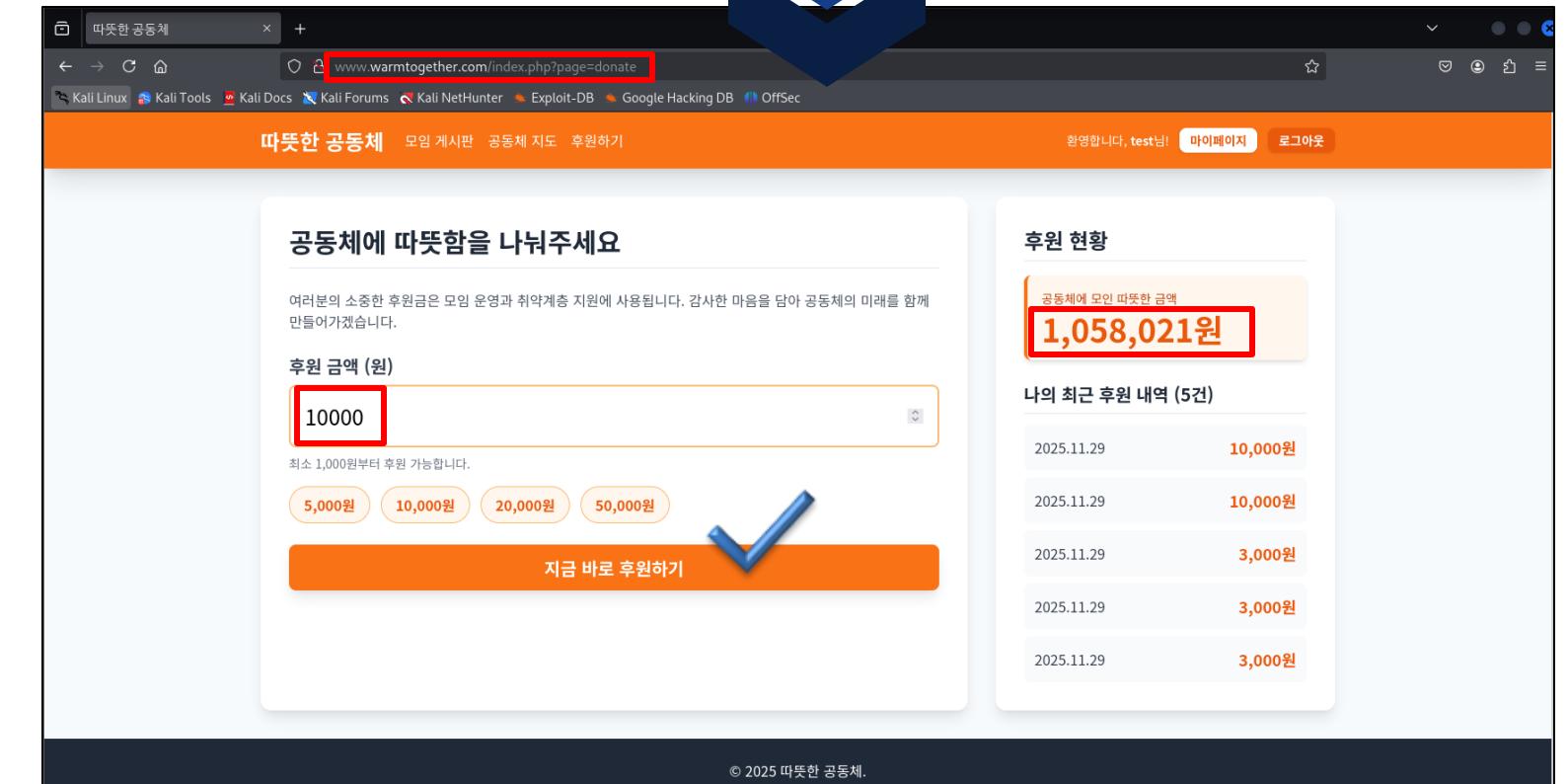
10000

최소 1,000원부터 후원 가능합니다.

5,000원 10,000원 20,000원 50,000원

지금 바로 후원하기

© 2025 따뜻한 공동체.



www.warmtogether.com/index.php?page=donate

따뜻한 공동체 모임 게시판 공동체 지도 후원하기

환영합니다, test! 마이페이지 로그아웃

공동체에 따뜻함을 나눠주세요

여러분의 소중한 후원금은 모임 운영과 취약계층 지원에 사용됩니다. 감사한 마음을 담아 공동체의 미래를 함께 만들어가겠습니다.

후원 금액 (원)

10,000

최소 1,000원부터 후원 가능합니다.

5,000원 10,000원 20,000원 50,000원

지금 바로 후원하기

공동체에 모인 따뜻한 금액 **1,058,021원**

나의 최근 후원 내역 (5건)

날짜	금액
2025.11.29	10,000원
2025.11.29	10,000원
2025.11.29	3,000원
2025.11.29	3,000원
2025.11.29	3,000원

© 2025 따뜻한 공동체.

후원 페이지

공동체에 따뜻함을 나눠주세요

여러분의 소중한 후원금은 모임 운영과 취약계층 지원에 사용됩니다. 감사한 마음을 담아 공동체의 미래를 함께 만들어가겠습니다.

후원 금액 (원)

7000

최소 1,000원부터 후원 가능합니다.

5,000원 10,000원 20,000원 50,000원

지금 바로 후원하기

후원 현황

공동체에 모인 따뜻한 금액
630,000원

나의 최근 후원 내역 (1건)
2025.11.29 600,000원

감사합니다! 7,000원이 공동체에 후원되었습니다.

공동체에 따뜻함을 나눠주세요

여러분의 소중한 후원금은 모임 운영과 취약계층 지원에 사용됩니다. 감사한 마음을 담아 공동체의 미래를 함께 만들어가겠습니다.

후원 금액 (원)

10000

최소 1,000원부터 후원 가능합니다.

5,000원 10,000원 20,000원 50,000원

지금 바로 후원하기

후원 현황

공동체에 모인 따뜻한 금액
637,000원

나의 최근 후원 내역 (2건)
2025.11.29 67,000원
2025.11.29 600,000원

▶ 입력 값 검증 미흡

1 입력 값 검증 미흡

2 서버 사이드 검증 부족

공동체에 따뜻함을 나눠주세요

여러분의 소중한 후원금은 모임 운영과 취약계층 지원에 사용됩니다. 감사한 마음을 담아 공동체의 미래를 함께 만들어가겠습니다.

후원 금액 (원)

7000

최소 1,000원부터 후원 가능합니다.

5,000원 10,000원 20,000원 50,000원

지금 바로 후원하기

630,000원

감사합니다! 67,000원이 공동체에 후원되었습니다.

나의 최근 후원 내역 (1건)

2025.11.29 67,000원

600,000원

후원 현황

697,000원

나의 최근 후원 내역 (2건)

2025.11.29 67,000원

600,000원

공동체에 따뜻함을 나눠주세요

여러분의 소중한 후원금은 모임 운영과 취약계층 지원에 사용됩니다. 감사한 마음을 담아 공동체의 미래를 함께 만들어가겠습니다.

후원 금액 (원)

7000

최소 1,000원부터 후원 가능합니다.

5,000원 10,000원 20,000원 50,000원

지금 바로 후원하기

630,000원

감사합니다! 67,000원이 공동체에 후원되었습니다.

나의 최근 후원 내역 (1건)

2025.11.29 67,000원

600,000원

후원 현황

697,000원

나의 최근 후원 내역 (2건)

2025.11.29 67,000원

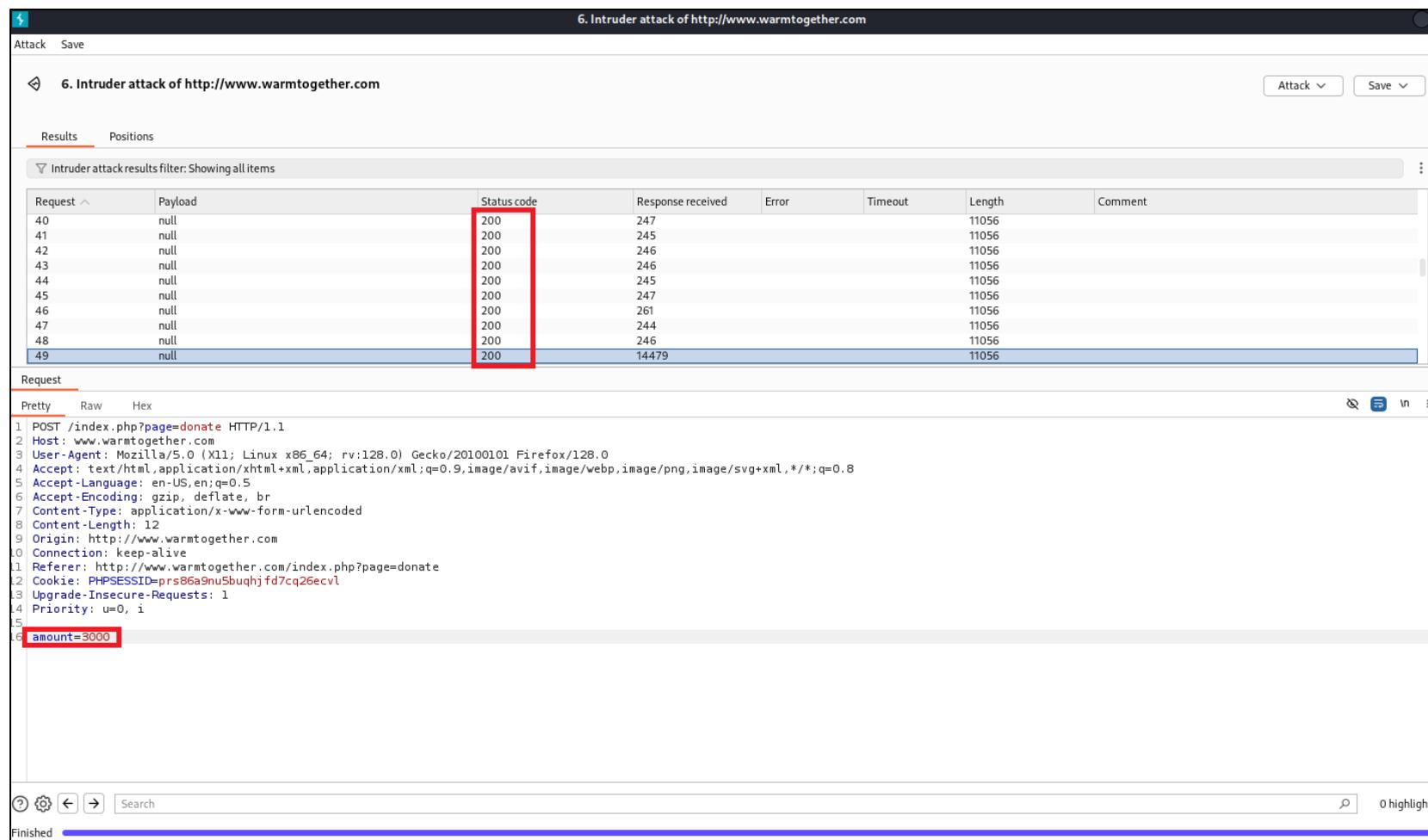
600,000원

Burp Suite Community Edition v2024.9.4 - Temporary F

Request

```
1 POST /index.php?page=donate HTTP/1.1
2 Host: www.warmtogether.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 11
9 Origin: http://www.warmtogether.com
10 Connection: keep-alive
11 Referer: http://www.warmtogether.com/index.php?page=donate
12 Cookie: PHPSESSID=prs86a9nu5buqhjfd7cq26ecvl
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 amount=67000
```

중복 요청 검증 미흡

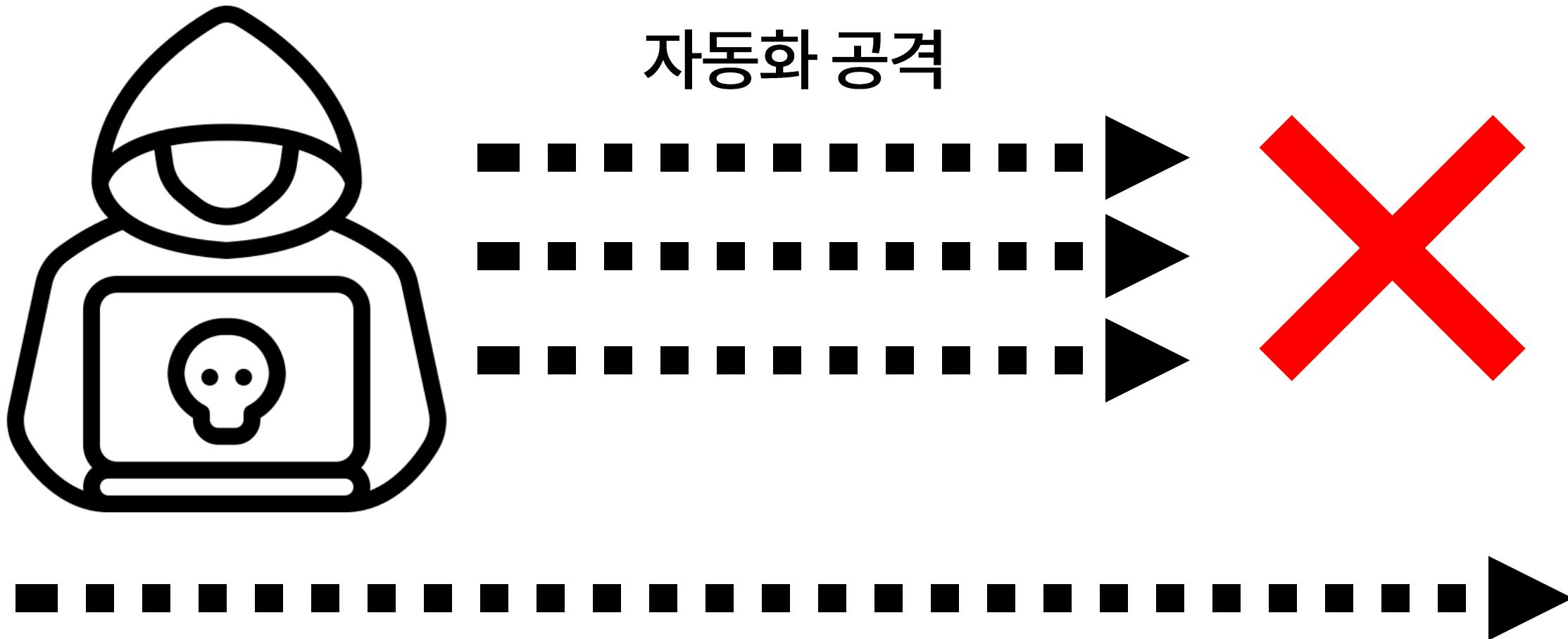


The screenshot shows the OWASP ZAP tool interface with a list of requests. The 'Status code' column is highlighted with a red box. Request 49 has a status code of 200, which is highlighted with a red box.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
40	null	200	247			11056	
41	null	200	245			11056	
42	null	200	246			11056	
43	null	200	246			11056	
44	null	200	245			11056	
45	null	200	247			11056	
46	null	200	261			11056	
47	null	200	244			11056	
48	null	200	246			11056	
49	null	200	14479			11056	

Request
Pretty Raw Hex
1 POST /index.php?page=donate HTTP/1.1
2 Host: www.warmtogether.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 12
9 Origin: http://www.warmtogether.com
0 Connection: keep-alive
1 Referer: http://www.warmtogether.com/index.php?page=donate
2 Cookie: PHPSESSID=pr86a9nu5buqhjfd7cq26ecvl
3 Upgrade-Insecure-Requests: 1
4 Priority: u=0, i
5
6 amount=3000
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
5510
5511
5512
5513
5514
5515
5516
5517
5518
5519
5520
5521
5522
5523
5524
5525
5526
5527
5528
5529
5530
5531
5532
5533
5534
5535
5536
5537
5538
5539
5540
5541
5542
5543
5544
5545
5546
5547
5548
5549
55410
55411
55412
55413
55414
55415
55416
55417
55418
55419
55420
55421
55422
55423
55424
55425
55426
55427
55428
55429
55430
55431
55432
55433
55434
55435
55436
55437
55438
55439
55440
55441
55442
55443
55444
55445
55446
55447
55448
55449
55450
55451
55452
55453
55454
55455
55456
55457
55458
55459
55460
55461
55462
55463
55464
55465
55466
55467
55468
55469
55470
55471
55472
55473
55474
55475
55476
55477
55478
55479
55480
55481
55482
55483
55484
55485
55486
55487
55488
55489
55490
55491
55492
55493
55494
55495
55496
55497
55498
55499
55500
55501
55502
55503
55504
55505
55506
55507
55508
55509
55510
55511
55512
55513
55514
55515
55516
55517
55518
55519
55520
55521
55522
55523
55524
55525
55526
55527
55528
55529
55530
55531
55532
55533
55534
55535
55536
55537
55538
55539
55540
55541
55542
55543
55544
55545
55546
55547
55548
55549
55550
55551
55552
55553
55554
55555
55556
55557
55558
55559
55560
55561
55562
55563
55564
55565
55566
55567
55568
55569
55570
55571
55572
55573
55574
55575
55576
55577
55578
55579
55580
55581
55582
55583
55584
55585
55586
55587
55588
55589
55590
55591
55592
55593
55594
55595
55596
55597
55598
55599
555100
555101
555102
555103
555104
555105
555106
555107
555108
555109
555110
555111
555112
555113
555114
555115
555116
555117
555118
555119
555120
555121
555122
555123
555124
555125
555126
555127
555128
555129
555130
555131
555132
555133
555134
555135
555136
555137
555138
555139
555140
555141
555142
555143
555144
555145
555146
555147
555148
555149
555150
555151
555152
555153
555154
555155
555156
555157
555158
555159
555160
555161
555162
555163
555164
555165
555166
555167
555168
555169
555170
555171
555172
555173
555174
555175
555176
555177
555178
555179
555180
555181
555182
555183
555184
555185
555186
555187
555188
555189
555190
555191
555192
555193
555194
555195
555196
555197
555198
555199
555200
555201
555202
555203
555204
555205
555206
555207
555208
555209
555210
555211
555212
555213
555214
555215
555216
555217
555218
555219
555220
555221
555222
555223
555224
555225
555226
555227
555228
555229
555230
555231
555232
555233
555234
555235
555236
555237
555238
555239
555240
555241
555242
555243
555244
555245
555246
555247
555248
555249
555250
555251
555252
555253
555254
555255
555256
555257
555258
555259
555260
555261
555262
555263
555264
555265
555266
555267
555268
555269
555270
555271
555272
555273
555274
555275
555276
555277
555278
555279
555280
555281
555282
555283
555284
555285
555286
555287
555288
555289
555290
555291
555292
555293
555294
555295
555296
555297
555298
555299
555300
555301
555302
555303
555304
555305
555306
555307
555308
555309
555310
555311
555312
555313
555314
555315
555316
555317
555318
555319
555320
555321
555322
555323
555324
555325
555326
555327
555328
555329
555330
555331
555332
555333
555334
555335
555336
555337
555338
555339
555340
555341
555342
555343
555344
555345
555346
555347
555348
555349
555350
555351
555352
555353
555354
555355
555356
555357
555358
555359
555360
555361
555362
555363
555364
555365
555366
555367
555368
555369
555370
555371
555372
555373
555374
555375
555376
555377
555378
555379
555380
555381
555382
555383
555384
555385
555386
555387
555388
555389
555390
555391
555392
555393
555394
555395
555396
555397
555398
555399
555400
555401

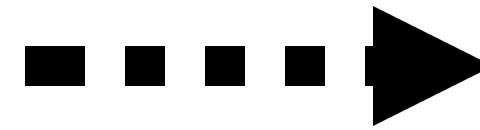
➤ 중복 요청 검증 미흡(자동화 공격) 해결 방안



- 1 CSRF 토큰 적용
- 2 Rate Limit 설정
- 3 중복 요청 방지

> 시큐어 코딩

```
/*
 * 기존
 1. CSRF 토큰 => 없음
 */
```



1 CSRF 토큰 검증을 통해 요청 위·변조 및 자동화 공격 차단

2 C후원 금액을 서버 세션 기반으로 관리하여 클라이언트 변조 방지

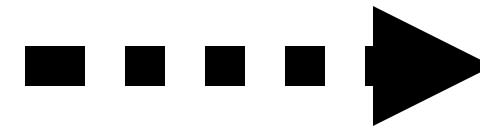
```
if (!isset($_SESSION['csrf_token'])) {
    $_SESSION['csrf_token'] = bin2hex(openssl_random_pseudo_bytes(32));
}

if (
    !isset($_POST['csrf_token']) ||
    !hash_equals($_SESSION['csrf_token'], $_POST['csrf_token'])
) {
    display_message("잘못된 요청입니다.", 'error');
    exit();
}

<form method="POST" action="index.php?page=donate">
    <input type="hidden" name="csrf_token"
           value=<?php echo htmlspecialchars($_SESSION['csrf_token']); ?>">
    <button
        type="submit"
        class="warm-btn w-full py-3 text-xl"
        <?php echo empty($_SESSION['donation_amount']) ? 'disabled' : ''; ?>
    >
        선택한 금액으로 후원하기
    </button>
</form>
```

 시큐어 코딩

```
/*
 * 기준
 1. Rate Limit => 없음
 */
```



```
$limit_seconds = 10;
$limit_count   = 3;
$now = time();

if (!isset($_SESSION['donate_rate'])) {
    $_SESSION['donate_rate'] = array();
}

$_SESSION['donate_rate'] = array_filter(
    $_SESSION['donate_rate'],
    function ($t) use ($now, $limit_seconds) {
        return $t > ($now - $limit_seconds);
});

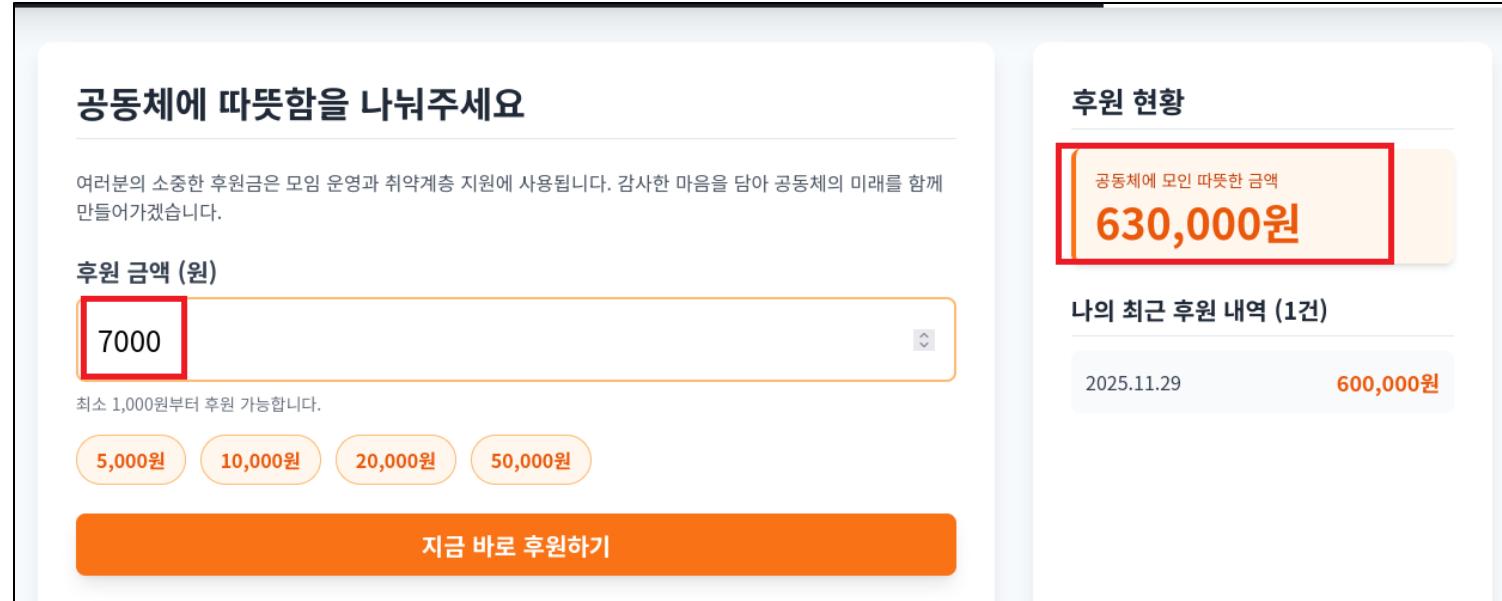
if (count($_SESSION['donate_rate']) >= $limit_count) {
    display_message("요청이 너무 많습니다. 잠시 후 다시 시도해주세요.", 'error');
    exit();
}

$_SESSION['donate_rate'][] = $now;
```

1 세션 기반 Rate Limit을 적용하여 일정 시간 내 반복적인 후원 요청 횟수를 제한

2 자동화 도구를 이용한 POST 공격 차단

중요 정보 평문 전송



공동체에 따뜻함을 나눠주세요

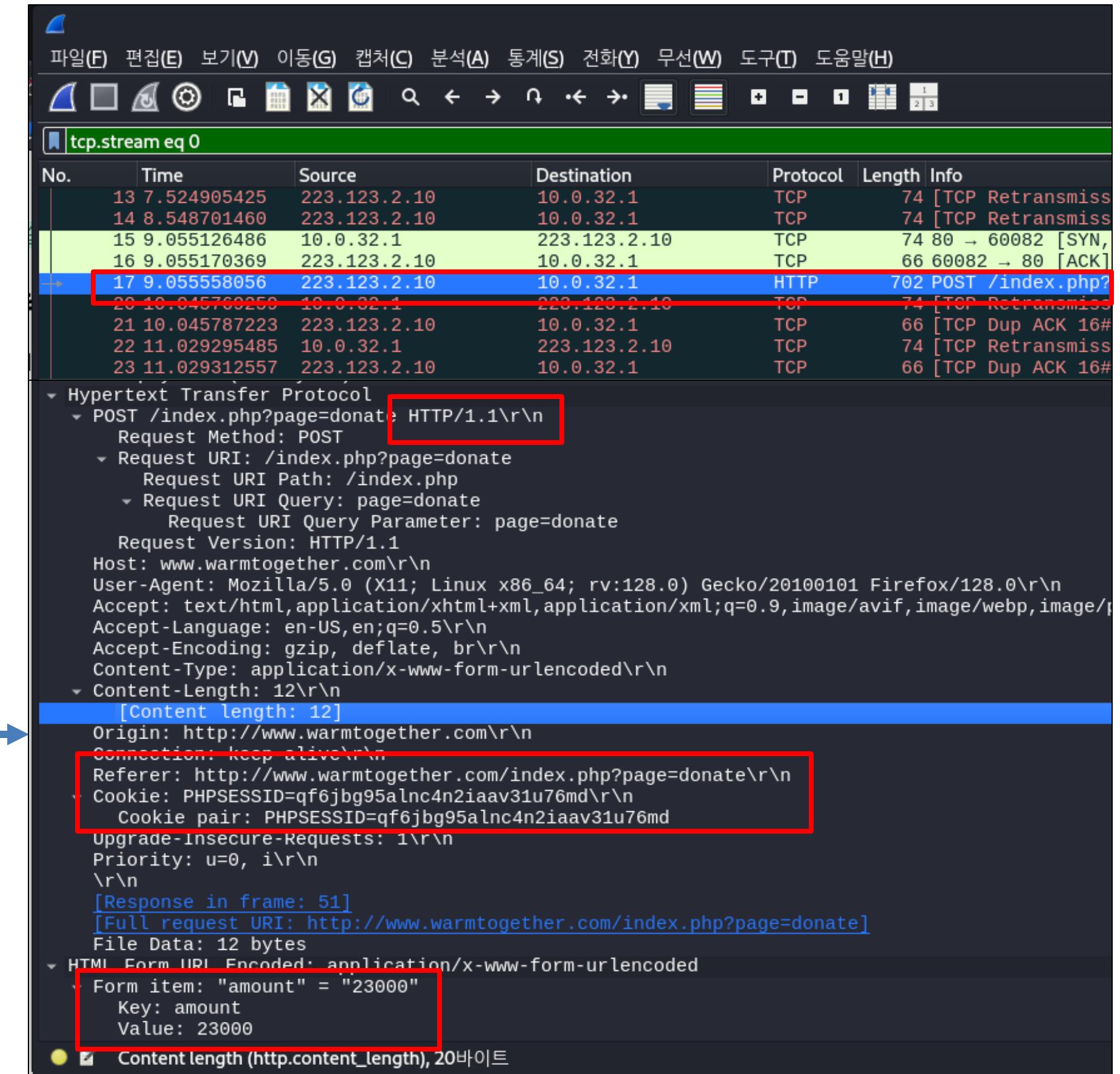
여러분의 소중한 후원금은 모임 운영과 취약계층 지원에 사용됩니다. 감사한 마음을 담아 공동체의 미래를 함께 만들어가겠습니다.

후원 금액 (원)

7000

최소 1,000원부터 후원 가능합니다.

- 1 HTTP 사용
- 2 Cookie 평문 전송
- 3 입력 값(후원 금액) 평문 전송



tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
13	7.524905425	223.123.2.10	10.0.32.1	TCP	74	[TCP Retransmiss]
14	8.548701460	223.123.2.10	10.0.32.1	TCP	74	[TCP Retransmiss]
15	9.055126486	10.0.32.1	223.123.2.10	TCP	74	80 → 60082 [SYN,
16	9.055170369	223.123.2.10	10.0.32.1	TCP	66	60082 → 80 [ACK]
17	9.055558056	223.123.2.10	10.0.32.1	HTTP	702	POST /index.php?
20	10.045760250	10.0.32.1	223.123.2.10	TCP	74	[TCP Retransmiss]
21	10.045787223	223.123.2.10	10.0.32.1	TCP	66	[TCP Dup ACK 16#]
22	11.029295485	10.0.32.1	223.123.2.10	TCP	74	[TCP Retransmiss]
23	11.029312557	223.123.2.10	10.0.32.1	TCP	66	[TCP Dup ACK 16#]

▼ Hypertext Transfer Protocol

 ▼ POST /index.php?page=donate HTTP/1.1\r\n

 Request Method: POST

 ▼ Request URI: /index.php?page=donate

 Request URI Path: /index.php

 ▼ Request URI Query: page=donate

 Request URI Query Parameter: page=donate

 Request Version: HTTP/1.1

 Host: www.warmtogether.com\r\n

 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\r\n

 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/\r\n

 Accept-Language: en-US,en;q=0.5\r\n

 Accept-Encoding: gzip, deflate, br\r\n

 Content-Type: application/x-www-form-urlencoded\r\n

 ▼ Content-Length: 12\r\n

 [Content length: 12]

 Origin: http://www.warmtogether.com\r\n

 Connection: keep-alive\r\n

 Referer: http://www.warmtogether.com/index.php?page=donate\r\n

 Cookie: PHPSESSID=qf6jbg95alnc4n2iaav31u76md\r\n

 Cookie pair: PHPSESSID=qf6jbg95alnc4n2iaav31u76md

 Upgrade-Insecure-Requests: 1\r\n

 Priority: u=0, i\r\n

 \r\n

 [Response in frame: 51]

 [Full request URI: http://www.warmtogether.com/index.php?page=donate]

 File Data: 12 bytes

 ▼ HTML Form URL Encoded: application/x-www-form-urlencoded

 Form item: "amount" = "23000"

 Key: amount

 Value: 23000

 Content length (http.content_length), 20바이트

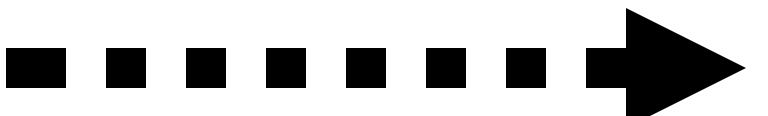
> 중요 정보 평문 전송 해결 방안



- 1 통신 암호화
- 2 Cookie 값 Secure, HttpOnly 설정
- 3 요청 시 검증을 통해 보안 강화

> 시큐어 코딩

```
// 기존 코드
session_start();
```



```
session_set_cookie_params(
    0,           // lifetime
    '/',         // path
    '',          // domain
    true,        // secure
    true         // httponly
);

session_start();
```

```
<span>
    <?= htmlspecialchars(date('Y.m.d', strtotime($donation['donation_date']))) ?>
    <!-- XSS 방지 -->
</span>
```

1 세션 쿠키에 Secure · HttpOnly 옵션을 적용

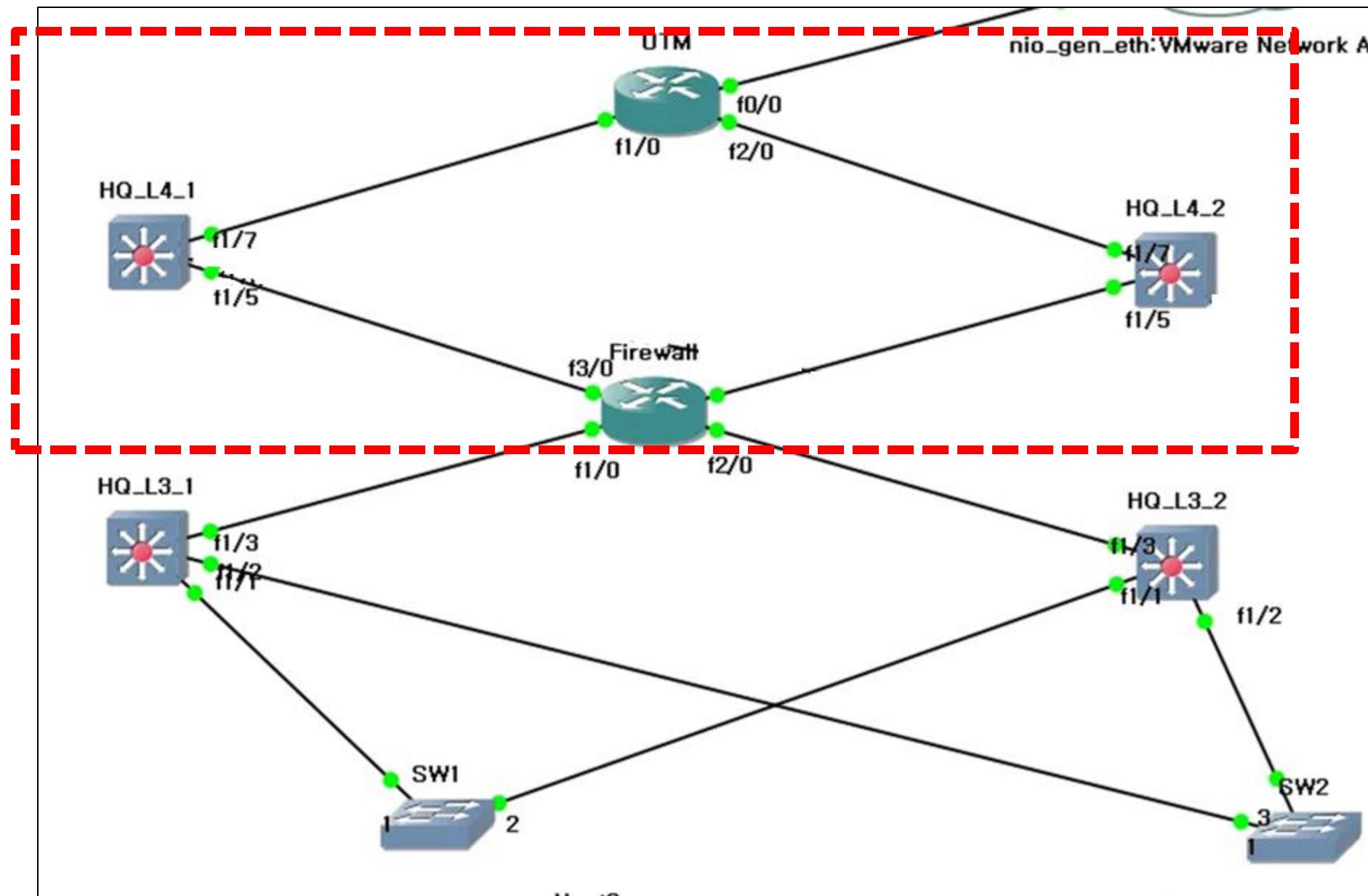
2 CSRF + Rate Limit + Prepared Statement를 결합해 자동화 공격 대응

03

개인 발표

트러블 슈팅

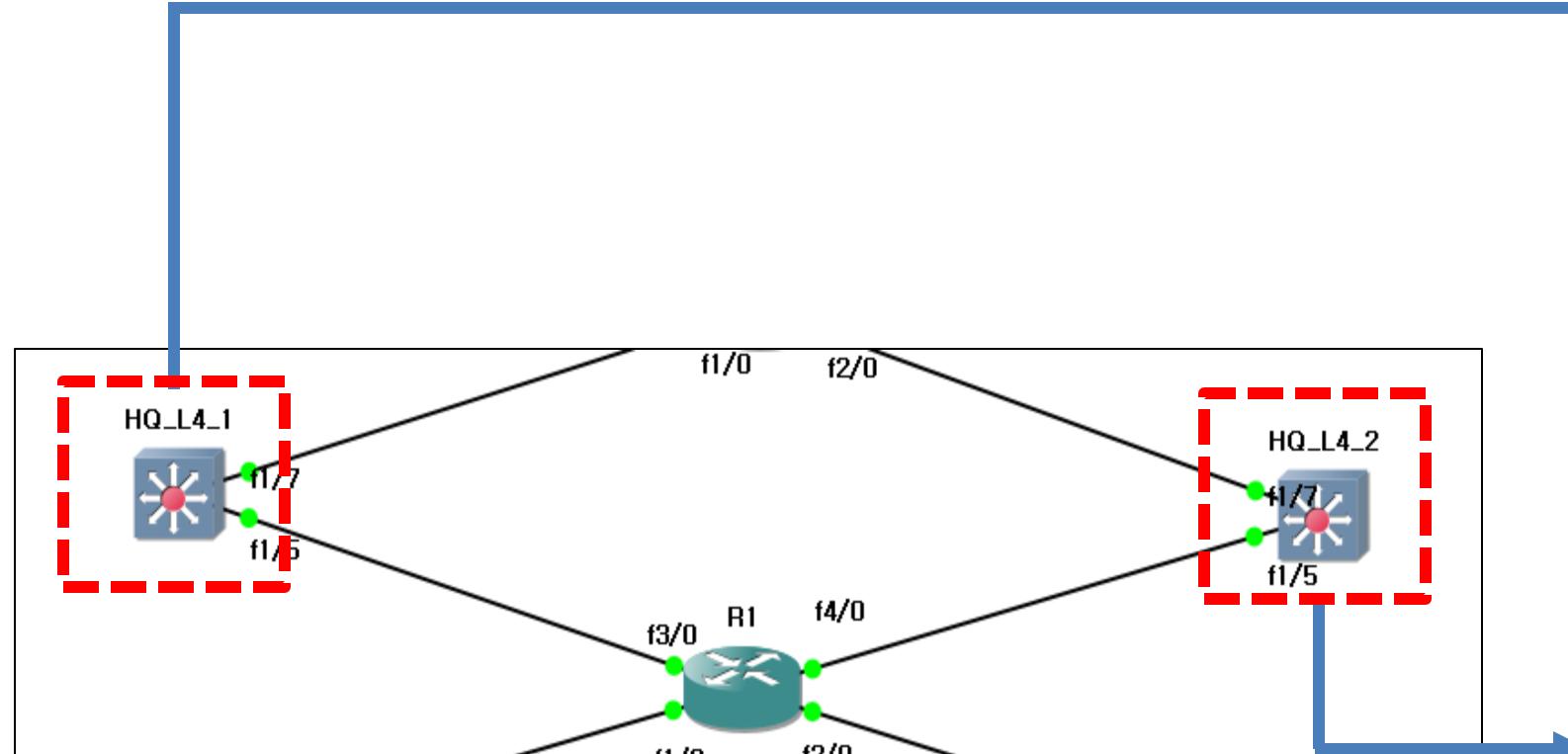
> OSPF Cost 설정



1 L4 구간은 라우팅 Core

2 OSPF Cost 기반의 경로 이중화

> HQ_L4_1/2 OSPF Cost 설정



```
HQ_L4_1#show ip ospf int bri
```

Interface	PID	Area
Fa1/5	110	0
Fa1/7	110	0

IP Address/Mask	Cost
10.0.3.9/30	10
10.0.3.2/30	10

```
HQ_L4_2#show ip ospf int bri
```

Interface	PID	Area
Fa1/5	110	0
Fa1/7	110	0

IP Address/Mask	Cost
10.0.3.13/30	50
10.0.3.6/30	50

- 1 HQ_L4_1은 cost값 10으로 주 경로로 설정

03

개인 발표

프로젝트 후 느낀 점

 프로젝트 후 느낀 점

프로젝트를 진행하며 네트워크 구축 과정에서 발생한 여러 문제를
직접 해결하며 인프라 설계와 보안의 중요성을 깊이 체감했다.

또한 PL의 역할을 맡고 프로젝트를 진행하며 문제를 해결하는 과정에서 기술 역량 뿐 아니라 소통 능력과
책임감이 요구된다는 점을 몸으로 경험했다.

이 경험을 통해 문제 해결 능력과 성취감을 얻었고, 앞으로 보안 전문가로 성장하기 위한 중요한 발판을 마련할 수 있었다.

THANK YOU