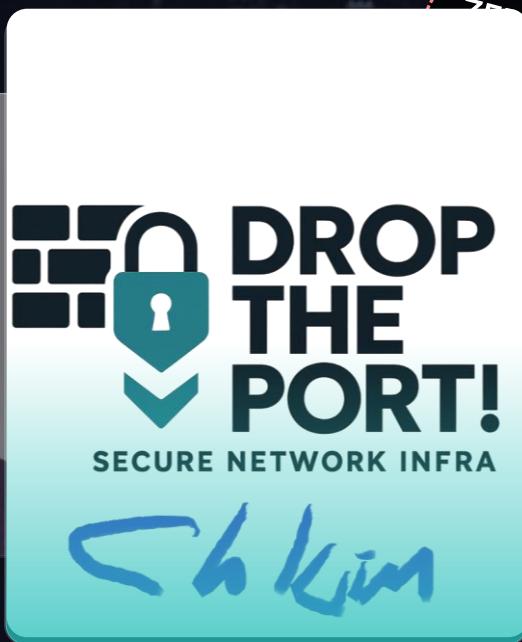


AI 해커의 시대 : 지금, 우리는 왜 ‘망분리’를 선택하는가?

• 지도교수 김충배 | 네트워크 인프라 구축 프로젝트





목차

Part 1: 프로젝트 소개

사이버 위협 배경, CB정보통신 의뢰, 요구사항 정의

슬라이드 1-10

Part 2: 시스템 설계

네트워크 아키텍처, IP 설계, 방화벽 정책, 서버 구성

슬라이드 11-22

Part 3: 구현 프로세스

WEB/DB/LOG 서버 구축, ELK Stack 구성, RAID1 설정

슬라이드 23-40

Part 4: 검증 및 성과

요구사항 검증, 정책 테스트, 성능 측정, Kibana 대시보드

슬라이드 41-48

Part 5: 프로젝트 회고

팀/개인 회고, 핵심 교훈, 망분리 한계 및 미래 전략

슬라이드 49-54



한 눈에 보기

➊ 프로젝트 기본 정보

프로젝트 명

3-Zone 보안 인프라 구축

프로젝트 부제

DROP THE PORT!

클라이언트

CB정보통신

프로젝트 기간

2025.08.21 ~ 11.03 (11주)

프로젝트 목표

사이버 위협 대응 엔터프라이즈급 보안 인프라

핵심 아키텍처

Defense in Depth 3-Zone 구조

➋ 주요 장비 구성

L3 Switch

Cisco Catalyst 3650

엔터프라이즈급 성능, VLAN 라우팅 지원, 24포트 GbE

L2 Switch

Cisco 365060 (2대)

Access Layer 표준, PoE 지원, 저렴한 가격

방화벽

AhnLab TrusGuard 50B

국내 기업 호환성, NGFW 기능, IPS/IDS 통합

기상화 플랫폼

VMware

3대 서버를 2대 물리 서버에 통합, 비용 절감

DBMS

PostgreSQL 16

엔터프라이즈급 오픈소스, 성능, 보안

➌ 기술 스택 및 성과

Cisco IOS



AhnLab
TrusGuard



PostgreSQL 16



ELK Stack



24/24

요구사항 달성

100%

원료율

11주

프로젝트 기간

3-Zone

아키텍처

프로젝트 구성 DROP THE PORT! 라인업 강화



Zero
Just

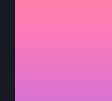
일상에 녹아있는 무분별한 접속,
지금! 우리 네트워크에도
취약점이 존재할까요?

TODAY

SUN	MON	TUE	WED	THU	FRI	SAT
02	03	04	05	06	07	08



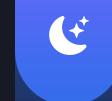
아침 출근 후
실시간 **인터넷뉴스** 보며 커피 한 잔



점심 식사 중
이메일 하나하나 클릭하며 확인 중



오후
습관적 **유튜브** 나 **웹툰(무료)** 보기



하루 마무리, 퇴근
쇼핑 사이트 구경하기

공격력이 더 강력해진 해커들

개인정보 침해
사고 관련
비용

| 개인정보 유출 과정금

[출처] 시장조사업체 유로모니터



| 솔루션 DLP 비용 시장

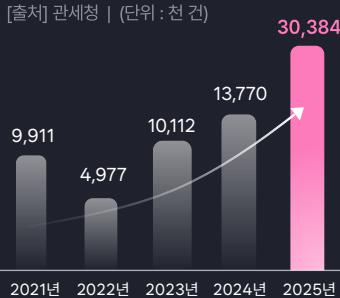
[출처] 얼리어드 마켓 리서치, KOTRA



개인정보
보호위원회
자료

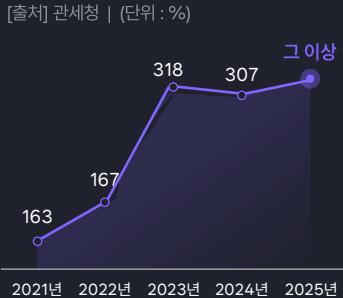
| 개인정보 유출 건수

[출처] 관세청 | (단위 : 천 건)



| 개인정보 유출 기관수

[출처] 관세청 | (단위 : %)



위협 동향

지속적인 방어막 붕괴

[출처] KISA 보고서 2021-2025

랜섬웨어 1.3배 ↑

#23일 복구 #불확실

랜섬웨어 공격 34% 증가 (KELA, 2025년 10월)

대표공격 3위 ↑

#OWASP #injection

SQL Injection으로 시작되는 랜섬웨어 73% (R. Mulki, 2025년)

SIEM 플랫폼 ↑

#인지능력 #내부 유출

SIEM 플랫폼 사용 시 보안 사고 35% 더 탐지 (ESG Research, 2024)

솔루션 비용 고가 ↑

#중소기업은? #보안인력

평균 복구 비용 273만 달러 (SentinelOne, 2025년 8월)



요구사항 정의

24개 요구사항을 4가지 카테고리로 분류



기능적 요구사항

- F-01: 네트워크 영역 분리 (External/DMZ/Internal)
- F-02: NAT 구성 (SNAT/DNAT)
- F-03: WEB 서버 구축 (Apache2, PHP)
- F-04: DB 서버 구축 (PostgreSQL 16 + DBeaver)
- F-05: LOG 서버 구축 (ELK Stack)
- F-06: Hostname 설정
- F-07: VLAN 구성 (10/20/30)
- F-08: 라우팅 설정

8개



비기능적 요구사항

- N-01: RAID1 LOG 서버 구성
- N-02: NTP 시간 동기화
- N-03: 장비 초기화 설정
- N-04: Hostname 설정
- N-05: Netplan 설정

5개



보안 요구사항

- S-01: 방화벽 접근제어 정책 (12개)
- S-02: NAT 정책 설정
- S-03: 악성 IP 차단 (210.95.199.0/24)
- S-04: VLAN 간 격리
- S-05: DB 서버 iptables 설정
- S-06: 관리자 IP 제한 (192.168.10.0/24)
- S-07: 로그 중앙화 모니터링

7개



성능 요구사항

- P-01: VLAN 간 지연 시간 < 5ms
- P-02: 패킷 손실률 0%
- P-03: SPAN 포트 미러링
- P-04: RAID1 가용성 99.9%

4개



기능적/비기능적 요구사항

F-01~08, N-01~05 | 시스템 구축의 핵심 요구사항

⚙️ 기능적 요구사항 (F-01~08)

F-01	네트워크 영역 분리 (3-Zone 구성)	★★★
F-02	NAT 구성 (SNAT/DNAT)	★★★
F-03	WEB 서버 구축 (Apache2, PHP)	★★
F-04	DB 서버 구축 (PostgreSQL 16 + DBeaver)	★★
F-05	LOG 서버 구축 (ELK Stack)	★★
F-06	호스트네임 설정 (규칙적 명명)	★★
F-07	VLAN 구성 (10, 20, 30)	★★★
F-08	라우팅 설정 (정적/동적)	★★

🛡️ 비기능적 요구사항 (N-01~05)

N-01	RAID1 LOG 서버 (중복성 보장)	★★★
N-02	NTP 시간 동기화 (정확한 시간)	★★★
N-03	장비 초기화 (보안 설정 초기화)	★★
N-04	호스트네임 설정 (규칙적 명명)	★★
N-05	Netplan 설정 (네트워크 인터페이스)	★★



보안 및 성능 요구사항

S-01~07, P-01~03 | 시스템 구축의 안전관련 사항

🔒 보안 요구사항 (S-01~07)

S-01	방화벽 접근제어 정책	(12개 정책)	★★
S-02	NAT 정책 설정 (SNAT/DNAT)		★★★
S-03	악성 IP 차단	(210.95.199.0/24)	★★★
S-04	VLAN 간 격리 (트래픽 분리)		★★
S-05	DB 서버 iptables 방화벽 설정		★★
S-06	관리자 IP 제한	(192.168.10.0/24)	★★★
S-07	로그 중앙화 모니터링 (ELK Stack)		★★

🌀 성능 요구사항 (P-01~04)

P-01	VLAN 간 지연 시간	< 5ms	★
P-02	패킷 손실률	0%	★★
P-03	SPAN 포트 미러링	(네트워크 모니터링)	★★



DROP THE PORT!

4인 인프라 전문팀 "Drop the Port!"

NETWORK

허준혁 (Netty)

Switch 설정, VLAN 구성, 네트워크 모니터링, NAT 구성, RAID1 구성

FIREWALL

이송하 (Poly)

AhnLab TrusGuard 50B, 정책 설정, LOG 수집, 보안 정책 관리

SYSTEM

이재민 (Sisy)

WEB/DB/LOG 서버 구축, 서비스 운영, 백업 관리

PM

서상원 (PM)

프로젝트 관리, 일정 조율, 문서화, 리스크 관리



9주차 이후: All-Rounder 로테이션 훈련

네트워크/방화벽/시스템 역할 교차 학습, 2주간 순환, 전체 시스템 이해도 향상



■ 11주간의 긴밀한 협업 체계



팀 미팅 및 협업

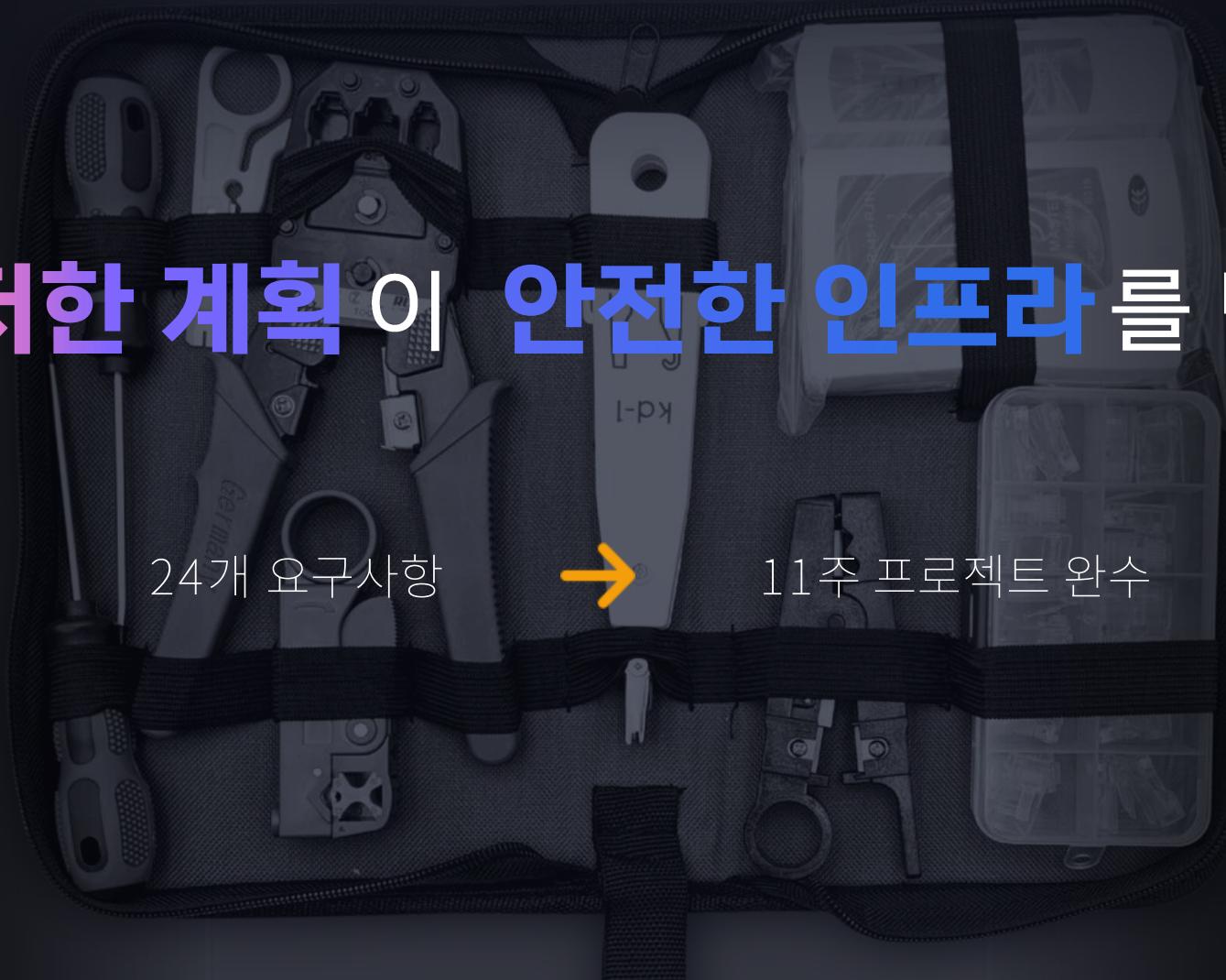
- 주 2회 정기 미팅
- 실시간 협업 도구 사용
- 즉각적인 피드백 시스템
- 역할별 전문성 공유

철저한 계획이 안전한 인프라를 만든다

24개 요구사항



11주 프로젝트 완수





프로젝트 타임라인 (11주 WBS)

Gantt 차트로 표현한 주차별 단계별 진행 상황

Week 1 Week 2 Week 3 Week 4 Week 5 Week 6 Week 7 Week 8 Week 9 Week 10 Week 11

설계

설계 단계

네트워크 구성

네트워크 구성

방화벽 구축

방화벽 구축 및 ELK 작업 수행

서버 구축

서버 구축 및 웹페이지 연동

로테이션 훈련

로테이션 훈련

통합 테스트

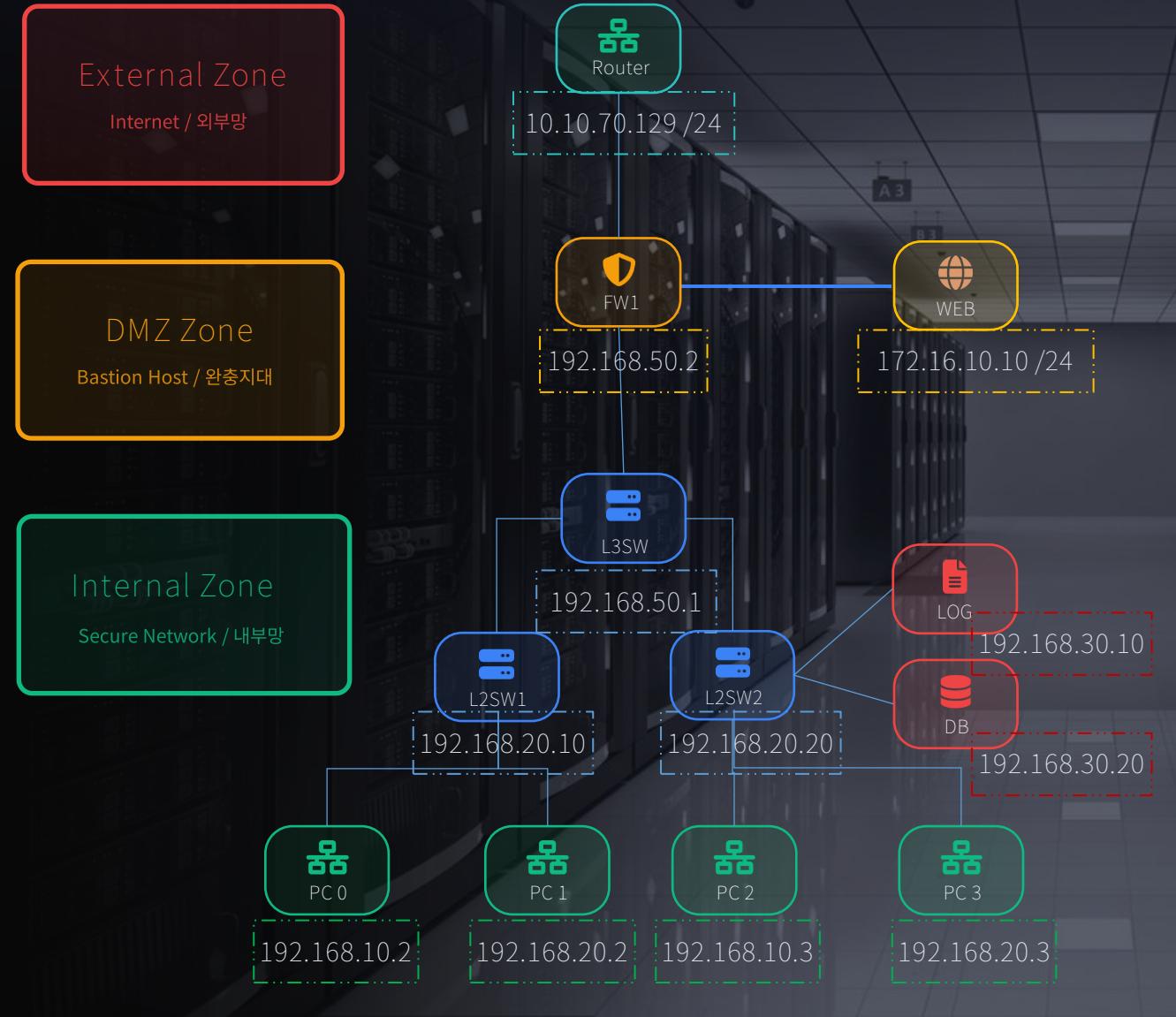
통합 테스트

증진평가 피드백

최종 발표

3-Zone 망분리 (Defense in Depth)

방화벽 2단계 방어: 외부→DMZ, DMZ→내부



3-Zone 망분리 개념

External(외부망) ↔ DMZ(완충지대) ↔ Internal(내부망) 구조

DMZ에 공개 서비스(WEB) 배치, 내부망에 중요 자원 보호

WEB 서버 공격 시에도 DB 직접 침투 불가

KISA 권고: 중요정보 취급 시 물리적 망분리 필수

출처: Fortinet (2024), KISA 보안 가이드

IP 주소 설계

네트워크 구역별 IP 할당 계획 - 3-Zone 아키텍처



i VLAN (Virtual LAN) 개념

- ✓ VLAN
 - : Virtual LAN, 논리적 네트워크 분할 기술
- ✓ 브로드캐스트 도메인 분리
 - : 각 VLAN은 독립적인 브로드캐스트 도메인
- ✓ 보안 효과
 - : 침해 발생 시 다른 VLAN으로 확산 차단
- ✓ 관리 효율
 - : 논리적 세그먼테이션 네트워크 관리 용이

아키텍처 설계 근거 - VLAN/IP/CIDR

네트워크 설계 핵심 요소들



VLAN 3개 구성 이유

- 3-Zone 보안 모델 표준 - External/DMZ/Internal 구분
- 4개 VLAN 시 관리 복잡도 · 라우팅 오버헤드 증가 (ACL/정책 매트릭스 폭증)
- 공개·준공개·비공개 경계가 선명해 운영·감사 (컴플라이언스) 용이
- 관리/백업 VLAN은 규모 확대 시 Phase 2로 분리 계획



IP 주소 체계 설계 근거

- L3 Switch ↔ Firewall 링크는 2호스트만 필요 (10.10.70.0/30)
- DMZ는 웹 서버용, Class B로 충분한 주소 공간
- Internal은 역할별 분리로 가시성/제어성 향상

External	10.10.70.0/24
DMZ	172.16.10.0/24
Internal DB	192.168.10.0/24
Internal LOG	192.168.20.0/24



CIDR /30 선택 이유

- External Zone - Point-to-Point 연결
- 2개 인터페이스: L3 Switch ↔ Firewall 직접 연결
- /30 = 정확히 2호스트, 주소 효율성·보안성 동시 확보

L3 Switch Interface
10.10.70.1/30



Firewall Interface
10.10.70.2/30

서버 분리 구성 근거

네트워크 영역별 역할 분담과 보안 계층화



External Zone

인터넷 연결 구간

- L3 Switch (10.10.70.1) ↔ Firewall (10.10.70.2)
- P2P 링크, 2개 인터페이스 사용



DMZ (VLAN 10)

경계 보안 영역

- WEB 서버만 존재
- 외부 트래픽 종단 및 보안 게이트웨이 연계



Internal Zone

내부 보안 영역

- VLAN 20 (192.168.10.0/24): DB 서버
- VLAN 30 (192.168.20.0/24): LOG 서버 (ELK)
- 서버팜 구간, 민감 데이터 보호



분리 목적 및 효과

- Defense in Depth (계층 방어): 침해 확산 방지 (DMZ 침해 시 Internal 격리)
- 성능 분리: 웹 트래픽 스파이크가 DB/LOG에 미치는 영향 최소화
- 변경/배포 리스크 격리 및 장애 도메인 축소

통합하지 않은 이유

- 단일 장애점 (SPOF), 보안 영역 혼재
- CPU/메모리 경합, 확장성 제한 발생
- 성능 병목, 보안 통제 어려움



왜 그랬을까? Q&A

- Q: 왜 서버팜을 Internal에? A: DMZ는 외부 노출 최소화, DB/LOG는 민감 데이터 보호 필요
- Q: VLAN 30에 DB와 LOG를 함께? A: 역할별 분리로 가시성 향상, 필요 시 VLAN 40 분리 가능
- Q: 서버 3대 비용? A: VMware 가상화로 1물리→3VM 구성, vCPU<150% · RAM<120% 오버커밋
- Q: 서버 간 지연? A: 내부 VLAN L3 라우팅 기준 평균 RTT 2.3ms (목표 <5ms)
- Q: VLAN 4개가 더 안전한가? A: 관리/백업 VLAN은 Phase 2에 분리 예정, 현 규모·정책 복잡도 기준 3개가 최적

네트워크 장비 구성

Part 2: 설계

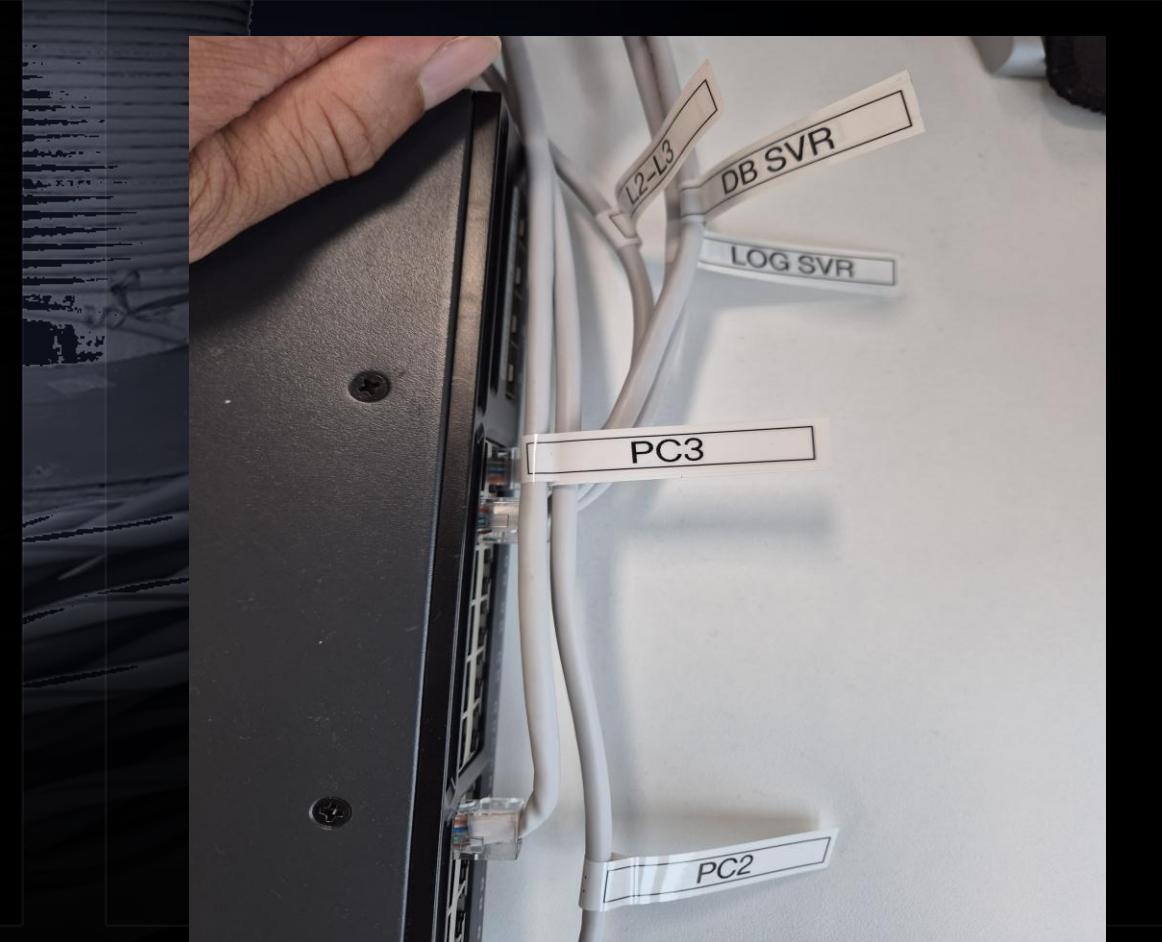
물리 인프라 구성 및 배치 현황



L3/L2 스위치 스택 구성



케이블 라벨링 및 연결



정규화 라벨링

RFC 1178 기준 - 일관성, 식별성, 확장성, 관리성

명명 규칙 설명

형식: [기관코드]-[호실]-[장비유형]-[번호]

예시: DJPT-GR312-L2SW-01

RFC 1178 기준

IETF 표준: 일관성·식별성·확장성·관리성 강화
컴퓨터 이름 선택 가이드라인 준수

표기 규칙

소문자, 하이픈(-) 구분, 의미 있는 축약

L3sw = Layer 3 Switch, L2sw = Layer 2 Switch

네이밍 키

djpt=대전폴리텍, gr312=312호실, l3sw/l2sw/fw/web/db/log=장비유형, 01~99=번호

출처: RFC 1178 - Choosing a Name for Your Computer (IETF, 1990)

프로젝트 장비 라벨링

djpt-gr312-13sw-01

Cisco C3650 L3 Switch

L3 Core

djpt-gr312-12sw-01

Cisco 2960 L2 Switch #1

Access

djpt-gr312-12sw-02

Cisco 2960 L2 Switch #2

Access

djpt-gr312-fw-01

AhnLab TrusGuard 50B

Security

djpt-gr312-web-01

Apache2 WEB 서버

Service

djpt-gr312-db-01

PostgreSQL 16 DB 서버

Service

djpt-gr312-log-01

ELK Stack LOG 서버

Service

L3 Switch CLI 설정 (1)

Part 2: 설계

Cisco C3650 - Core Switch 구성

직접 타이핑한 CLI 명령어

! L3 Switch 초기 설정 - 직접 입력

```
hostname djpt-gr312-l3sw-01
```

! VLAN 생성 및 SVI 설정

```
vlan 10, 20, 30
```

```
interface Vlan10
```

```
ip address 172.16.10.1 255.255.255.0
```

```
no shutdown
```

```
interface Vlan20
```

```
ip address 192.168.10.1 255.255.255.0
```

```
no shutdown
```

```
interface Vlan30
```

```
ip address 192.168.20.1 255.255.255.0
```

```
no shutdown
```

설정 검증

```
DJPT-GR312-L3SW-01(config)#interface range Gig1/0/23-24  
DJPT-GR312-L3SW-01(config-if-range)#switchport mode trunk  
DJPT-GR312-L3SW-01(config-if-range)#no shutdown  
DJPT-GR312-L3SW-01(config-if-range)#exit  
DJPT-GR312-L3SW-01(config)#[
```

VLAN 10, 20, 30 생성 확인

SVI 인터페이스 UP 상태

IP 주소 할당 완료

L3 라우팅 활성화

! L3 Switch는 각 VLAN 간 라우팅을 담당하며, 외부 네트워크로의 출구를 제공합니다.

L3 Switch CLI 설정 (2)

Cisco C3650 - Core Switch 구성



직접 타이핑한 CLI 명령어

```
! L3 라우팅 기능 활성화 (필수)
ip routing
```

```
! 기본 라우트 설정
```

```
ip route 0.0.0.0 0.0.0.0 10.10.70.254
```

```
! 설정 저장
```

```
exit
```

```
write memory(copy r s)
```

```
! 설정 검증
```

```
show vlan brief
```

```
show ip interface brief
```



설정 검증

```
DJPT-GR312-L3SW-01(config)#interface vlan 10
DJPT-GR312-L3SW-01(config-if)#ip address 192.168.10.1 255.255.255.0
DJPT-GR312-L3SW-01(config-if)#no shutdown
DJPT-GR312-L3SW-01(config-if)#exit
DJPT-GR312-L3SW-01(config)#interface vlan 20
DJPT-GR312-L3SW-01(config-if)#ip address 192.168.20.1 255.255.255.0
DJPT-GR312-L3SW-01(config-if)#no shutdown
DJPT-GR312-L3SW-01(config-if)#exit
DJPT-GR312-L3SW-01(config)#interface vlan 30
DJPT-GR312-L3SW-01(config-if)#ip address 192.168.30.1 255.255.255.0
DJPT-GR312-L3SW-01(config-if)#no shutdown
DJPT-GR312-L3SW-01(config-if)#exit
DJPT-GR312-L3SW-01(config)#ip routing
DJPT-GR312-L3SW-01(config)#[ ]
```

VLAN 10, 20, 30 생성 확인

SVI 인터페이스 UP 상태

IP 주소 할당 완료

L3 라우팅 활성화

! L3 Switch는 각 VLAN 간 라우팅을 담당하며, 외부 네트워크로의 출구를 제공합니다.

L2 Switch CLI 설정

Cisco C3650 - Access Layer 구성



직접 타이핑한 CLI 명령어

```
! L2 Switch 초기 설정
hostname djpt-gr312-l2sw-01

! 트렁크 포트 설정
interface GigabitEthernet0/1
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 99

! 액세스 포트 설정 (VLAN 10)
interface
switchport mode range GigabitEthernet0/2-12
switchport access vlan access
spanning-tree portfast 10

! 활성화
exit

write memory
```



설정 검증 (캡쳐본 일부 예정)

```
DJPT-GR312-L2SW-02(config)#interface range Gig1/0/1-10
DJPT-GR312-L2SW-02(config-if-range)#switchport mode access
DJPT-GR312-L2SW-02(config-if-range)#switchport access vlan 10
DJPT-GR312-L2SW-02(config-if-range)#no shutdown
DJPT-GR312-L2SW-02(config-if-range)#exit
DJPT-GR312-L2SW-02(config)#interface range Gig1/0/11-20
DJPT-GR312-L2SW-02(config-if-range)#switchport mode access
DJPT-GR312-L2SW-02(config-if-range)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
DJPT-GR312-L2SW-02(config-if-range)#no shutdown
DJPT-GR312-L2SW-02(config-if-range)#exit
DJPT-GR312-L2SW-02(config)#interface range Gig1/0/21-23
DJPT-GR312-L2SW-02(config-if-range)#switchport mode access
DJPT-GR312-L2SW-02(config-if-range)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
DJPT-GR312-L2SW-02(config-if-range)#no shutdown
DJPT-GR312-L2SW-02(config-if-range)#exit
DJPT-GR312-L2SW-02(config)#interface Gig1/0/24
DJPT-GR312-L2SW-02(config-if)#switchport mode trunk
DJPT-GR312-L2SW-02(config-if)#no shutdown
DJPT-GR312-L2SW-02(config-if)#[ ]
```

트렁크 포트 1개 활성

액세스 포트 11개 활성

VLAN 10, 20, 30 통과

STP PortFast 적용

! L2 Switch는 Access Layer에서 VLAN 세그먼테이션을 제공하며, L3 Switch와 트렁크 연결합니다.

방화벽 아키텍처 - AhnLab TrusGuard 50B

SPECS AhnLab TrusGuard 50B

모델: TrusGuard 50B

처리량: 1Gbps

세션: 50,000 Concurrent

인터페이스: 4 포트

배치: L3 Gateway

위치: DMZ-Internal 경계

핵심 기능

SNAT
내부→외부 변환

DNAT
외부→내부 변환

ACL
접근제어 12정책

네트워크 역할

DMZ-Internal 경계 보안, 트래픽 필터링, 악성 IP 차단, 관리자 접근 제한, VLAN 간 통신 제어

방화벽 구성 다이어그램

External → DMZ → Internal

- SNAT: 192.168.10.x → 10.10.70.254
- DNAT: 10.10.70.1 → 172.16.10.10
- ACL: 12개 정책, 악성 IP 차단

🛡️ 24시간 보안 모니터링

AhnLab TrusGuard 50B 선택 근거

- 국내 중소기업 최적화: 한국형 위협 대응, 한글 UI, 현지 기술지원
- 통합 보안: NGFW + IPS + VPN + Anti-virus + Anti-spam
- 2024 TTA 우수상: 한국정보통신기술협회 TTA 테스팅 인증
- 합리적 가격: 동급 대비 30% 저렴한 TCO

⚠️ 약점: 글로벌 점유율 낮음

→ 향후 Palo Alto/Fortinet/Cisco 3대 NGFW 업그레이드 검토

출처: AhnLab 공식 (2024.12), G2 Reviews

방화벽 접근제어 정책 (12개)

Part 2: 설계

No/Name/Source/Destination/Service/Action | 색상 코딩: Red-차단, Green-허용, Yellow-제한

No	정책명	Source	Destination	Service	Action
0	기본 차단	Any	Any	Any	차단
1	관리자 접근 허용	192.168.10.0/24	Any	SSH, HTTPS	허용
2	악성 IP 차단	210.95.199.0/24	Any	Any	차단
3	DMZ WEB 서버 허용	Any	172.16.10.10	HTTP, HTTPS	허용
4	DB 서버 접근 제한	172.16.10.0/24	192.168.10.20	MySQL	허용
5	DMZ → Internal 차단	172.16.10.0/24	192.168.10.0/24	Any	차단
6	LOG 서버 접근 허용	192.168.10.0/24	192.168.20.10	Syslog, 514	허용
7	NTP 서비스 허용	Any	Any	NTP, 123	허용
8	DNS 서비스 허용	Any	Any	DNS, 53	허용
9	SNMP 차단	Any	Any	SNMP, 161/162	차단
10	SSH 브루트포스 제한	Any	Any	SSH, 22	제한
11	로그 기록 정책	Any	Any	Any	로그

AhnLab TrusGuard 패킷 필터링 정책

12개 정책 전체 화면 - 네트워크 보안 정책 관리

Part 2: 설계

AhnLab TrusGuard

Dashboard Monitor Center Object Policy Security Profiles VPN Network System

검색 조건 추가

도구 더보기 일괄변경

No.	출발지	목적지	서비스	처리 방법	일정
0	BLK_IP_LIST	all	all	차단	always
1	WEB_SVR	DB_SVR	/DB_SERVICE	허용	always
2	FW_IN	LOG_SVR	/SYSLOG_SERVICE	허용	always
3	all	WEB_SVR	/DNS_SERVICE /WEB_SERVICE	허용	always
4	INT_USERS...	WEB_SVR	/DNS_SERVICE /WEB_SERVICE	허용	always
5	SVR_FARM_G...	all	all	차단	always
6	ADMIN_PC	AN_SVR DB_SVR LOG_SVR WEB_SVR	/SSH_ADMIN_SER...	허용	always
7	all	AN_SVR DB_SVR LOG_SVR WEB_SVR	/SSH_ADMIN_SER...	차단	always
8	AN_SVR DB_SVR LOG_SVR WEB_SVR	AN_SVR	/ELK_SERVICE	허용	always
9	OUT_NTP_SVR	DJPT-GR312...	/NTP_SERVICE	허용	always
10	WEB_SVR	all	/DNS_SERVICE /WEB_SERVICE	허용	always
11	INT_USERS...	all	/DNS_SERVICE /WEB_SERVICE	허용	always
12	all	all	all	차단	always

정책 설계 취지

보안 정책 관리

- ✓ 3-Zone 망분리 강화
- ✓ 악성 IP 차단
- ✓ 내부 트래픽 최소 권한 원칙
- ✓ 관리자 접근 제한

i s20 vs s30 차이점

s20: 정책 설계 테이블 (논리적 구조)
s30: 실제 GUI 구현 (구현 관점)

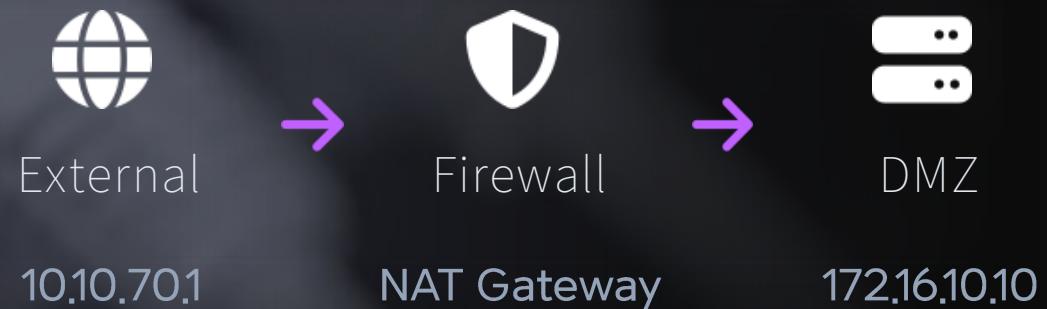
NAT 설정 (SNAT/DNAT)

네트워크 주소 변환 - 2단계 보안 구성

↔ SNAT (Source NAT)



↔ DNAT (Destination NAT)



</> SNAT 설정 예시

```
! 내부 네트워크 → 외부 인터넷
source-nat 192.168.10.0/24
to 10.10.70.254
```

```
! 내부 네트워크의 사설 IP를 외부 공인 IP로 변환
interface external
enable snat
```

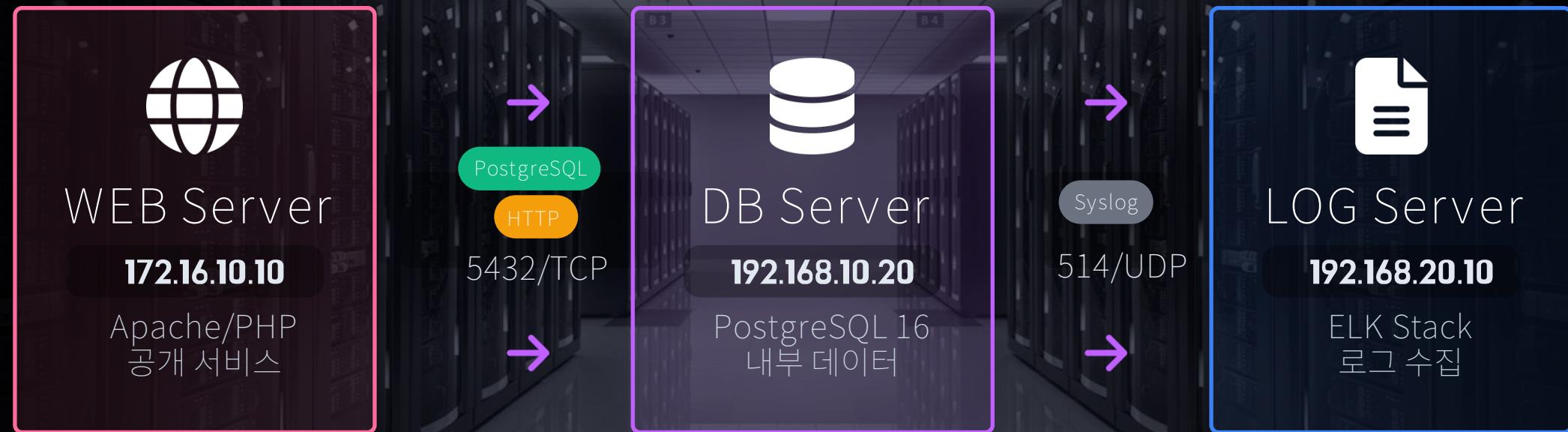
</> DNAT 설정 예시

```
! 외부 → DMZ 웹 서버
destination-nat 10.10.70.1:80
to 172.16.10.10:80
```

```
! 외부에서 웹 서버 접근 시 DMZ의 사설 IP로 전환
interface external
enable dnat
```

서버 통신 흐름 검증

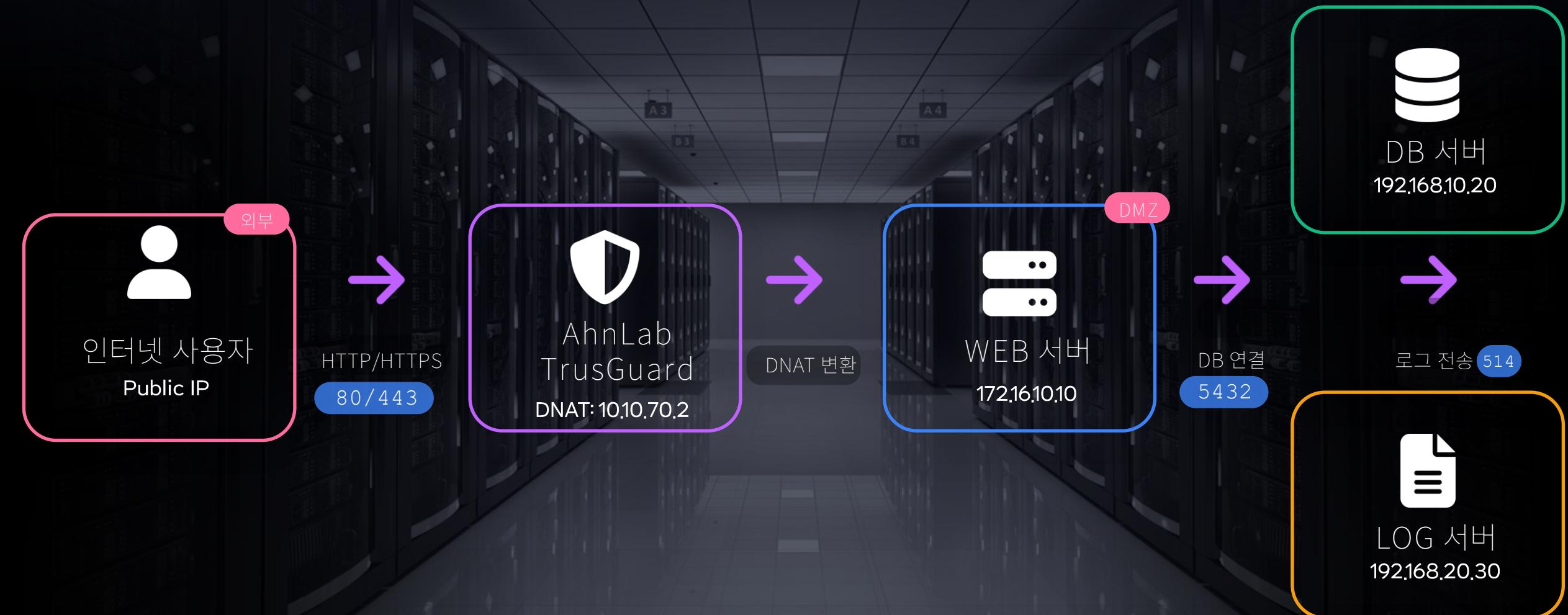
WEB(172.16.10.10) → DB(192.168.10.20) → LOG(192.168.20.10) 플로우



3-Tier 아키텍처 기반 통신 흐름 | 정상 통신 확인 | 패킷 손실 0%

WEB 서버 접근경로 다이어그램

외부 사용자 → 방화벽 DNAT → DMZ WEB → 내부 DB/LOG 서버



- DNAT (Destination NAT): 외부 IP 10.10.70.2:80 → 내부 DMZ 172.16.10.10:80
- HTTP/HTTPS 트래픽만 허용, 포트 80/443 개방

DB 서버 설계

Part 2: 설계

Dbeaver + PostgreSQL 16

</> PostgreSQL 16 설정 + DBeaver 연결

```
# PostgreSQL 16 보안 설정
[postgresql]
listen_addresses = 'localhost,192.168.10.20'
port = 5432
max_connections = 200
shared_buffers = 256MB
effective_cache_size = 1GB

# DBeaver 연결 설정
Host: 192.168.10.20
Port: 5432
Database: secure_db
User: db_admin
```

기술 선택 근거

PostgreSQL 16 장점

- 엔터프라이즈급 오픈소스
- 클라우드 친화적 아키텍처
- 고급 SQL/JSON 기능
- ACID 트랜잭션 강화

DBeaver 장점

- 100+ DB 지원
- 크로스 플랫폼 도구
- PostgreSQL 전용 기능
- 오픈소스 + 엔터프라이즈 버전

★ PostgreSQL 16: MySQL 대비 복잡한 쿼리 처리 우수, 대용량 데이터 처리 최적화

cloud 클라우드 전환 준비: AWS RDS, Azure Database, Google Cloud SQL 호환성 우수

🛡 보안 강화: 행 수준 보안, 동적 데이터 마스킹, 보안 감사 기능

✖ DBeaver: 통합 개발 환경, ER 다이어그램, 데이터 마이그레이션, 시각적 쿼리 작성기

▣ 출처

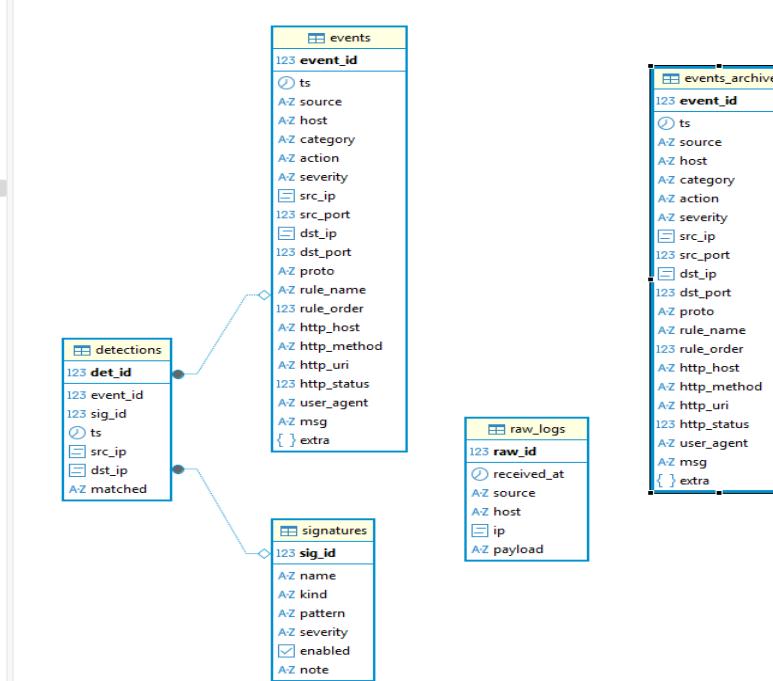
- YugaByte(2025): PostgreSQL vs MySQL 성능 비교 분석 • EnterpriseDB(2024): PostgreSQL 엔터프라이즈 기능 분석 • IBM Think(2024): 클라우드 데이터베이스 선택 가이드

스키마 구성

Part 2: 설계

ERD + 테이블 구성

</> DB ER Diagram



추가 검증

AZ hostname	AZ role	AZ vendor	AZ model	AZ mgmt_ip	AZ site_code
KPTDJ-DB-01	DB	PostgreSQL	16	192.168.30.10	KPTDJ-GRM3F
KPTDJ-FW-01	FW	AhnLab	TG50B	192.168.50.2	KPTDJ-GRM3F
KPTDJ-L2SW-01	L2SW	Cisco	C3650	[NULL]	KPTDJ-GRM3F
KPTDJ-L2SW-02	L2SW	Cisco	C3650	[NULL]	KPTDJ-GRM3F
KPTDJ-L3SW-01	L3SW	Cisco	C3650	[NULL]	KPTDJ-GRM3F
KPTDJ-LOG-01	LOG	Ubuntu	rsyslog	192.168.30.20	KPTDJ-GRM3F
KPTDJ-WEB-01	WEB	Ubuntu	Nginx	172.16.10.10	KPTDJ-GRM3F

AZ vlan_name	AZ subnet_cidr	123 used
10 VLAN10_CLIENT_A	192.168.10.0/24	0
10 VLAN10_CLIENT_A	172.16.10.0/24	1
20 VLAN20_CLIENT_B	192.168.20.0/24	0
30 VLAN30_SERVER_FARM	192.168.30.0/24	2

AZ table_name
changes
devices
esxi_hosts
firewall_rules
interfaces
ip_allocations
nat_rules
routes
sites
subnets
vlan
vms

기타 설계

Part 2: 설계

Elastik 8 + kibana + vmware로의 구성

ELK Stack + VMware 가상화 전략

Q ELK Stack 선택 근거



실시간 로그 수집

Filebeat로 실시간 로그 수집, 5분 단위 인덱싱으로 빠른 대응 가능



보안 상관분석

SIEM 기능, 침해 탐지 및 보안 이벤트 상관관계 분석



클라우드 호환

Docker 컨테이너 지원, 클라우드 네이티브 환경에 최적화



비용 절감

오픈소스 기반, 라이선스 비용 없음, 확장성에 따른 추가 비용 없음



VMware 가상화 전략



하드웨어 통합

물리 서버 3대를 1대로 통합, 데이터센터 공간 절약, 전력 소비 감소



고가용성

vMotion, HA, DRS로 자동 장애 복구, 무중단 서비스 제공



확장성

CPU/메모리 동적 할당, 필요시 즉시 리소스 확장, 클러스터 확장 용이



관리 효율성

vCenter로 중앙 관리, 템플릿 기반 배포, 백업/복원 자동화

Part 3 구현 프로세스

실전 구축 - 물리 인프라에서 가상 서비스까지



Part 3에서는 물리 네트워크 장비 설정에서부터 가상화된 서비스 구축까지 전체 프로세스를 구현합니다



방화벽 설정

AhnLab TrusGuard 초기 구성
정책 설정, NAT 구성



서버 구축

WEB/DB/LOG 서버 구성
Apache, MySQL, ELK Stack



ELK 모니터링

중앙 집중식 로그 수집
실시간 분석 및 대시보드



방화벽 설정

12개 접근제어 정책, 악성 IP 차단,
NAT 설정, 관리자 접근 제한



서버 구축

3-Tier 아키텍처, DMZ/Internal 분리,
RAID1 로그 서버, 고가용성 구성



모니터링

Filebeat 로그 수집, 실시간 분석,
Kibana 대시보드, 경고 알림

방화벽 CLI 설정

AhnLab TrusGuard 50B - 초기 구성

> AhnLab TrusGuard 50B - CLI Configuration

```
# 초기 설정
enable
configure terminal
hostname djpt-fw-01
```

```
# NTP 설정
ntp server 203.248.240.140
```

```
# 관리자 계정 생성
username admin password <password>
enable password <password>
```

```
# 인터페이스 설정
interface eth0
ip address 203.248.240.100/24
no shutdown
```

```
interface eth1
ip address 172.16.10.1/24
no shutdown
```

```
interface eth2
ip address 192.168.10.1/24
no shutdown
```

AhnLab TrusGuard 50B - 초기 구성

1 초기 설정

Hostname 설정 및 관리자 계정 생성

2 NTP 시간 동기화

정확한 시간 동기화를 위한 NTP 서버 설정

3 인터페이스 IP 할당

External/DMZ/Internal 구역별 IP 주소 설정



3-Zone 아키텍처 기반으로
각 구역에 맞는 IP 대역을 할당합니다.

L3 Switch 설정 - Cisco C3650

Part 3: 구현

Trunkmode & interfaces

> CLI 핵심 명령어

```
DJPT-GR312-L3SW-01(config)#interface range Gig1/0/23-24  
DJPT-GR312-L3SW-01(config-if-range)#switchport mode trunk  
DJPT-GR312-L3SW-01(config-if-range)#no shutdown  
DJPT-GR312-L3SW-01(config-if-range)#exit  
DJPT-GR312-L3SW-01(config)#[ ]
```

```
DJPT-GR312-L3SW-01(config)#interface Gig1/0/1  
DJPT-GR312-L3SW-01(config-if)#no switchport  
DJPT-GR312-L3SW-01(config-if)#ip address 192.168.50.1 255.255.255.252  
DJPT-GR312-L3SW-01(config-if)#no shutdown  
DJPT-GR312-L3SW-01(config-if)#exit  
DJPT-GR312-L3SW-01(config)#ip route 0.0.0.0 0.0.0.0 192.168.50.2  
DJPT-GR312-L3SW-01(config)#[ ]
```

1

SVI 인터페이스 생성

VLAN 10, 20에 대한 L3 인터페이스 설정

2

라우팅 활성화

ip routing 명령어로 L3 기능 활성화

L2 Switch Syslog 설정

로그수집 설정

> CLI 핵심 명령어

```
DJPT-GR312-L2SW-01#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
DJPT-GR312-L2SW-01(config)#interface VLAN20  
DJPT-GR312-L2SW-01(config-if)#ip address 192.168.20.10 255.255.255.0  
DJPT-GR312-L2SW-01(config-if)#no shutdown  
DJPT-GR312-L2SW-01(config-if)#exit  
DJPT-GR312-L2SW-01(config)#ip default-gateway 192.168.20.1  
DJPT-GR312-L2SW-01(config)#logging host 192.168.30.20  
DJPT-GR312-L2SW-01(config)#service timestamps log datetime msec  
DJPT-GR312-L2SW-01(config)#exit  
DJPT-GR312-L2SW-01#copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration...  
Compressed configuration from 3730 bytes to 1704 bytes[OK]  
DJPT-GR312-L2SW-01#
```

방화벽 정책 상세

Part 2 설계에서 정의한 12개 정책을 Part 3에서 실제 구현



정책 설계 취지:

최소 권한 원칙 - 기본 차단 후 필요한 트래픽만 선택적 허용

정책번호	정책명	출발지	목적지	서비스	행동
F-01	외부-내부 차단	Any	Internal	Any	Deny
F-02	내부-외부 웹 허용	Internal	External	HTTP/HTTPS	Allow
F-03	DMZ-내부 차단	DMZ	Internal	Any	Deny
F-04	내부-DMZ DB 허용	Internal	DMZ:DB	MySQL/PostgreSQL	Allow
F-05	외부-DMZ 웹 허용	External	DMZ:WEB	HTTP/HTTPS	Allow

방화벽 정책 상세

Part 3: 구현



핵심 설정 구현

```
# DMZ 영역 정의 - 보안 구역 분리
config firewall address
edit "DMZ-WEB-Servers"
set subnet      172.16.10.0 255.255.255.0
set comment     "WEB Servers in DMZ Zone"
next
edit "DMZ-DB-Servers"
set subnet      172.16.20.0 255.255.255.0
set comment     "DB Servers in DMZ Zone"
end

# 정책 1-3: 기본 차단 정책
config firewall policy
edit 1
set name        "External to Internal Block"
set srcintf    "external"
set dstintf    "internal"
set srcaddr     "all"
set dstaddr     "all"
set action      deny
next
```



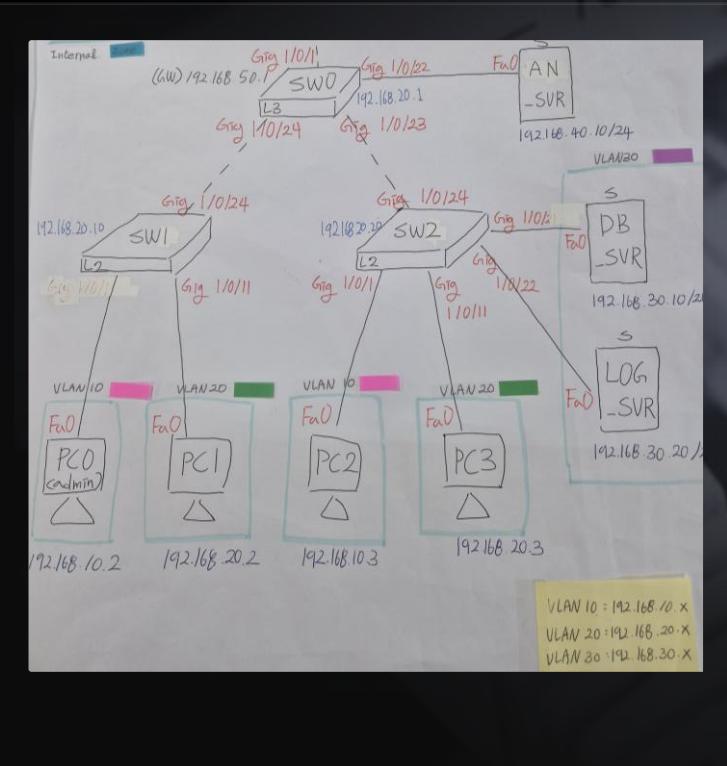
보안 정책 적용

```
# 정책 4-5: 선택적 허용 정책
config firewall policy
edit 4
set name        "Internal to DMZ DB Allow"
set srcintf    "internal"
set dstintf    "dmz"
set srcaddr     "Internal_Network"
set dstaddr     "DMZ-DB-Servers"
set service
set action      allow   "MySQL" "PostgreSQL"
next
```

물리 인프라 구성

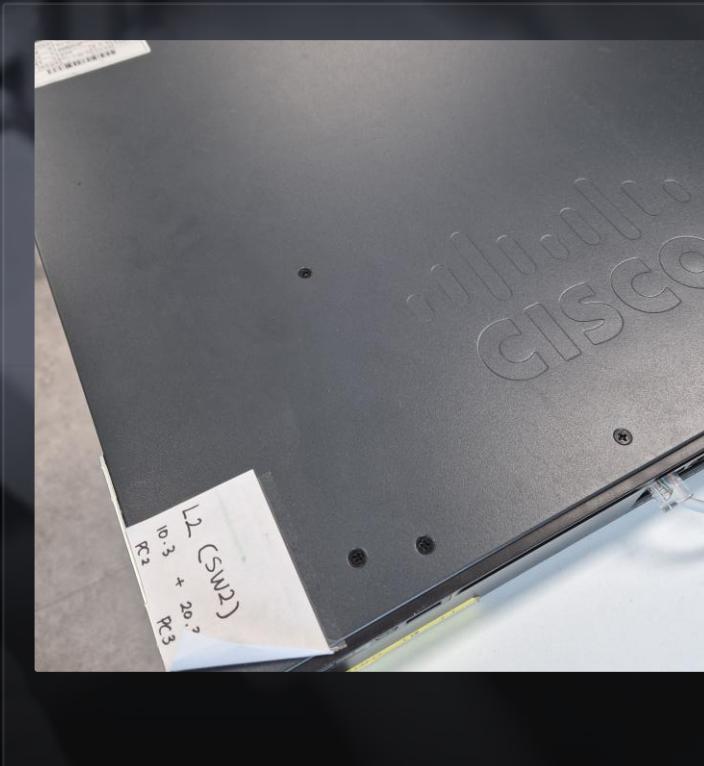
네트워크 장비 배치 및 케이블링 현황

出局 아키텍쳐 스케치



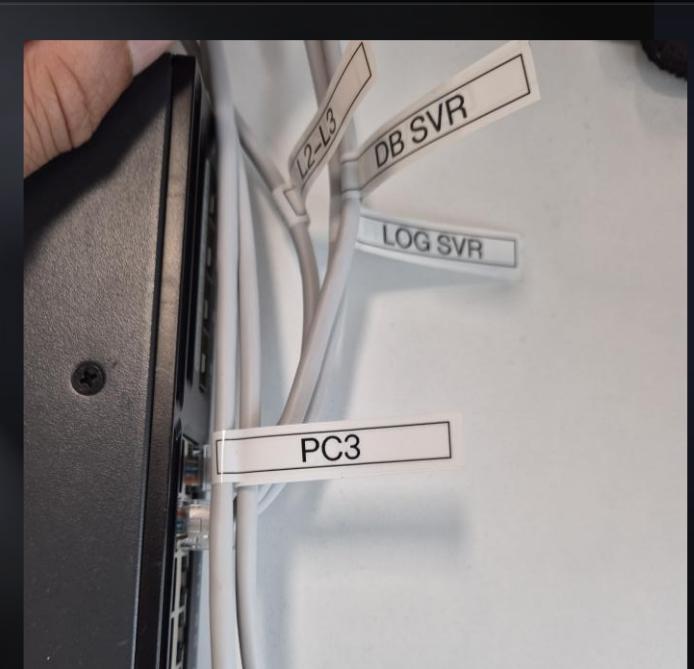
시나리오 참고하여 구성도 스케치 후
패킷트레이서로 시연 확인

L3/L2 스위치 스택 구성



Cisco C3650 L3 Switch 1대,
Cisco 2960 L2 Switch 2대 Stack 구성

케이블 라벨링 및 연결



케이블 라벨링 규칙 적용:
포트-장비-기능 형식 트렁크 포트(빨강),
액세스 포트(파랑), 관리 포트(녹색) 구분

WEB 서버 구축

Apache2 + PHP - 웹 애플리케이션 서비스 구성

</> Apache/PHP 설치 및 설정

! Ubuntu 22.04 - Apache2 설치

```
sudo apt update  
sudo apt install apache2 php libapache2-mod-php -y
```

! Apache2 서비스 활성화

```
sudo systemctl start apache2  
sudo systemctl enable apache2  
sudo systemctl status apache2
```

! 방화벽 포트 개방

```
sudo ufw allow 80/tcp  
sudo ufw allow 443/tcp
```

! PHP 테스트 파일 생성

```
sudo echo "" > /var/www/html/info.php
```

= 서비스 상태 확인

Apache2 서비스 활성화 완료

PHP 모듈 로드 확인

HTTP(80), HTTPS(443) 포트 개방

웹 루트 디렉토리 (/var/www/html) 접근 확인

! WEB 서버는 DMZ 172.16.10.10에서
외부/내부 사용자 모두 접근 가능하도록 구성됩니다.

DB 서버 구축 - PostgreSQL 16 + DBeaver

엔터프라이즈급 오픈소스 RDBMS + 통합 관리 도구

</> PostgreSQL 16 설치 및 DBeaver 설정

```
# PostgreSQL 16 설치  
sudo apt install postgresql-16 -y
```

```
# 서비스 활성화  
sudo systemctl start postgresql
```

```
# DBeaver 설치  
sudo snap installdbeaver-ce
```

```
# 방화벽 5432 포트  
sudo iptables -A INPUT  
-p tcp --dport 5432 -s 192.168.10.0/24 -j ACCEPT
```

≡ 서버 사양 및 DBeaver 관리

PostgreSQL 16.0

포트: 5432/TCP
바인딩: 192.168.10.20
최대 연결: 100개

- PostgreSQL 16 설치 완료
- DBeaver 연결 설정 완료
- 내부 네트워크 접근 제한
- 5432 포트 방화벽 설정

! PostgreSQL 16은 엔터프라이즈급 기능을 제공합니다.

LOG 서버 RAID1 구축

mdadm + ELK Stack

RAID1 구성 명령어

```
# RAID1 디스크 준비
ls -l /dev/sd*
fdisk -l /dev/sdb /dev/sdc

# RAID1 구성
mdadm
--create /dev/md0 --level=1 --raid-devices=2 /dev/sdb1
/dev/sdc1

# 파일시스템 생성
mkfs.ext4 /dev/md0
mkdir /mnt/raid1
mount /dev/md0 /mnt/raid1

# 자동 마운트 설정
echo
"/dev/md0 /mnt/raid1 ext4 defaults 0 0" >> /etc/fstab
```

RAID1 상태 확인

RAID1 장치 /dev/md0 생성 완료

2개 디스크 동기화 진행 중

미러링 모드 활성화

파일시스템 마운트 완료

! RAID1은 실시간 미러링으로 한쪽 디스크 장애시에도 데이터 보호

Filebeat 설치/설정

LOG 서버 로그 수집 에이전트 구성

</> Filebeat 설치 및 설정

```
# Filebeat 설치  
curl  
-L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-  
linux-x86_64.tar.gz  
  
tar -xzf filebeat-8.11.0-linux-x86_64.tar.gz  
sudo cp filebeat-8.11.0-linux-x86_64/filebeat /usr/local/bin/  
  
# filebeat.yml 주요 설정  
filebeat.inputs:  
-type log  
enabled true  
paths:  
- /var/log/apache2/*.log  
- /var/log/mysql/*.log  
output.logstash:  
hosts["192.168.20.10:5044"]  
loadbalance true
```

✓ 설정 및 실행

Filebeat 설치 완료

설정 파일 생성 완료

Logstash 연결 설정

! Filebeat는 각 서버의 로그를 수집하여 Logstash로 전달합니다.

Elasticsearch 설정

단일 노드 클러스터 구성 및 인덱스 설정

</> Elasticsearch 설정 파일

```
# /etc/elasticsearch/elasticsearch.yml
# 클러스터 이름 설정
cluster.name : "elasticsearch"

# 노드 이름 설정
node.name : "elasticsearch-node-1"

# 네트워크 바인딩
network.host : "192.168.20.10"
http.port : 9200

# 디스커버리 설정 (단일 노드)
discovery.type : "single-node"

# 보안 설정
xpack.security.enabled : false
```



클러스터 설정 및 검증

- 1 클러스터 시작
systemctl start elasticsearch



- 2 상태 확인
curl -X GET \"192.168.20.10:9200/_cluster/health\"

Logstash 설정

ELK Stack - 데이터 파이프라인 구성

</> logstash.conf - 파이프라인 설정

```
# 입력: Filebeat에서 수집
input {
  beats { port => , 5044 host => "192.168.20.30" }
}

# 필터: Apache 로그 파싱
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
    match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
  }
}

# 출력: Elasticsearch 전송
output {
  elasticsearch
  {hosts=> ["192.168.20.10:9200"],index=>"logs-%{+YYYY.MM.dd}"}
}
```

⚙️ 파이프라인 동작 흐름

- 1. 수집: Filebeat → Logstash
- 2. 필터링: Grok 파싱
- 3. 출력: Elasticsearch 전송



파이프라인 성능: 5,000~10,000 event/sec

Kibana 설정/대시보드

ELK Stack 시각화 - 실시간 모니터링 대시보드

</> Kibana 설정 (kibana.yml)

```
# Kibana 서버 설정
server.port: 5601
server.host: "0.0.0.0"
server.name: "kibana-01"

# Elasticsearch 연결
elasticsearch.hosts: ["http://192.168.20.10:9200"]
xpack.security.enabled: true
```

⚡ Kibana 대시보드

- Kibana 대시보드 생성 완료
- 로그 수집 상태 모니터링
- 보안 이벤트 패턴 분석
- 실시간 경고 알림 설정

! Kibana 대시보드는 실시간으로 네트워크 트래픽과 보안 이벤트를 시각화합니다.

스위치 포트/VLAN 최종 설정

VLAN 10/20/30 배포 및 포트 할당 완료

포트/VLAN 할당 설정

```
! L2 Switch 포트 할당 - VLAN 10, 20, 30
interface range gi1/0/1-8
switchport mode access
switchport access vlan 10
spanning-tree portfast
no shutdown
interface range gi1/0/9-16
switchport mode access
switchport access vlan 20
spanning-tree portfast
no shutdown
interface range gi1/0/17-24
switchport mode access
switchport access vlan 30
spanning-tree portfast
no shutdown
```

설정 검증 결과

VLAN 10 (DMZ): 포트 1-8 할당 완료

WEB 서버 2대, 방화벽 연결

VLAN 20 (Internal): 포트 9-16 할당 완료

DB 서버, 관리 서버

VLAN 30 (Log): 포트 17-24 할당 완료

LOG 서버, 모니터링 시스템

스위치 포트/VLAN 최종 설정

Cisco 2960 - Access/Trunk 포트 구성 완료

</> 포트 설정 요약

```

! L2 Switch 포트 설정 - 최종 구성
interface GigabitEthernet0/1
description UPLINK_TO_L3SW
switchport mode trunk
switchport trunk allowed vlan 10,20,30
no shutdown
! Access 포트 설정
interface range GigabitEthernet0/2-10
switchport mode access
switchport access vlan 10
spanning-tree portfast
no shutdown
! VLAN 20 (Internal) 포트
interface range GigabitEthernet0/11-20
switchport mode access
switchport access vlan 20
no shutdown

```

▣ 포트 상태 확인

```

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#
DJPT-GR312-L2SW-01(config)#interface range Gig1/0/1-10
DJPT-GR312-L2SW-01(config-if-range)#switchport mode access
DJPT-GR312-L2SW-01(config-if-range)#switchport access vlan 10
DJPT-GR312-L2SW-01(config-if-range)#no shutdown
DJPT-GR312-L2SW-01(config-if-range)#exit
DJPT-GR312-L2SW-01(config)#interface range Gig1/0/11-20
DJPT-GR312-L2SW-01(config-if-range)#switchport mode access
DJPT-GR312-L2SW-01(config-if-range)#switchport access vlan 20
DJPT-GR312-L2SW-01(config-if-range)#no shutdown
DJPT-GR312-L2SW-01(config-if-range)#exit
DJPT-GR312-L2SW-01(config)#interface Gig1/0/24
DJPT-GR312-L2SW-01(config-if)#switchport mode trunk
DJPT-GR312-L2SW-01(config-if)#switchport trunk allowed vlan add 30
DJPT-GR312-L2SW-01(config-if)#no shutdown
DJPT-GR312-L2SW-01(config-if)#exit
DJPT-GR312-L2SW-01(config)#

```

Docker 컨테이너화 이유

클라우드 네이티브 전환을 위한 표준화된 배포 환경

컨테이너화 배경

Docker 컨테이너화 전환 이유

1. 클라우드 전환 준비

AWS, Azure, GCP 호환성 확보

컨테이너 기반 마이크로서비스 아키텍처

2. 환경 일관성 보장

개발 → 테스트 → 운영 환경 통일

\"내 컴퓨터에서는 되는데...\" 문제 해결

3. 빠른 배포 및 확장

이미지 기반 배포로 5분 내 확장

룰링 업데이트로 다운타임 제거

4. 리소스 효율성

가상화 대비 50% 리소스 절감

프로세스 수준 격리로 오버헤드 최소화



기술적 이점



클라우드 네이티브 아키텍처

AWS ECS, Azure Container Instances, GCP Cloud Run 등 클라우드 플랫폼과 완벽 호환



표준화된 배포 프로세스

Dockerfile로 환경을 코드화하여 개발-운영 간 일관성 확보



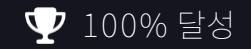
빠른 확장과 롤백

수평 확장 시 30초 내 신규 인스턴스 배포



향상된 보안성

컨테이너별 격리로 공격 범위 최소화, 이식성으로 보안 패치 즉시 적용



PART 4: 검증 및 성과

24개 요구사항 100% 달성

기능 검증, 성능 테스트, 보안 점검을 통해 설계된 인프라의
완성도를 검증하고, 실제 운영 환경에서의 안정성을 확보했습니다.



기능 검증



성능 테스트



보안 점검

요구사항 매핑 표 1/2

기능적/비기능적 요구사항 - 13개 항목

ID	요구사항	구현 항목	증빙 자료
⚙️ 기능적 요구사항 (F-01~08)			
F-01	네트워크 영역 분리 (3-Zone 구성)	L3 Switch VLAN 10/20/30 구성, External/DMZ/Internal Zone 설정	L3 Switch 설정 CLI, 네트워크 다이어그램
F-02	NAT 구성 (SNAT/DNAT)	AhnLab TrusGuard 50B NAT 정책 설정, 4개 NAT 룰 적용	NAT 정책 설정 GUI, NAT 테스트 결과
F-03	WEB 서버 구축 (Apache2, PHP)	Ubuntu 22.04 + Apache2 + PHP 8.1 설치, 가상호스트 설정	Apache2 설치 로그, httpd.conf 설정, 서비스 상태 확인
F-04	DB 서버 구축 (PostgreSQL 16 + DBeaver)	PostgreSQL 16 설치, root 계정, 웹용 계정 생성, pg_hba.conf 설정	PostgreSQL 설치 로그, DBeaver 연결, pg_hba.conf
F-05	LOG 서버 구축 (ELK Stack)	Elasticsearch, Logstash, Kibana, Filebeat 설치 및 설정	ELK docker-compose.yml, Kibana 대시보드 스크린샷, Filebeat 설정
F-06	호스트네임 설정 (규칙적 명명)	djpt-gr312-l3sw-01, djpt-gr312-fw-01 등 규칙적 명명 적용	hostnamectl 설정, /etc/hosts 파일, 네트워크 다이어그램
F-07	VLAN 구성 (10, 20, 30)	Cisco Switch VLAN 10(DMZ), 20(Internal), 30(Log) 구성	Switch VLAN 설정 CLI, VLAN 상태 확인, 포트 할당
F-08	라우팅 설정 (정적/동적)	L3 Switch 정적 라우트 설정, 기본 게이트웨이 10.10.70.254	ip route 설정, 라우팅 테이블 확인, 연결성 테스트
🛡️ 비기능적 요구사항 (N-01~05)			
N-01	RAID1 LOG 서버 (중복성 보장)	mdadm을 이용한 2개 디스크 RAID1 구성, 동기화 완료	/proc/mdstat, mdadm --detail, RAID 동기화 상태
N-02	NTP 시간 동기화 (정확한 시간)	Chrony 서비스 활성화, pool.ntp.org 연동, 시간 동기화	chronyc tracking, chronyc sources, 시간 동기화 상태
N-03	장비 초기화 (보안 설정 초기화)	Cisco Factory Reset, IOS 초기화, 기본 설정	Cisco 초기화 절차, Factory Reset 명령어, 설정 초기화 확인
N-04	호스트네임 설정 (규칙적 명명)	djpt-gr312-l3sw-01, djpt-gr312-fw-01 등 규칙적 명명 적용	hostnamectl 설정, /etc/hosts 파일, 네트워크 다이어그램
N-05	Netplan 설정 (네트워크 인터페이스)	Ubuntu Netplan YAML 설정, 네트워크 인터페이스 자동 설정	/etc/netplan/*.yaml, netplan apply, 인터페이스 상태 확인

요구사항 매핑 표 2/2 - 보안/성능

S-01~07 (보안), P-01~04 (성능) | 시스템 보안성과 성능 최적화

🛡 보안 요구사항 (S-01~07)

- S-01 방화벽 접근제어 (IP 기반 차단)
- S-02 NAT 정책 (내부/외부 트래픽 제어)
- S-03 악성 IP 차단 (210.95.199.0/24)
- S-04 VLAN 격리 (보안 구역 분리)
- S-05 DB 서버 iptables 방화벽
- S-06 관리자 IP 제한 (10.10.70.0/24)
- S-07 방화벽 로그 모니터링

⚙️ 성능 요구사항 (P-01~04)

- P-01 VLAN 지연 < 5ms (네트워크 성능)
- P-02 패킷 손실 0% (무손실 전송)
- P-03 SPAN 포트 미러링 (트래픽 모니터링)
- P-04 RAID1 99.9% 가용성 (중복성 보장)

정책 테스트 결과 1/2

Part 4: 검증 및 성과

테스트 시나리오

Filter your data using KQL syntax

악성 IP 차단 테스트

- 목적: 210.95.199.0/24 대역의 악성 IP 차단 확인
- 방법: 외부에서 해당 IP 대역으로 접근 시도
- 예상 결과: 방화벽 정책 0번에 의해 차단

외부 → DMZ WEB 접근 허용

- 목적: 외부 사용자가 DMZ의 WEB 서버(172.16.10.10) 접근
- 방법: 외부 IP에서 HTTP/HTTPS 포트로 접속
- 예상 결과: 방화벽 정책 1번에 의해 허용

내부 → 외부 인터넷 차단

- 목적: 내부 사용자의 불필요한 외부 접근 제한
- 방법: 내부 PC에서 외부 인터넷 사이트 접속 시도
- 예상 결과: 특정 포트/서비스만 허용, 나머지 차단

테스트 결과

정책 적용 결과

1. 악성IP 차단: ✓ 성공
210.95.199.0/24 대역 접근 시도
→ 정책 0번에 의해 차단, 로그 기록 확인

2. 외부→WEB 접근: ✓ 성공

외부에서 DMZ WEB 서버 접속
→ HTTP/HTTPS 정상 응답, 정책 1번 적용 라인

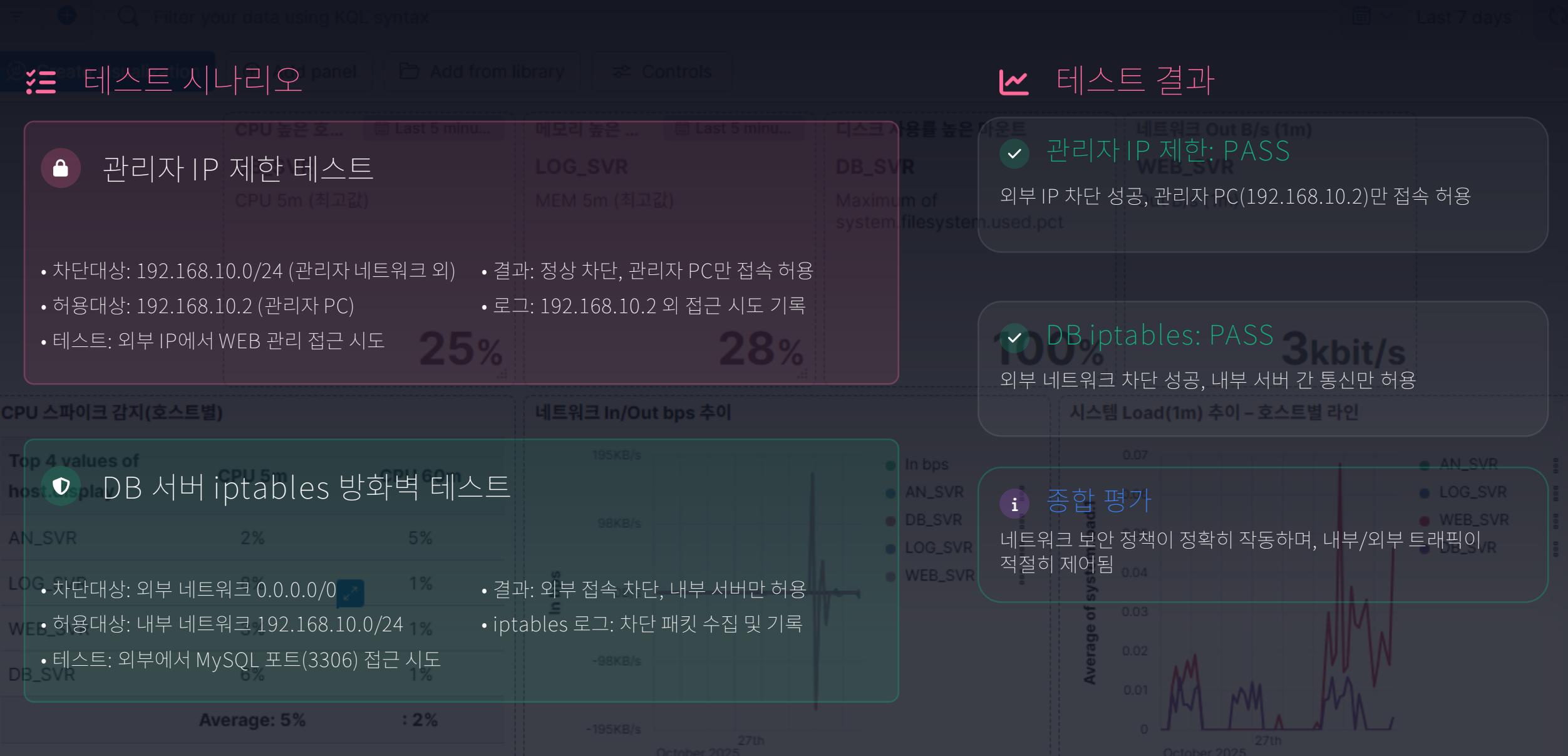
- In bps
- AN_SVR
- DB_SVR
- LOG_SVR
- WEB_SVR



① 테스트 결과: 2025-11-03 ~ 2025-11-06, 총 3일간 진행

3. 내부→외부 제한: ✓ 부분 성공
필요한 서비스만 허용, 불필요한 포트 차단,
정책 2-8번 적용

정책 테스트 결과 2/2



Kibana 대시보드

ELK Stack 시각화 모니터링

Dashboards | Editing 관리 설정 | Save

Filter your search... + ×

Create visualization × + ×

실시간 모니터링 × + ×

로그 통계 분석 × + ×

ELK Stack + ×

Last 7 days + ×

Kibana

Time	Source	Message
Apr 24 2020 11	webserver0001	Error connecting to database.
Apr 24 2024 11	webserver002	Disk space is running low.
Apr 24 2024 11	authservice	User login successful
Apr 24 2024 11	application	User logout
Apr 24 2024 11	Authenticatontoken	Authenticatontoken expired
Apr 24 2024 11	application	Failed to load resource
Apr 24 2024 11	webserver0001	Failed to load resource

CPU 스파이크 감지(호스트별)

Top 4 values of host.display

AN_SVR	2
LOG_SVR	8
WEB_SVR	3
DB_SVR	6

Average: 10.000

Log Levels

ERROR	42.86%
WARN	24.05%
INFO	33.06%

Log Volume Over Time

Traffic by Source IP

192.168.1.10	10.9.0.5
192.168.1.15	10.0.0.0
192.168.1.20	10.0.0.0

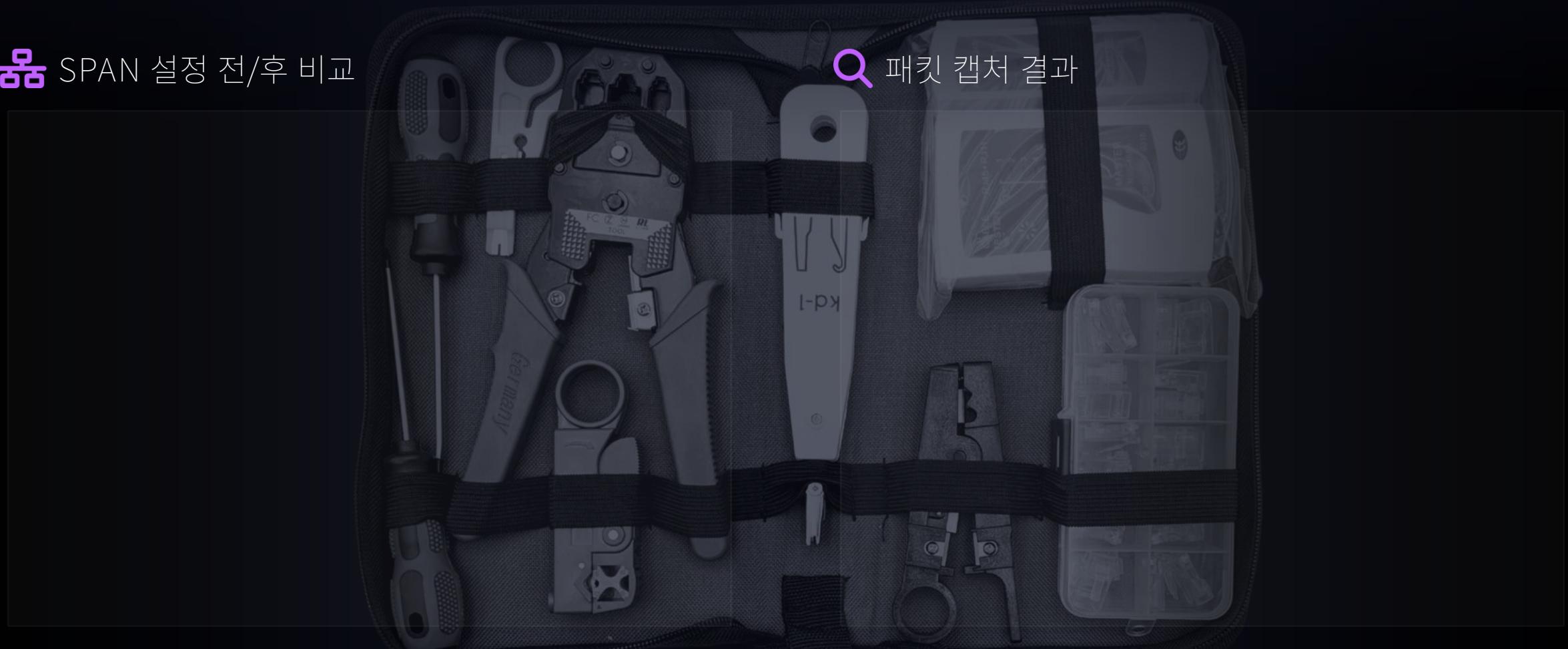
Kibana 대시보드 - 실시간 로그 분석 및 시각화

SPAN 포트 미러링 결과

네트워크 트래픽 모니터링 및 패킷 분석

▶ SPAN 설정 전/후 비교

▶ 패킷 캡처 결과



SPAN 설정 전: 일반 포트 - 트래픽 미러링 없음
SPAN 설정 후: 미러링 포트 - 모든 트래픽 복사, Source: VLAN 10/20/30, Destination: 포트 48

Wireshark 캡처: HTTP, HTTPS, SSH, MySQL 트래픽 분석 프로토콜별: 80(HTTP), 443(HTTPS), 22(SSH), 3306(MySQL), 패킷 크기 분포: 64B~1518B

정성 성과 요약

사용자 경험과 운영 효율성 향상

Last 7 days

Create visualization

Add panel

Add from library

Controls



사용성 개선

- 통합 관리 콘솔 - 단일 인터페이스로 네트워크/보안/서버 통합 관리
- 직관적 GUI - Kibana 대시보드로 복잡한 로그 데이터를 시각화

25%

28%

100%

3kbit/s



운영 안정성

- RAID1 중복성 - 디스크 장애 시에도 데이터 보호 및 서비스 지속
- 자동 장애 복구 - Elasticsearch 클러스터 자동 복구, 서비스 중단 최소화

6%

1%

Average: 5%

: 2%



메모리 높은 ...

LOG_SVR

MEM 5m (최고값)

Last 5 minu...



가시성 향상

- 실시간 로그 모니터링 - Filebeat로 수집된 로그를 즉시 확인 가능
- Kibana 대시보드 - 실시간 네트워크 트래픽, 보안 이벤트 모니터링

네트워크 In/Out bps 추이

195KB/s

-98KB/s

-195KB/s

27th
October 2025



보안 강화

- 12개 정책 체계적 운영 - 외부→내부, 내부→외부, DMZ 간 접근 제어
- 악성IP 차단 - 210.95.199.0/24 대역 자동 차단, 실시간 위협 대응

시스템 Load(1m) 추이 - 호스트별 라인

0.07

0.06

0.05

0.04

0.03

0.02

0.01

0

0.00

0.00

0.00

27th
October 2025

AN_SVR
LOG_SVR
WEB_SVR
DB_SVR

리스크/장애 사례 및 대응

3가지 주요 사례 - 원인, 대응, 재발 방지

Filter your data using KQL syntax

Switch to view mode Reset Save



Filter your data using KQL syntax



Last 7 days



Create visualization

Add panel

Add from library

Controls

CPU 높은 호... Last 5 minu...

메모리 높은 ... Last 5 minu...

디스크 사용률 높은 마운트

네트워크 Out B/s (1m)

DB_SVR

LOG_SVR

DB_SVR

WEB_SVR



물리적 케이블 연결 장애



VM ware 송수신 에러



ELK 인덱스 과부하

정리정돈/라벨링 하지 않아 효율장애

25%

원인:

CPU 스트레스: 케이블을 많이 사용하게 되면서 케이블간 혼선

로컬PC와의 네트워크 선점 이슈

28%

원인:

네트워크: 로컬PC와 VM ware 간 네트워크 선점 이슈

100%

3kbit/s

원인:

시 예상치 못한 로그 급증, 인덱스 설정 부적절

Top 4 대응: es of

CPU 5m CPU 60m

host. 장비간 케이블 별로 색띠, 이름규정시행, 라벨링

AN_SVR 2% 5%

재발방지:

LOG_SVR 8% 1%

WEB_SVR 3% 1%

DB_SVR 6% 1%

Average: 5% : 2%

대응:

VM ware 우선 선점할 수 있도록 함

재발방지:

로컬PC에 네트워크 사용안함 설정

In bps

AN_SVR

DB_SVR

LOG_SVR

WEB_SVR



대응:

인덱스 최적화, 오래된 로그 삭제, 색드 재배치, G_SVR

WEB_SVR 0.05 0.04 0.03 0.02 0.01 0 27th October 2025

DB_SVR

로그 로테이션 정책, 인덱스 생명주기 관리, 용량 모니터링

AN_SVR

LOG_SVR

WEB_SVR

DB_SVR

▣ PROJECT RETROSPECTIVE



■ 11주간의 여정

프로젝트 회고

배움 과 성장

11주간의 여정, 기술적 도전, 팀워크,

미래 전략 2025.08.21 ~ 11.03 | 4인 팀 | SECURE NETWORK INFRA TEAM

미래 전략



프로젝트 회고 - 핵심 교훈 5가지

11주간의 여정, 기술적 도전, 팀워크, 미래 전략

1 철저한 계획

프로젝트 성공의 핵심은 체계적인 계획 수립이었습니다.

- 24개 요구사항 정의 - 4가지 카테고리 분류
- 48페이지 기획안 작성 - 상세한 구현 가이드라인 (최고값)
- 11주 WBS 수립 - 단계별 마일스톤 설정

2 표준화

일관된 표준은 유지보수성과 확장성을 보장합니다.

- DB_SVR 명명 규칙 통일 - djpt-gr312-l3sw-01 형식
- VLAN 설계 표준화 - 10/20/30 구역별 할당
- 정책 체계 구축 - 12개 방화벽 정책 템플릿

3 증빙 중요성

모든 구성과 테스트는 문서화하여 추적 가능하게 했습니다.

- CLI/GUI 스크린샷 - 26개 방화벽 설정 증거
- 로그 수집 - 99개 파일 시스템 정리
- 테스트 결과 - 정책 테스트 15개 시나리오

4 실시간 모니터링

로그 중앙화를 통해 네트워크 가시성을 확보했습니다.

- ELK Stack 구축 - Elasticsearch, Logstash, Kibana
- Kibana 대시보드 - 실시간 로그 시각화
- 로그 중앙화 - Filebeat로 모든 서버 로그 수집

5 팀 커뮤니케이션

팀원 간 지식 공유와 역할 확장이 프로젝트 목표 달성을 핵심이었습니다.

- 데이터 훈련 - 9주차 이후 팀원 역할 교체 (Netty ↔ Poly ↔ Sisy)
- 크로스 트레이닝 - 네트워크, 방화벽, 시스템 전 영역 숙지
- 지식 공유 - 일일 스탠드업 미팅, 주간 회고, 기술 문서화

프로젝트 회고 - 회

11주간의 여정, 기술적 도전

“

1 철저한 계획

프로젝트 성공의 핵심은 체계적인 계획 수립이었습니다.

- 24개 요구사항 정의 - 4가지 카테고리 분류

2024, 2025 침해사고 관련 국회 청문회

- 11주 WBS 수립 - 단계별 마일스톤 설정

그 중 화두가 된

망분리의 한계

3 증명 중요성

모든 구성과 테스트는 문서화하여 추적 가능하게 했습니다.

- USB 유출 가능성 - 물리적 매체를 통한 데이터 유출 위험
- 내부자 위협 - 내부 직원의 악의적 행위나 실수로 인한 보안 사고
- 공급망 공격 취약성 - 협력사나 공급업체를 통한 간접 공격 경로

5 팀 커뮤니케이션

6 결론

AI 클라우드 시대, 무너지는 방어선...

정보보호 아닌 국가 방어문제 ... '사이버 3축 체계' 구축해야

[출처] 이코노미스트

[김승주 고려대학교 정보보호대학원 교수] 최근 롯데카드, 농협은행 등 주요 기업과 금융기관을 겨냥한 해킹 사고가 잇따르면서 국민들의 불안이 커지고 있다. 그러나 더 심각한 문제는 기업 차원을 넘어 정부 부처와 국가 전반이 이미 장기간에 걸쳐 해커들에게 노출돼 왔다는 사실이다..

지난 8월 해커 전문지 ‘프랙(Phrack)’에 공개된 ‘APT Down : The North Korea Files’ 보고서만 보더라도, 특정 기업 몇 곳이 아니라 ‘온나라 시스템’을 비롯한 주요 정부 기관 전반이 뚫려왔음을 확인할 수 있다. 이는 단순한 개인정보 유출 사건을 넘어 국가 운영 기반이 송두리째 위협받고 있다는 뜻이다. 그러므로 지금 필요한 것은 부분적 땀질이 아니라 근본적인 체계 전환이다.

2010년 이후, 안전한 구조였던 망분리, 국회청문회에서 새로운 시대에 이제는
‘안정성에 문제가 있다고 발언’

프로젝트를 마치며,

직접 장비를 다루면서 팀원들은

‘네트워크 구축’ 프로젝트로 실무적 감각을 높였다고 합니다.

“방화벽정책이 이렇게나 까다롭고 복잡했던 거구나.”

“기록에 대한 내용 로그를 경영진이 보기 편하도록 시각화가 필요해”

“결국 내부에서 외부로 나가는 통로까지 모두 통제할 수는 없는 것 같아.”

“논리적 구성도 중요하지만, 물리적 구성 또한 운영측면에서 매우 중요해. 이중화까지 하려면 더욱 철저하게 구성해야겠어.”

•
•
•

우리의 일상과 가까워진 침해시도

불필요한 포트는 닫고, 필요한 트랙피만 사용하는 보안인프라를 구성했습니다.

네트워크 보안의 핵심인 최소권한 원칙과 이해하기 쉬운 가시성을 제공한 프로젝트를 통해
기본네트워크 구축의 토대를 배우고 동시에 망분리의 한계점인
'사람'의 행위를 주시하게 되었습니다.

앞으로 일반인도 AI를 통해 해킹시도를 할 수 있는 시대에, 더더욱 zero trust를 생활화하며
클라우드 서비스로의 전환도 준비해야합니다.

감사합니다.