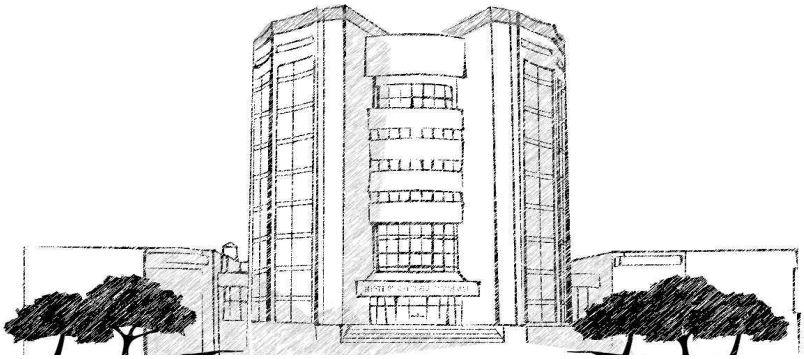
2014년 KISTI 원내망 성능향상 분석보고서



2014. 12.

한국과학기술정보연구원

목 차

I. 개요 1

1. 목적 및 필요성 1
2. 분석 활용 계획 1
3. 원내망 성능향상 테스트 방법 및 내용 2

II. 원내망 성능향상 테스트 수행 결과 분석 3

1. 1차 원내망 성능향상 테스트 수행 현황 분석 3
2. 2차 원내망 성능향상 테스트 수행 현황 분석 6
3. 3차 원내망 성능향상 테스트 수행 현황 분석 9
4. 원내망 테스트 수행 결과 종합분석 12

III. 원내 무선망 점검 수행 결과 분석 14

1. 원내 무선AP 구성 및 정책 현황 14
2. 원내 불법 AP 탐지 및 차단 현황 15
3. 원내 불법 AP 차단 방법 및 테스트 수행 분석 32

IV. 종합분석 및 성능향상 방안 34

그림 목차

[그림 1. 1차 원내망 테스트 구성도] ····· 3

[그림 2. 2차 원내망 테스트 구성도] ····· 6

[그림 3. 3차 원내망 테스트 구성도] ····· 9

[그림 4. 무선 AP 보안 정책] ····· 14

[그림 5. 무선AP 차단 정책] ····· 15

[그림 6. 원내 불법AP 탐지 현황] ····· 15

[그림 7. 본원 1층 불법AP 차단 건수] ····· 16

[그림 8. 본원 2층 불법AP 차단 건수] ····· 17

[그림 9. 본원 3층 불법AP 차단 건수] ····· 18

[그림 10. 본원 5층 불법AP 차단 건수] ····· 19

[그림 11. 본원 6층 불법AP 차단 건수] ····· 20

[그림 12. 본원 7층 불법AP 차단 건수] ····· 21

[그림 13. 별관 2층 불법AP 차단 건수] ····· 22

[그림 14. 분원 2층 불법AP 차단 건수] ····· 24

[그림 16. 경인지원 불법AP 차단 건수] ····· 26

[그림 17. 대구 경북지원 불법AP 차단 건수] ····· 30

[그림 18. 원내 불법AP 차단 테스트 화면] ····· 32

표 목차

[표 1. 1차 원내망 테스트 수행표] ····· 4

[표 2. 2차 원내망 테스트 수행표] ····· 7

[표 3. 3차 원내망 테스트 수행표] ····· 10

[표 4. 원내 무선AP 구성 항목] ····· 14

[표 5. 본원 1층 불법AP 차단 현황] ····· 16

[표 6. 본원 1층 불법AP 차단 세부 현황] ····· 17

[표 7. 본원 2층 불법AP 차단 현황] ····· 17

[표 8. 본원 2층 불법AP 차단 세부 현황] ····· 18

[표 9. 본원 3층 불법AP 차단 현황] ····· 18

[표 10. 본원 3층 불법AP 차단 세부 현황] ····· 19

[표 12. 본원 5층 불법AP 차단 세부 현황] ····· 20

[표 13. 본원 6층 불법AP 차단 현황] ····· 20

[표 14. 본원 6층 불법AP 차단 세부 현황] ····· 21

[표 15. 본원 7층 불법AP 차단 현황] ····· 21

[표 16. 본원 7층 불법AP 차단 세부 현황] ····· 22

[표 17. 별관 2층 불법AP 차단 현황] ····· 22

[표 18. 별관 2층 불법AP 차단 세부 현황] ····· 23

[표 19. 분원 2층 불법AP 차단 현황] ····· 24

[표 20. 분원 2층 불법AP 차단 세부 현황] ····· 24

[표 21. 분원 4층 불법AP 차단 현황] ····· 25

[표 22. 분원 4층 불법AP 차단 세부 현황] ····· 25

[표 23. 경인지원 불법AP 차단 현황] ····· 26

[표 24. 경인지원 불법AP 차단 세부 현황1] ····· 27

[표 25. 경인지원 불법AP 차단 세부 현황2] ····· 28

[표 26. 경인지원 불법AP 차단 세부 현황3] ····· 29

[표 27. 대구 경부지원 불법AP 차단 현황] ····· 30

[표 28. 대구 경부지원 불법AP 차단 세부 현황] ····· 31

Ⅰ 개요

1. 목적 및 필요성

□ KISTI 원내망의 안정적인 운영 및 효율적인 관리를 위하
2014년 8월 통합 UTM 보안장비를 도입한바, 통합 UTM
장비의 원내 자체 DDoS 공격 테스트를 통한 성능향상 및
보안성 강화를 통해 향후 발생 할 수 있는 보안사고에 대비

□ KISTI 불법 AP 사용 실태 점검을 통한 원내 무선 AP 사용자의
의식을 제고하고, 효과적인 불법 무선 AP 차단 방법의 분석을
통한 보안성 강화에 기여

□ KISTI 원내망 성능향상을 통한 안정적인 운영 및 보안성
강화를 통해 보안 취약점을 개선하고 사용자 보안사고 예방에 기여
하고자 함

2. 분석 활용 계획

□ 통합 보안 장비 성능 향상 전략 수립

- ㅇ 통합 UTM 장비의 성능 향상 및 원내망의 안정성 고도화
- ㅇ 원내 보안 사고에 대한 안정적인 대비 및 효과적 대응

□ 효과적 불법 AP 차단 전략의 수립

- ㅇ 불법 AP를 통한 사고 방지 및 차단 방법의 효율화
- ㅇ 효과적 보안 사고 처리 지원 방법 도출

3. 원내망 성능향상 테스트 방법 및 내용

□ 원내 DDoS 공격 장비를 통한 테스트 수행 및 결과 분석

- ㅇ 총 3회에 걸친 테스트를 통해 결과 값 신뢰성 제고
- ㅇ 안정적인 원내망 구축을 위해 전문 엔지니어를 통한 심도 높은 분석 수행
- ㅇ 테스트 결과 값을 통한 원내망 성능 향상 및 안정성 향상 방법 제시

□ 무선 AP 센서를 통한 불법 AP 탐지 및 차단

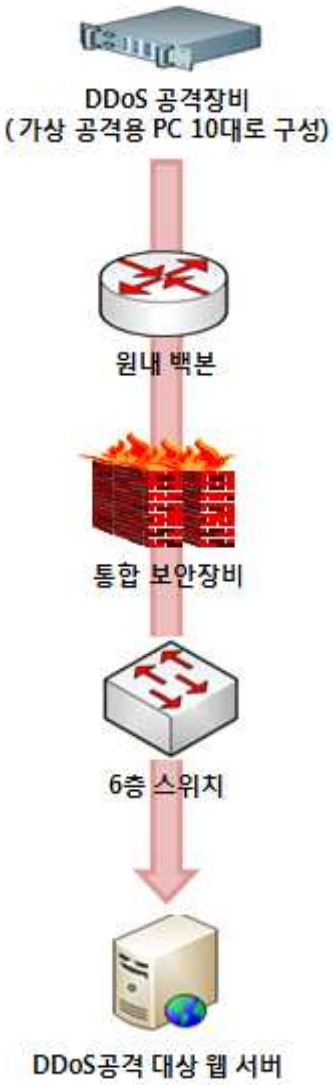
- ㅇ 기관전체(분원, 지원 포함)에 대한 불법 AP 탐지 수행
- ㅇ 기관전체 불법 AP 탐지현황을 통한 사용자 보안의식 제고
- ㅇ 무선 AP 센서를 통한 1차적 불법 AP 차단 및 향후 효과적 차단 방법 분석

Ⅱ 원내망 테스트 수행 결과 분석

1. 1차 원내망 테스트 수행 현황 분석

□ 원내 테스트 망 구성도

- ㅇ DDoS 공격 전용 장비를 통한 통합 보안장비 원내망 테스트 수행
- ㅇ 가상 공격용 PC 10대를 통해 DDoS 공격 한계점을 높임



<그림 1>1차 원내망 테스트 구성도

□ 1차 원내망 테스트 수행표

유형	순번	공격종류	공격량			네트워크 상태	홈페이지 지연여부
			봇넷IP개수	HTTP세션수/초	대역폭		
복합공격	①	TCP+Slowloris	10	14,000	100	단절	접속불가
	②	TCP+Cache Control Attack	10	1,000	200	정상작동	정상
			10	5,000	200	단절	접속불가
	③	TCP+정상get+Sloloris	10		500	정상작동	정상
플러딩	④	TCP Random Flooding			100	모의훈련 중단	모의훈련 중단
					300		
	⑤	UDP Flooding			100		
					300		
	⑥	ICMP Flooding			100		
					300		
세션	⑦	Establish (정상 GET)	10	14000			
			10	20,000			
부하가중	⑧	Http POST	10	14,000			
			10	20,000			
	⑨	Slowloris	10	14,000			
			10	20,000			
	⑩	Cache Control Attack	10	14,000			
			10	20,000			

<표 1> 1차 원내망 테스트 수행표

- 2014년 08월 26일 안정적인 운영 및 성능향상을 위한 1차 원내망
테스트를 진행 하였다. 그 결과 ①번 복합공격을 진행 중 원내 네트워크
단절 현상이 발생하였다.

- 원내망 네트워크 단절 후 초당 세션수와 패킷수를 조절 하여 테스트를
실시한 결과 1000 세션에서는 정상적으로 작동 하였으나 5000세션에서
네트워크 단절 현상이 발생하였다.

150.183.89.1(방화벽 상단 게이트웨이)에서 Ping 테스트 시 Request TimeOut 현상 발생

□ 1차 원내망 테스트 수행 분석

- 2014. 08. 26 1차 원내망 테스트에서 ①번 테스트(초당 세션 14000 / 대역폭
100Mbps) 결과 네트워크 단절현상이 발생하였다.

- ①번 DDoS 공격 테스트 후 초당 세션 1000으로 조정하여 테스트 진행
결과 네트워크 정상 작동 하였다.

150.183.89.1에서 Ping 테스트 시 Request TimeOut 현상 발생(방화벽 상단 게이트웨이

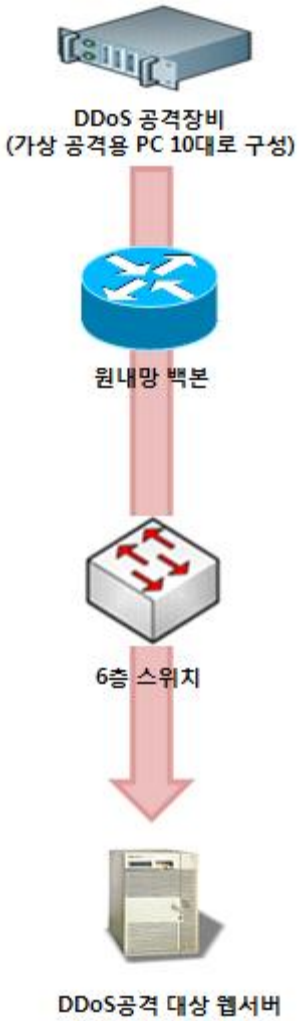
- 초당 세션 5000으로 조정하여 DDoS공격 테스트 진행 결과 네트워크 단절
현상 발생 하였다.

- 1차 원내망 테스트를 통해 원내망의 네트워크 단절 발생 가능성을 확인
하였으며, 차후 정확한 원인 분석을 위한 2차 원내망 테스트를 진행

2. 2차 원내망 테스트 수행 현황 분석

□ 테스트 망 구성도

- ㅇ 2차 원내망 테스트 구성 변경
- ㅇ 2차 원내망 테스트는 DDoS 공격 장비와 네트워크 스위치를 직접 연결하여 진행(통합 UTM 장비 배제)
- ㅇ KISTI 원내망 DDoS 공격 테스트 관련 망 구성도는 <그림 1>과 같다.



<그림 2>2차 원내망 테스트 구성도

□ 2차 원내망 테스트 수행표

유형	순번	공격종류	공격량			네트워크 상태	홈페이지 지연여부
			봇넷IP개수	HTTP세션수/초	대역폭 (Mbps)		
복합공격	①	T C P + Establish (정상 GET)	10	1000	100	정상	간간히 지연
			10	5000	100	정상	지연
			10	8000	100	정상	접속불가
			10	14000	100	정상	접속불가
			10	20000	100	정상	접속불가
			10	25000	100	정상	접속불가
	②	T C P + Establish (정상 GET) + HTTP POST	10	14000	300	정상	접속불가
플러딩	④	TCP Random Flooding			100	정상	정상
					300	정상	정상
					600	정상	간간히 지연
					900	정상	간간히 지연
부하가중	⑤	Cache Control Flooding	10	20000		정상	접속불가
플러딩	⑥	UDP Flooding			500	정상	정상

<표 2>2차 원내망 테스트 수행표

- 2014. 08. 27 2차 원내망 테스트 에서는 기존의 통합UTM 장비를 배제하고, DDoS공격 장비와 원내 네트워크 스위치를 직접 연결하여 공격 테스트를 진행 하였다.

- 1차 테스트 시 네트워크 단절 현상이 발생 하였던 복합공격 위주의 테스트를 실시한 결과 원내 네트워크는 모두 정상작동 하였으나, 공격 대상 웹서버는 지연 및 접속불가 현상이 발생 하였다.

□ 2차 원내망 테스트 수행 결과 및 분석

- 2014. 08. 27 실시한 2차 원내망 테스트에서는 1차 테스트 시의 방화벽(통합UTM)을 배제하고 DDoS 공격 장비와 네트워크 스위치를 직접 연결하여 테스트를 진행 하였다.

- 복합 공격 위주의 DDoS 공격으로 대역폭 100Mbps / 세션수 1000 ~ 25000 사이에서 네트워크는 정상 작동 하였으나, 공격 대상 웹서비스는 지연 및 접속불가 현상이 발생 하였다.

- 복합 공격 이후 TCP Random Flooding 공격 및 HTTP 세션 공격을 진행 하였으며 원내 네트워크는 모두 정상적으로 작동 하였다.

- 2차 원내망 테스트를 통해 통합UTM(방화벽) 장비를 기점으로 원내 네트워크 단절이 발생하는 것으로 판단 되어 지며, 통합UTM 장비 내의 정확한 원인 분석을 위한 제조사(WatchGuard)측의 계측기를 이용한 3차 테스트를 진행.

3. 3차 원내망 테스트 수행 현황 분석

□ 테스트 망 구성도

- ㅇ 3차 원내 DDoS 공격 테스트는 제조사 측이 임대한 DDoS 공격 전용 장비를 이용하여 진행 하였다.
- ㅇ 1차 원내망 테스트와 동일한 구성도에 DDoS 공격장비를 제조사 측의 계측기로 교체 하여 진행 하였다.
- ㅇ KISTI 원내망 DDoS 공격 테스트 관련 망 구성도는 <그림 1>과 같다

<그림 2>3차 원내망 테스트 구성도

□ 3차 원내망 테스트 수행표

유형	공격종류	공격량			네트워크 상태	방화벽 정책설정	홈페이지 서비스 지연여부
		공격IP개수	HTTP패킷 수/초	대역폭 (Mbyte)			
복합공격 및 부하가중	TCP+정상get	10	14000	100	단절	ANY	서비스지
		10	14000	100	단절	ANY	서비스지
		10	14000	100	단절	ANY	서비스지
	Http POST	10	20000	-	단절	ANY	접속불가
	TCP+정상get	10	14000	100	단절	ANY	서비스지
		10	20000	300	단절	ANY	접속불가

<표 3>3차 원내망 테스트 수행표

- 2014. 11. 19 3차 원내망 테스트 진행 시 네트워크 단절현상 확인을 위해 제조사 측의 계측기를 이용하여 DDoS 공격 테스트 진행 하였다

□ 3차 원내망 테스트 수행 결과 및 분석

- 2014. 11. 19 실시한 3차 DDoS 공격 테스트는 제조사 측의 계측장비를 이용하여 보다 정확한 원내 네트워크 단절 현상에 대한 원인 분석을 실시 하였다.

- 계측 장비를 이용한 원내 DDoS 공격 테스트 결과 1 ~ 2차 테스트 시 발생하였던 네트워크 단절 현상이 동일하게 발생 하였다.

- 3차 원내망 테스트 수행 중 통합UTM(방화벽) 장비의 설정 문제를 확인하였고, 정확한 분석 수행을 위해 테스트 자료를 토대로 정밀 분석을 실시 하였다.

4. 원내망 테스트 수행 결과 종합분석

□ 원내망 테스트 수행 결과

ㅇ 총3회(DDoS공격 장비 2회 + 계측기 1회)에 걸쳐 해당 이슈를 확인하기 위하여 테스트 진행 하였다.

ㅇ 그 결과 동일 조건(동일장비, 동일버젼, 통일 테스트 시나리오)으로 원내 테스트 시 네트워크 단절 현상이 발생 하였다.

□ 계측 장비를 이용한 DDoS 공격 테스트 수행

ㅇ 계측장비를 이용한 테스트 진행

- IXIA사의 Breaking Point
- Watch Guard 한국 지사의 계측장비를 통한 원인분석 테스트 수행
- 3차 테스트간 앞서 진행된 1 ~ 2 차 테스트와 동일한 네트워크 단절 현상 발생

□ 원내망 성능향상 테스트 시 단절현상 원인

ㅇ Watck Guard XTM 장비의 경우 Link Aggregation 모드 구성 방법으로 3가지를 지원

- Dynamic(802.3ad) : 묶여진 모든 링크에 대해 다이나믹하게 Active로 동작
- Static : 모든 Link Group 이 Active이나 수동으로 바인딩 된 장비의 링크 정보로 Group 구성.
- Active / Backup : Link Aggregation 그룹에 Join된 Member Link하나를 Active로 다른 하나를 Backup으로 설정하여 문제시 Active Link를 넘기는 방식

ㅇ 원내 Link Aggregation 모드 구성 확인 결과 장비 간 모드 불일치
현상 확인

- XTM 장비 : Active / Backup 모드로 구성.
- Cisco 백본 장비 : Link Aggregation 구성이 아닌 Vlan 설정으로 대
장비의 Link Group 트래픽 정보를 Vlan 통신으로 연결
- 패킷 분석결과 주, 예비 포트로 각각 Inbound와 Outbound 트래픽
분리되어 Flow 되고 있는 현상을 확인함
- 이와 같은 이유는 현 구성이 정상적인 Link Aggregation 구성으로
연동된 것이 아니라 한쪽 장비에만 장비 설정이 이루어져 발생된
것으로 추정

□ 원내망 테스트 시 문제점 해결방안

- 보안장비와 백본장비간 Link Aggregation 구성 확인을 통해 KISTI 원내
구성 초기 작업 간 Link Aggregation 연동을 위해 가장 많이 사용되는
표준 Dynamic 구성(802.3ad) 테스트 시 백본 장비와 보안장비 간 연동이
제한되는 부분을 확인하였다.

- 이에 대한 해결방안으로 WatchGuard 장비와 Cisco 장비 간 해당 표준
프로토콜 구성 방안을 정확하게 확인하여 최적의 적용 방안으로 변경
구성 및 적용을 할 계획이며, 향후 원내 네트워크의 보안성 강화에 기여
할 것 으로 판단 된다.

Ⅲ 원내 무선망 점검 수행 결과 분석

1. 원내 무선AP 구성 및 정책 현황

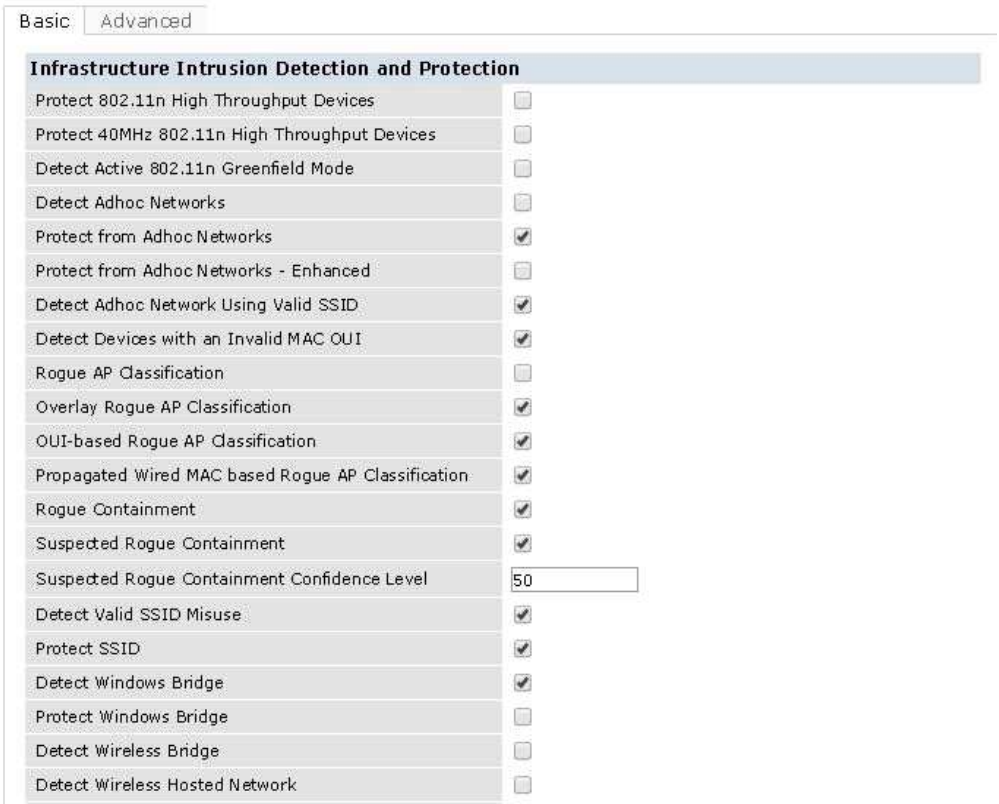
□ 원내 무선AP 구성 항목

항목	수량(대)	위치	비고
무선컨트롤러	1	대전	
무선컨트롤러	1	서울	
Access Point	50	대전	
Access Point	19	서울	

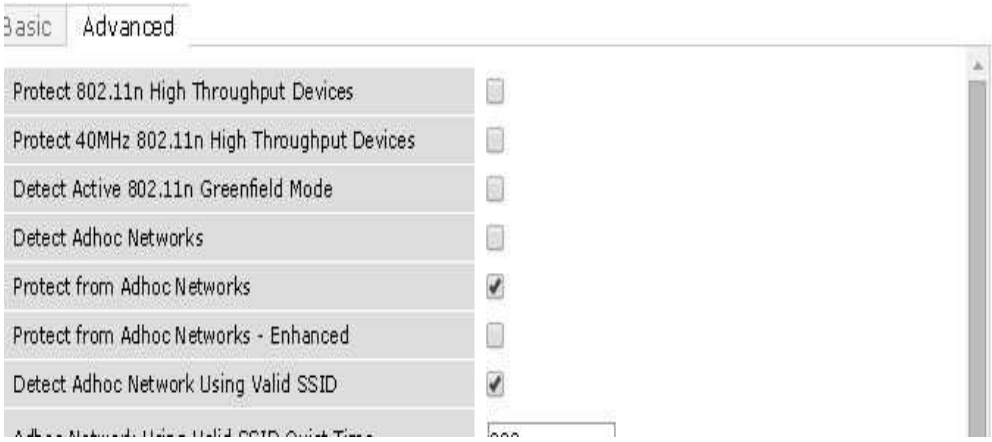
<표 4> 원내 무선AP 구성 항목

□ 원내 무선AP 정책

ㅇ 무선 AP 보안 정책 현황



o 무선 AP 네트워크 차단 정책 현황

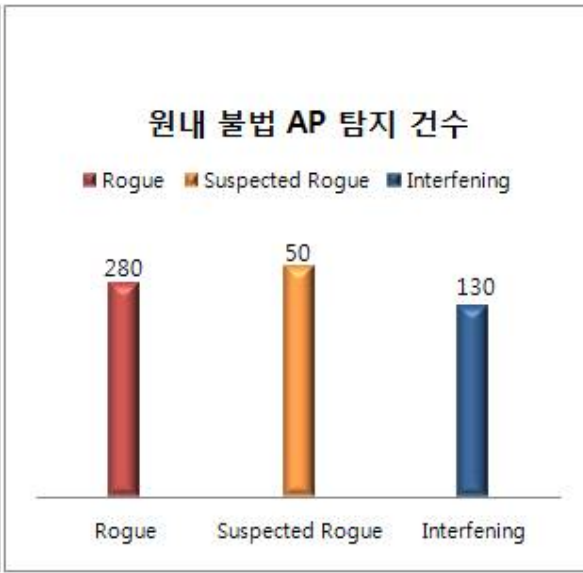


<그림 5> 무선AP 차단 정책

- <그림 5>의 무선AP의 정책을 보면 불법 AP 및 Adhoc 네트워크 차단 설정이 되어 있는 것을 볼 수 있다.
- 현재 원내의 인증된 무선 AP(Waps_01)를 제외한 기타 모든 AP는 불법으로 원내 무선 AP 센서를 통해 차단이 되고 있다.

2. 원내 불법 AP 탐지 및 차단 현황

□ 원내 불법 AP 탐지 현황



- 원내 불법 AP 탐지 현황을 보면 총 460대가 차단되고 있으며 스마트폰 태블릿 PC 등 휴대용 기기의 증가와 함께 불법 AP 차단 건수도 늘어날 것으로 판단된다.

□ 본원 1층 불법 AP 차단 분석

- 총 10대의 무선 공유기가 탐지 되어 모두 차단 되었다.

ㅇ 본원 1층 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	대전 본원 1층	10	
합 계		10건	

< 5> 본원 1층 불법AP 차단 현황

ㅇ 본원 1층 불법AP 차단 건수

<그림 7> 본원 1층 불법AP 차단 건수

ㅇ 본원 1층 불법AP 차단 세부 현황

구분	Bssid	Essid	Chan	Ap-type
무선공유기	d8:c7:c8:de:fa:e0	Welcome_KAIST	1	Rogue
무선공유기	64:e5:99:e6:e2:1c	IBFOOD	9	Rogue
무선공유기	28:c6:8e:74:f9:a7	Netgear_Dooho_2.4G	1	Rogue
무선공유기	00:08:9f:09:30:68	visualization_lab	9	Rogue
무선공유기	d8:c7:c8:de:fa:a1	Welcome_KAIST	1	Rogue
무선공유기	00:26:66:86:9b:f8	math_top	11	Rogue
무선공유기	64:e5:99:3f:bb:ec	wifi	12	Rogue
무선공유기	94:d7:71:e7:01:3d	1004	1	Rogue
무선공유기	96:44:52:a4:46:86	cyberEnv	1	Rogue
무선공유기	94:44:52:a4:46:85	숨김	1	Rogue

<표 6> 본원 1층 불법AP 차단 세부 현황

□ 본원 2층 불법AP 차단 분석

- 공유기 3대, 통신사 4대, 테더링 1대 가 탐지 되었으며 모두 차단 되었다

ㅇ 본원 2층 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	대전 본원 2층	3	
통신사AP	대전 본원 2층	4	
테더링	대전 본원 2층	1	
합 계		**8 건**	

< 7> 본원 2층 불법AP 차단 현황

ㅇ 본원 2층 불법AP 차단 건수

ㅇ 본원 2층 불법AP 차단 세부 현황

구분	Bssid	Essid	Chan	Ap-type
무선공유기	00:1d:7e:2b:e3:81	linksys	11	Rogue
무선공유기	24:a2:e1:ee:b7:d6	user***Wi-Fi *****	6	Rogue
무선공유기	20:c9:d0:18:66:39	nadia-Time-Capsule	11	Rogue
통신사AP	00:40:5a:a8:3c:fb	FREE_U+zone	13	Rogue
통신사AP	00:40:5a:a8:3c:fa	U+zone	13	Rogue
통신사AP	00:40:5a:a8:3c:f8	#LG@Vo1P*Service&	13	Rogue
통신사AP	00:40:5a:a8:3c:f9	LG Uplus	13	Rogue
테더링	f8:84:f2:b7:96:73	AndroidHotspot9379	hotspot	Rogue

<표 8> 본원 2층 불법AP 차단 세부 현황

□ 본원 3층 불법AP 차단 분석

- 공유기 7대, 통신사 6대가 탐지 되었으며 모두 차단 되었다.

ㅇ 본원 3층 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	대전 본원 3층	7	
통신사AP	대전 본원 3층	6	
합 계		**13 건**	

< 9> 본원 3층 불법AP 차단 현황

ㅇ 본원 3층 불법AP 차단 건수

ㅇ 본원 3층 불법AP 차단 세부 현황

구 분	Bssid	Essid	Chan	Ap-type
무선공유기	00:40:5a:a8:3c:f8	숨김	13	Rogue
무선공유기	24:a2:e1:ee:b7:d6	user*** Wi-Fi ********	6	Rogue
무선공유기	00:26:66:58:a9:12	iptime	11	Rogue
무선공유기	9c:d6:43:af:16:06	hyunjun	4	Rogue
무선공유기	28:cf:da:ac:94:b5	STN	1	Rogue
무선공유기	9c:d6:43:af:16:08	숨김	4	Rogue
무선공유기	94:d7:71:e7:01:3d	숨김	1	Rogue
통신사AP	00:40:5a:a8:3c:f9	LG Uplus	13	Rogue
통신사AP	00:08:5b:76:ed:39	U+NetED3B	3	Rogue
통신사AP	00:40:5a:a8:3c:fb	FREE_U+zone	13	Rogue
통신사AP	00:40:5a:a8:3c:fa	U+zone	13	Rogue
통신사AP	00:08:5b:45:68:f1	U+Net68F3	3	Rogue
통신사AP	00:08:5b:76:ed:3a	U+zone	3	Rogue

<표 10> 본원 3층 불법AP 차단 세부 현황

□ 본원 5층 불법AP 차단 분석

- 공유기 10대, 통신사 2대가 탐지 되었으며 모두 차단 됨.

ㅇ 본원 5층 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	대전 본원 5층	10	
통신사 AP	대전 본원 5층	2	
합 계		**12 건**	

< 11> 본원 5층 불법AP 차단 현황

ㅇ 본원 5층 불법AP 차단 건수

ㅇ 본원 5층 불법AP 차단 세부 현황

구 분	Bssid	Essid	Chan	Ap-type
무선공유기	28:cf:da:ac:94:b5	STN	1	Rogue
무선공유기	28:cf:da:ac:94:b6	STN	149	Rogue
무선공유기	00:26:66:58:a9:12	iptime	11	Rogue
무선공유기	02:15:99:10:87:d1	DIRECT-LEC460 Series	11	Rogue
무선공유기	00:26:66:6c:5d:18	ddhanbit3th	9	Rogue
무선공유기	94:44:52:a4:46:87	cyberEnv_5GHz	48	Rogue
무선공유기	94:44:52:a4:46:85	숨김	1	Rogue
무선공유기	96:44:52:a4:46:86	cyberEnv	1	Rogue
무선공유기	32:cd:a7:29:10:6e	DIRECT-DgC460 Series	11	Rogue
무선공유기	06:30:0d:14:23:4a	숨김	1	Rogue
통신사AP	0a:30:0d:14:23:4a	T wifi home	1	Rogue
통신사AP	00:30:0d:14:23:4a	SK_WiFi234B	1	Rogue

<표 12> 본원 5층 불법AP 차단 세부 현황

□ 본원 6층 불법AP 차단 분석

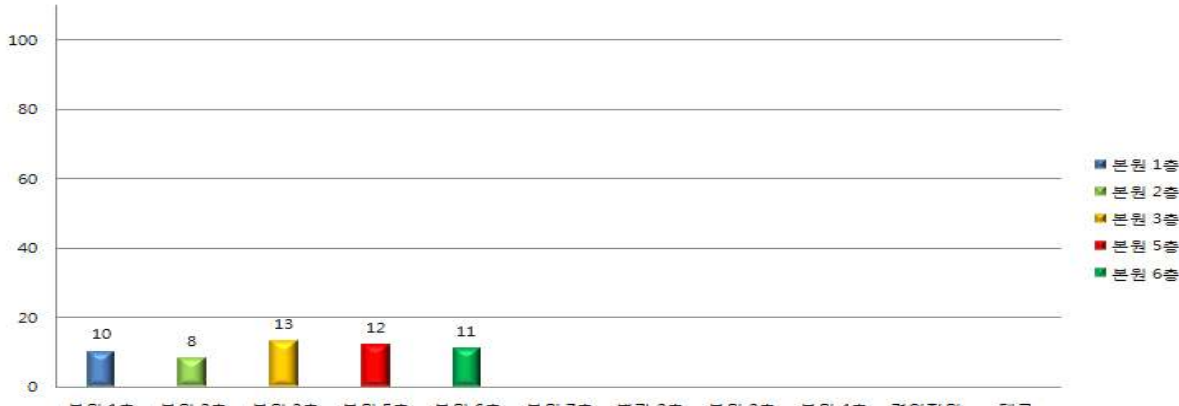
- 공유기 10대, 통신사 1대가 탐지 되었으며 모두 차단 됨.

ㅇ 본원 6층 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	대전 본원 6층	10	
통신사 AP	대전 본원 6층	1	
합 계		**11 건**	

< 13> 본원 6층 불법AP 차단 현황

ㅇ 본원 6층 불법AP 차단 건수



ㅇ 본원 6층 불법AP 차단 세부 현황

구 분	Bssid	Essid	Chan	Ap-type
무선공유기	00:26:66:6c:5d:18	ddhanbit3th	9	Rogue
무선공유기	00:26:66:58:a9:12	iptime	11	Rogue
무선공유기	28:cf:da:ac:94:b5	STN	1	Rogue
무선공유기	28:cf:da:ac:94:b6	STN	149	Rogue
무선공유기	02:15:99:10:87:d1	DIRECT-LEC460 Series	11	Rogue
무선공유기	96:44:52:a4:46:86	cyberEnv	1	Rogue
무선공유기	94:44:52:a4:46:85	숨김	1	Rogue
무선공유기	32:cd:a7:29:10:6e	DIRECT-DgC460 Series	11	Rogue
무선공유기	64:e5:99:4c:22:90	DHCP3F	11	Rogue
무선공유기	00:90:a2:0e:47:c0	숨김	7	Rogue
통신사AP	00:27:1c:23:66:b5	U+Net66B7	6	Rogue

<표 14> 본원 6층 불법AP 차단 세부 현황

□ 본원 7층 불법AP 차단 분석

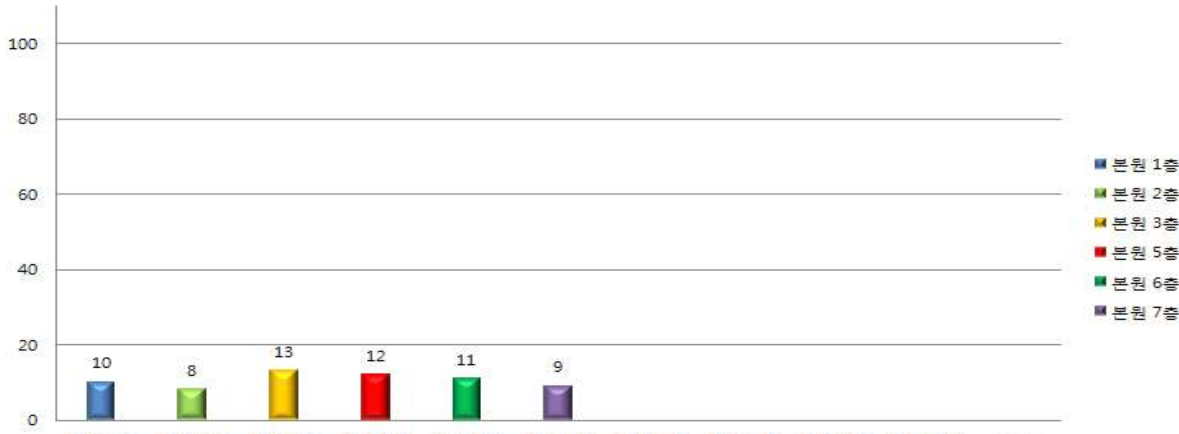
- 공유기 7대, 통신사 2대가 탐지 되었으며 모두 차단 됨.

ㅇ 본원 7층 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	대전 본원 7층	7	
통신사 AP	대전 본원 7층	2	
합 계		**9 건**	

< 15> 본원 7층 불법AP 차단 현황

ㅇ 본원 7층 불법AP 차단 건수



ㅇ 본원 7층 불법AP 차단 세부 현황

구 분	Bssid	Essid	Chan	Ap-type
무선공유기	00:26:66:6c:5d:18	ddhanbit3th	9	Rogue
무선공유기	02:15:99:10:87:d1	DIRECT-LEC460 Series	11	Rogue
무선공유기	00:26:66:58:a9:12	iptime	11	Rogue
무선공유기	28:cf:da:ac:94:b5	STN	1	Rogue
무선공유기	32:cd:a7:29:10:6e	DIRECT-DgC460 Series	11	Rogue
무선공유기	00:26:66:9d:0f:ba	jjuhappy	11	Rogue
무선공유기	00:27:1c:40:94:30	숨김	9	Rogue
통신사 AP	00:27:1c:40:94:31	U+Net9433	9	Rogue
통신사 AP	00:27:1c:40:94:32	U+zone	9	Rogue

<표 16> 본원 7층 불법AP 차단 세부 현황

□ 별관 2층 불법AP 차단 분석

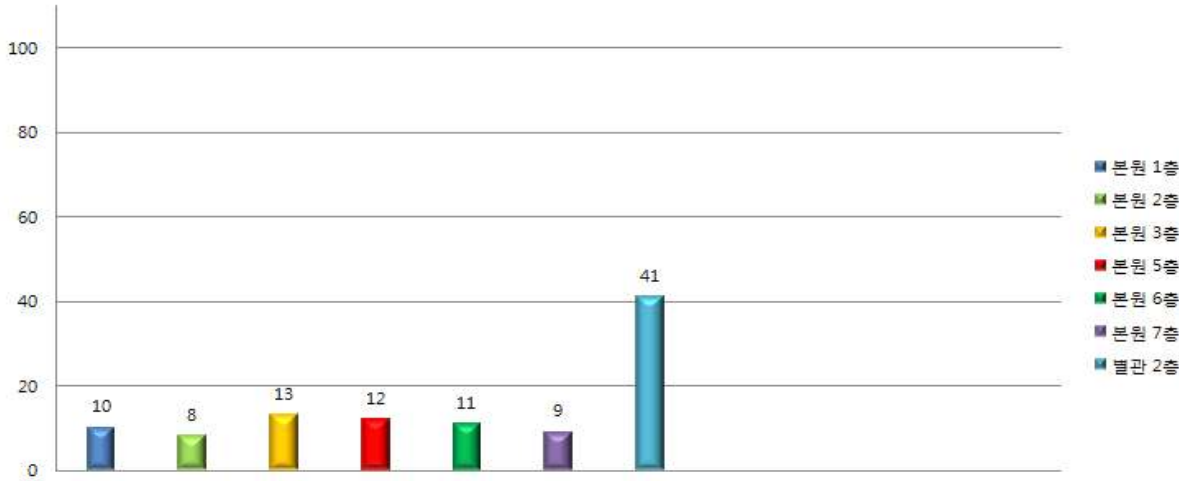
- 공유기 30대, 통신사 11대가 탐지 되었으며 모두 차단 됨.

ㅇ 별관 2층 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	대전 별관 2층	30	
통신사 AP	대전 별관 2층	11	
합 계		**41 건**	

< 17> 별관 2층 불법AP 차단 현황

ㅇ 별관 2층 불법AP 차단 건수



ㅇ 별관 2층 불법AP 차단 세부 현황

구 분	Bssid	Essid	Chan	Ap-type
무선공유기	b2:a9:05:10:ee:b0	hpsetup	6	Rogue
무선공유기	90:72:40:10:02:3e	Apple Network 10023f	6	Rogue
무선공유기	28:c6:8e:74:f9:a7	Netgear_Dooho_2.4G	1	Rogue
무선공유기	90:72:40:10:02:3f	Apple Network 10023f	149	Rogue
무선공유기	f4:d9:fb:67:ff:f0	Welcome_KAIST	9	Rogue
무선공유기	f4:d9:fb:67:ff:ef	Welcome_KAIST	9	Rogue
무선공유기	f4:d9:fb:67:ff:f1	Welcome_KAIST	9	Rogue
무선공유기	f4:d9:fb:67:ff:ee	Welcome_KAIST	9	Rogue
무선공유기	f4:d9:fb:67:ff:ed	Welcome_KAIST	9	Rogue
무선공유기	00:08:9f:a9:9f:a0	network	5	Rogue
무선공유기	00:08:9f:bf:43:f0	iptime4130	1	Rogue
무선공유기	64:e5:99:da:d5:28	dorm_ksj	1	Rogue
무선공유기	00:9c:85:99:bc:97	COM_AP	8	Rogue
무선공유기	64:e5:99:59:3a:d8	Cavaliero	13	Rogue
무선공유기	64:e5:99:e8:db:10	spsp	8	Rogue
무선공유기	64:e5:99:3f:bb:ec	wifi	12	Rogue
무선공유기	c8:3a:35:f5:92:b8	room1301	12	Rogue
무선공유기	64:e5:99:19:e3:4a	Bon	9	Rogue
무선공유기	00:26:66:8f:85:fc	leekyu	7	Rogue
무선공유기	c8:3a:35:fa:a0:a8	AirCubeSY	1	Rogue
무선공유기	64:e5:99:a9:7e:c4	****	1	Rogue
무선공유기	90:e6:ba:d3:c9:f4	HJ-WIFI	1	Rogue
무선공유기	00:08:5b:5f:ce:28	숨김	3	Rogue
무선공유기	6c:19:8f:cb:89:d0	Barnone	1	Rogue
무선공유기	04:8d:38:16:b0:f7	Winpark Network	10	Rogue
무선공유기	00:26:66:5b:d8:a0	iptime	11	Rogue
무선공유기	00:40:5a:d9:b5:a0	#LG@Vo1P*Service&	3	Rogue
무선공유기	00:26:66:27:f0:ca	SK	9	Rogue
무선공유기	64:e5:99:28:7b:54	singingzebra	5	Rogue
무선공유기	00:08:9f:0c:f4:a4	숨김	9	Rogue
통신사AP	00:30:0d:a3:36:c0	SK_WiFi36C1	1	Rogue
통신사AP	0a:30:0d:a3:36:c0	T wifi home	1	Rogue
통신사AP	06:30:0d:a3:36:c0	SK_VoIP	1	Rogue
통신사AP	00:27:1c:4a:b5:99	U+NetB59B	1	Rogue
통신사AP	00:27:1c:36:eb:09	U+NetEB0B	1	Rogue
통신사AP	00:08:5b:5f:ce:2a	U+zone	3	Rogue
통신사AP	00:27:1c:4a:b5:9a	U+zone	1	Rogue
통신사AP	00:27:1c:58:92:d1	U+Net92D3	9	Rogue
통신사AP	00:27:1c:58:92:d2	U+zone	9	Rogue
통신사AP	00:08:5b:5f:ce:29	U+NetCE2B	3	Rogue
통신사AP	00:40:5a:d9:b5:a2	U+zone	3	Rogue

<표 18> 별관 2층 불법AP 차단 세부 현황

□ 분원 2층 불법AP 차단 분석

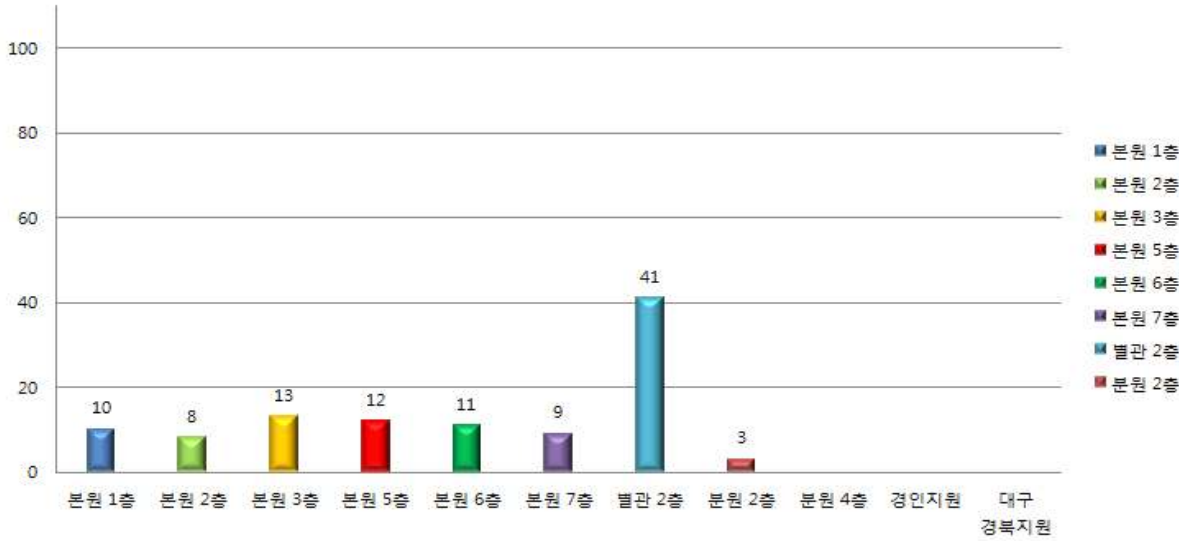
- 공유기 3대가 탐지 되었으며 모두 차단 됨.

ㅇ 분원 2층 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	서울 분원 2층	3	
합 계		**3 건**	

< 19> 분원 2층 불법AP 차단 현황

ㅇ 분원 2층 불법AP 차단 건수



<그림 14> 분원 2층 불법AP 차단 건수

ㅇ 분원 2층 불법AP 차단 세부 현황

구 분	Bssid	Essid	Chan	Ap-type
무선공유기	64:e5:99:c3:ed:b4	숨김	11	Rogue
무선공유기	02:15:99:0d:a1:e8	DIRECT-FXC410 Series	11	Rogue
무선공유기	02:2b:db:2a:52:29	HP-nomodel.5E0093	6	Interfering

<표 20> 분원 2층 불법AP 차단 세부 현황

□ 분원 4층 불법AP 차단 분석

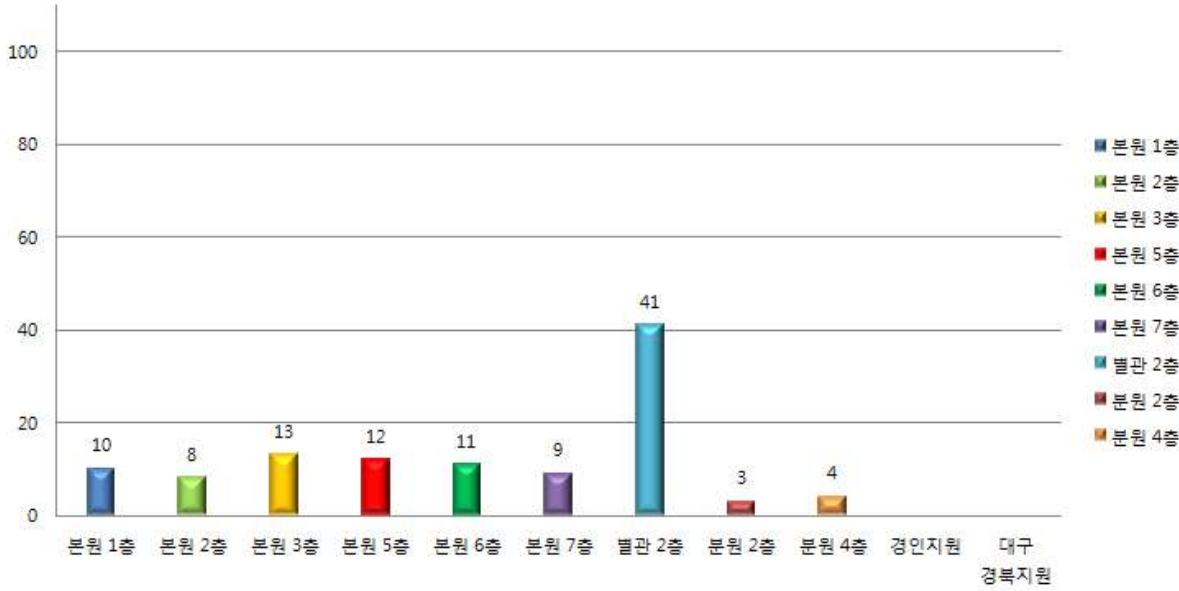
- 공유기 4대가 탐지 되었으며 모두 차단 되었다.

ㅇ 분원 4층 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	서울 분원 4층	4	
합 계		**4 건**	

< 21> 분원 4층 불법AP 차단 현황

ㅇ 분원 4층 불법AP 차단 건수



<그림 15> 분원 4층 불법AP 차단 건수

ㅇ 분원 4층 불법AP 차단 세부 현황

구 분	Bssid	Essid	Chan	Ap-type
무선공유기	00:08:9f:6e:c2:24	숨김	1	Rogue
무선공유기	00:08:9f:6e:c2:20	kangtta5G	36	Rogue
무선공유기	c4:88:e5:05:b9:5e	spj6674	6	Rogue
무선공유기	02:15:99:0d:a1:e8	DIRECT-FXC410 Series	11	Rogue

□ 경인지원 불법AP 차단 분석

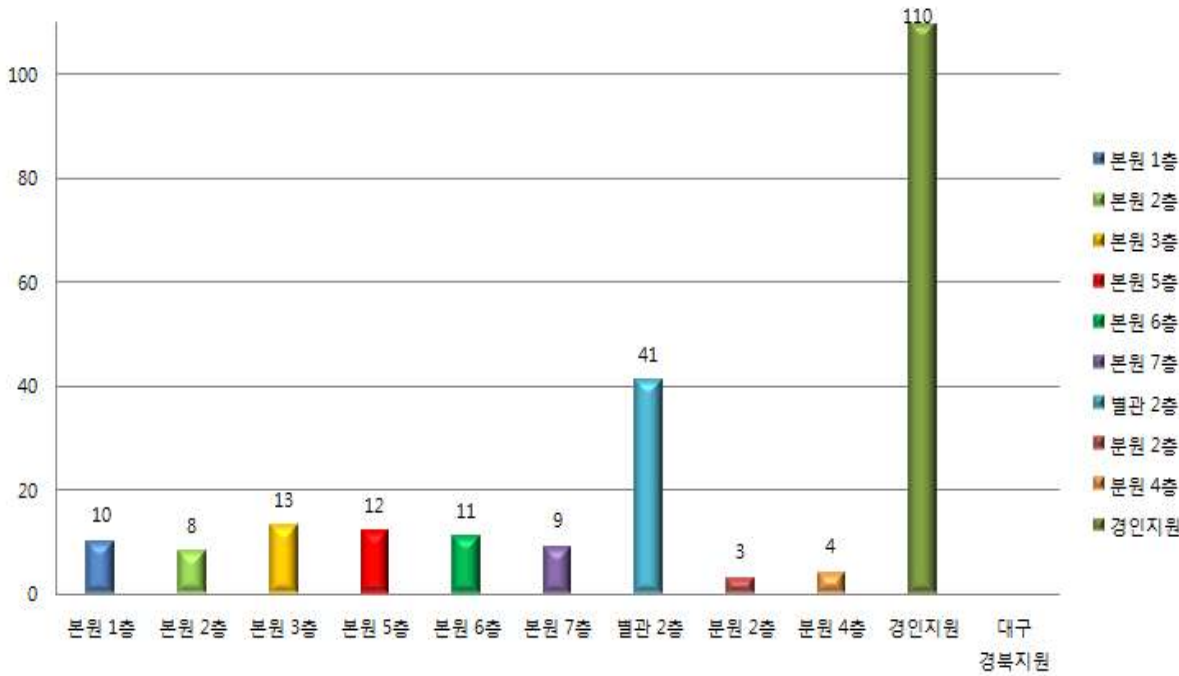
- 공유기 99대, 통신사 11대가 탐지 되었으며 모두 차단 되었다.
- 지원 특성상 인접 되어 있는 타 사무실을 통해 다수의 무선AP가 탐지 된 것으로 판단 된다.

ㅇ 경인지원 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	경인지원	99	
통신사 AP	경인지원	11	
합 계		**110 건**	

< 23> 경인지원 불법AP 차단 현황

ㅇ 경인지원 불법AP 차단 건수



<그림 16> 경인지원 불법AP 차단 건수

ㅇ 경인지원 불법AP 차단 세부 현황

구 분	Bssid	Essid	Chan	Ap-type
무선공유기	00:26:66:a1:44:fe	mi_conf	11	Rogue
무선공유기	00:0d:0b:d4:50:09	ParksystemsAP	3	Rogue
무선공유기	64:e5:99:da:c0:a8	chemon-2.4G	2	Rogue
무선공유기	00:26:66:cf:a0:dc	OliPass02	3	Rogue
무선공유기	00:08:9f:7c:a0:04	Prime2G	11	Rogue
무선공유기	00:26:66:2c:1c:10	KRCC_Lab2	2	Rogue
무선공유기	64:e5:99:ad:84:9c	nanonbrick2	5	Rogue
무선공유기	00:26:66:64:9b:2c	gsbc8	11	Rogue
무선공유기	00:08:9f:92:ab:3b	iptime	6	Rogue
무선공유기	00:26:66:2c:1c:4c	KRCC_Lab	1	Rogue
무선공유기	64:e5:99:c8:97:32	khusbc	5	Rogue
무선공유기	00:08:9f:ac:c6:20	ParkSystemsAP	6	Rogue
무선공유기	84:4b:f5:ab:d6:7c	HP-Print-7C-LaserJet 1102	6	Rogue
무선공유기	08:10:74:cf:58:4a	Chemonsmart	6	Rogue
무선공유기	d0:57:4c:09:cd:20	ag-guest	1	Rogue
무선공유기	06:0b:6b:23:ca:a2	UTIS-AUTH	157	Rogue
무선공유기	00:0b:6b:23:ca:a2	UTIS-MASTER	157	Rogue
무선공유기	00:26:66:fb:df:a8	FNF	9	Rogue
무선공유기	d0:57:4c:09:cd:21	spark	1	Rogue
무선공유기	64:e5:99:1d:ca:2e	harrys	13	Rogue
무선공유기	64:e5:99:da:96:30	iptime-B	10	Rogue
무선공유기	64:e5:99:64:85:f0	cross	36	Rogue
무선공유기	64:e5:99:0c:a4:aa	ParkSystemsAP(AS)	5	Rogue
무선공유기	04:f0:21:0a:75:07	숨김	36	Rogue
무선공유기	c8:3a:35:44:ac:90	crcfpp	6	Rogue
무선공유기	00:26:66:2c:12:4c	KRCC_OFFICE	1	Rogue
무선공유기	00:26:66:6b:cb:08	Lim and Adult	7	Rogue
무선공유기	00:08:9f:ac:fa:bc	KHCHEM	11	Rogue
무선공유기	00:08:9f:18:db:64	iptime89	9	Rogue
무선공유기	64:e5:99:1a:9e:66	academy5	11	Rogue
무선공유기	00:1f:1f:0c:3f:90	anygate_mi	11	Rogue
무선공유기	64:e5:99:ae:80:6c	scd	10	Rogue
무선공유기	3e:19:5e:b4:96:87	숨김	1	Rogue
무선공유기	00:26:66:b6:f8:b8	iptime(Crubs)	5	Rogue
무선공유기	64:e5:99:76:0c:34	Olipass03	4	Rogue
무선공유기	00:26:66:f1:4e:60	olipass01	13	Rogue
무선공유기	06:19:5e:b4:96:87	wjc_ap	1	Rogue
무선공유기	64:e5:99:9d:c1:c2	aictiptime	5	Rogue
무선공유기	00:02:a8:c8:a1:65	myLGNet	6	Rogue
무선공유기	64:e5:99:37:e4:fa	GoodLuck2You	5	Rogue
무선공유기	b2:79:ca:d8:d8:bc	hpsetup	6	Interfering
무선공유기	00:14:f2:70:8e:30	숨김	10	Rogue
무선공유기	00:40:5a:46:7e:16	myLGNet	8	Rogue
무선공유기	08:10:75:13:31:72	Rottweiler	6	Rogue
무선공유기	00:50:18:4e:22:2c	sky	11	Rogue

구 분	Bssid	Essid	Chan	Ap-type
무선공유기	00:26:66:96:06:48	jsck2	6	Rogue
무선공유기	00:08:9f:ad:8b:0c	MARGSTUDIO	9	Rogue
무선공유기	00:26:66:9c:34:50	newgenpharm	9	Rogue
무선공유기	00:26:66:94:cb:2c	INO_CAFE	5	Rogue
무선공유기	00:24:a5:13:71:74	Print (HP)	8	Rogue
무선공유기	64:e5:99:4c:15:e4	PFMS	6	Rogue
무선공유기	00:26:66:86:74:40	Ph.D.Ahn	5	Rogue
무선공유기	00:02:a8:c8:a1:64	숨김	1	Rogue
무선공유기	00:26:66:cf:a0:d8	Olipass02-5G	6	Rogue
무선공유기	64:e5:99:4f:1f:90	bio_store	36	Rogue
무선공유기	64:e5:99:fc:53:ca	GSBC10GSBC	5	Rogue
무선공유기	64:e5:99:38:df:ea	woojung1	3	Rogue
무선공유기	06:19:5e:b5:31:63	숨김	3	Rogue
무선공유기	3e:19:5e:b5:31:63	숨김	1	Rogue
무선공유기	00:26:66:12:90:50	ksc415_02	1	Rogue
무선공유기	00:0d:f0:19:cb:1c	숨김	3	Rogue
무선공유기	c8:3a:35:2d:a6:81	wevo	2	Rogue
무선공유기	00:24:01:07:57:3b	dlink	10	Rogue
무선공유기	08:10:75:c5:ab:9c	SUWONKCS 1F	13	Rogue
무선공유기	90:9f:33:11:dd:32	aictc218	8	Rogue
무선공유기	64:e5:99:de:6f:78	apple	10	Rogue
무선공유기	64:e5:99:fe:a9:2c	pilotStudy	11	Rogue
무선공유기	64:e5:99:64:85:f4	Internet4Guest	8	Rogue
무선공유기	64:e5:99:1a:8b:3e	academy4	10	Rogue
무선공유기	00:08:5b:60:ef:a8	#LG@Vo1P*Service&	2	Rogue
무선공유기	00:08:9f:ad:c6:dc	jsck1	2	Rogue
무선공유기	02:26:66:9f:43:87	SHOWMETHEMONEY	4	Rogue
무선공유기	64:e5:99:91:5b:d4	BOBMED7F	2	Rogue
무선공유기	10:6f:3f:6d:3e:96	PUBDATA	3	Rogue
무선공유기	00:26:66:22:8b:f4	C504	1	Rogue
무선공유기	00:26:66:de:37:14	RedPig	1	Rogue
무선공유기	64:e5:99:2c:43:8e	Elite	13	Rogue
무선공유기	64:e5:99:cf:fd:c4	HANS	8	Rogue
무선공유기	a0:d3:c1:df:a0:c3	HP-Print-C3-Officejet	4	Rogue
무선공유기	00:25:a6:be:66:68	숨김	1	Rogue
무선공유기	00:16:b6:3d:a5:cd	linksys_h703	6	Rogue
무선공유기	00:26:66:35:97:48	GSTEP	13	Rogue
무선공유기	00:26:66:64:8d:18	gsbc13	11	Rogue
무선공유기	00:40:5a:46:7e:15	숨김	8	Rogue
무선공유기	98:0c:82:16:3a:48	AndroidHotspot9006	6	Rogue
무선공유기	00:08:9f:70:29:40	iptime00	9	Rogue
무선공유기	00:26:66:9f:43:86	D508	4	Rogue
무선공유기	00:08:9f:0b:7d:50	숨김	9	Rogue
무선공유기	64:e5:99:bb:c3:22	iptime	11	Rogue
무선공유기	04:8d:38:18:ba:1e	netis	7	Rogue
무선공유기	00:08:9f:af:91:a4	quarry	5	Rogue
무선공유기	00:1d:73:b1:2d:e0	ParkSystemsAP	3	Rogue
무선공유기	00:26:66:8a:0d:00	KHUSBC_414	1	Rogue

구 분	Bssid	Essid	Chan	Ap-type
무선공유기	64:e5:99:58:52:1c	WinnerPhone	4	Rogue
무선공유기	00:08:5b:66:b2:f0	숨김	4	Rogue
무선공유기	00:27:1c:76:fb:d8	숨김	1	Rogue
무선공유기	00:08:9f:a5:38:44	AICT_CD_B1F	5	Rogue
무선공유기	00:e1:40:19:16:8d	janus_bb_gw200_19168D	6	Rogue
무선공유기	00:08:9f:0b:58:e4	iptime_kist	9	Rogue
무선공유기	64:e5:99:62:a1:f4	C503	2	Rogue
통신사AP	00:27:1c:76:fb:da	U+zone	1	Rogue
통신사AP	00:40:5a:97:14:42	U+zone	9	Rogue
통신사AP	00:08:5b:66:b2:f1	U+NetB2F3	4	Rogue
통신사AP	00:40:5a:97:14:41	U+Net1443	9	Rogue
통신사AP	00:08:5b:60:ef:a9	U+NetEFAB	4	Rogue
통신사AP	00:08:5b:7b:43:e1	U+Net43E3	2	Rogue
통신사AP	00:08:5b:60:ef:aa	U+zone	1	Rogue
통신사AP	00:08:5b:7b:43:e2	U+zone	11	Rogue
통신사AP	04:9f:06:90:3b:c6	T wifi zone	11	Rogue
통신사AP	00:25:a6:be:66:67	KT_WLAN_BE66	1	Rogue
통신사AP	00:08:5b:66:b2:f2	U+zone	4	Rogue

<표 26> 경인지원 불법AP 차단 세부 현황 3

□ 대구 경북지원 불법AP 차단 분석

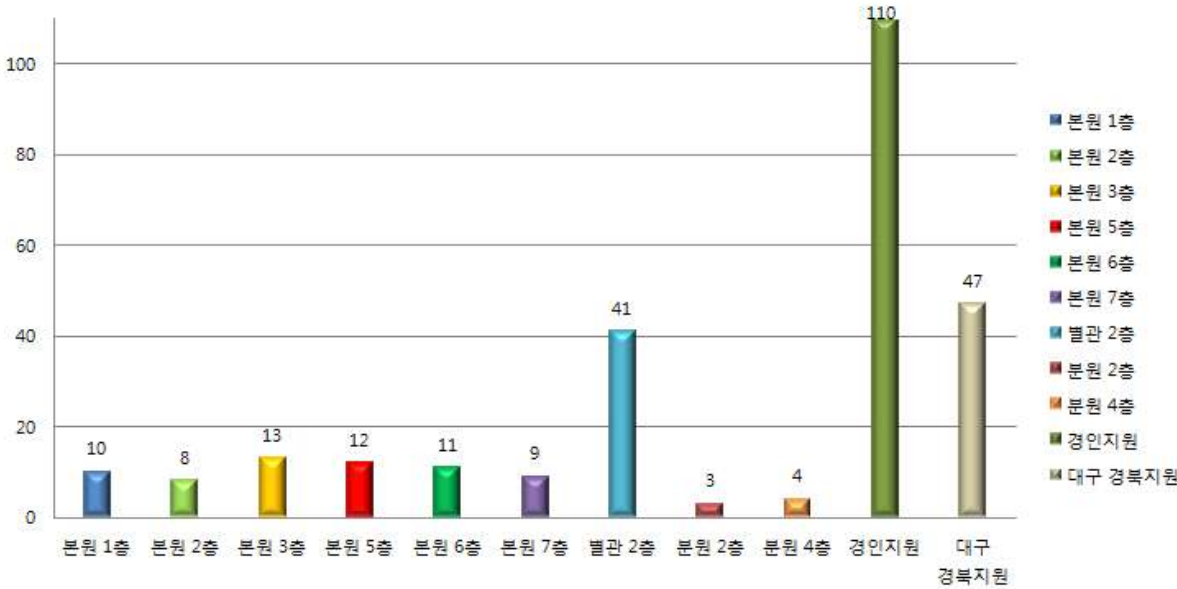
- 공유기 17대, 통신사 26대, 테더링 4대가 탐지 되었으며 모두 차단 됨

ㅇ 대구 경북지원 불법AP 차단 현황

구 분	위 치	건 수	비 고
무선공유기	대구 경북 지원	17	
통신사 AP	대구 경북 지원	26	
테더링	대구 경북 지원	4	
합 계		**47 건**	

< 27> 대구 경북지원 불법AP 차단 현황

ㅇ 대구 경북지원 불법AP 차단 건수



<그림 17> 대구 경북지원 불법AP 차단 건수

ㅇ 대구 경북지원 불법AP 차단 세부 현황

구 분	Bssid	Essid	Chan	Ap-type
통신사AP	02:30:0d:5c:29:44	ollehWiFi	5	Rogue
통신사AP	00:30:0d:4c:29:44	ollehWiFi	5	Rogue
통신사AP	00:30:0d:5d:e1:90	T wifi zone	9	Rogue
통신사AP	02:30:0d:5d:e1:90	SK_VoIP	9	Rogue
통신사AP	06:30:0d:5d:e1:90	T wifi zone_secure	9	Rogue
통신사AP	00:30:0d:5d:e3:04	T wifi zone	13	Rogue
통신사AP	06:30:0d:5d:e3:04	T wifi zone_secure	13	Rogue
통신사AP	00:30:0d:5c:4c:be	ollehWiFi	1	Rogue
통신사AP	02:30:0d:5c:4c:be	ollehWiFi	1	Rogue
통신사AP	00:30:0d:5c:38:a2	ollehWiFi	1	Rogue
통신사AP	02:30:0d:5c:38:a2	ollehWiFi	1	Rogue
통신사AP	00:30:0d:5c:28:34	ollehWiFi	5	Rogue
통신사AP	02:30:0d:5d:e7:24	SK_VoIP	13	Rogue
통신사AP	02:30:0d:5c:28:34	ollehWiFi	5	Rogue
통신사AP	06:30:0d:5d:e7:24	T wifi zone_secure	13	Rogue
통신사AP	00:30:0d:5d:e7:24	T wifi zone	13	Rogue
통신사AP	00:30:0d:81:b0:40	T wifi zone	1	Rogue
통신사AP	06:30:0d:81:b0:42	T wifi zone_secure	1	Rogue
통신사AP	02:30:0d:5c:45:26	ollehWiFi	5	Rogue
통신사AP	00:30:0d:5c:45:26	ollehWiFi	5	Rogue
통신사AP	00:30:0d:75:5e:90	T wifi zone	116	Rogue
통신사AP	0a:30:0d:75:5e:92	T wifi zone_secure	116	Rogue
통신사AP	00:30:0d:75:5e:80	T wifi zone	1	Rogue
통신사AP	02:30:0d:5c:38:a8	ollehWiFi	5	Rogue
통신사AP	00:30:0d:5c:38:a8	ollehWiFi	5	Rogue
통신사AP	06:30:0d:75:5e:82	T wifi zone_secure	1	Rogue
무선공유기	00:26:66:91:e4:08	iptime	11	Rogue
무선공유기	64:e5:99:16:36:6a	DAEGU-KPC412	2	Rogue
무선공유기	64:e5:99:ce:79:44	DAEGU-KPC	7	Rogue
무선공유기	64:e5:99:ce:79:40	iptime5G	149	Rogue
무선공유기	02:30:0d:5d:e3:04	SK_VoIP	13	Rogue
무선공유기	64:e5:99:de:a6:f8	DAEGU-KPC413	4	Rogue
무선공유기	a0:cf:5b:0f:5d:d0	EXCO	1	Rogue
무선공유기	06:30:0d:81:b0:41	SK_VoIP	1	Rogue
무선공유기	0a:30:0d:75:5e:91	숨김	116	Rogue
무선공유기	06:30:0d:75:5e:81	숨김	1	Rogue
무선공유기	a0:cf:5b:01:5c:a0	EXCO	13	Rogue
무선공유기	64:e5:99:32:35:a0	dgeupjong	48	Rogue
무선공유기	a0:cf:5b:68:90:10	EXCO	13	Rogue
무선공유기	00:25:42:e0:1b:d6	DR500GW-E01BD6	1	Rogue
무선공유기	64:e5:99:32:35:a4	dgeupjong	12	Rogue
무선공유기	a2:ea:96:23:3b:f9	Dahee's iPhone	11	Rogue
무선공유기	00:0e:e8:98:0f:58	NEPLE	6	Rogue
테더링	d0:57:85:f0:70:48	AndroidHotspot A880S	11	Rogue
테더링	78:59:5e:40:e9:b3	AndroidHotspot 4321	11	Rogue
테더링	d0:57:85:fd:e9:3c	AndroidHotspot A890S	8	Rogue

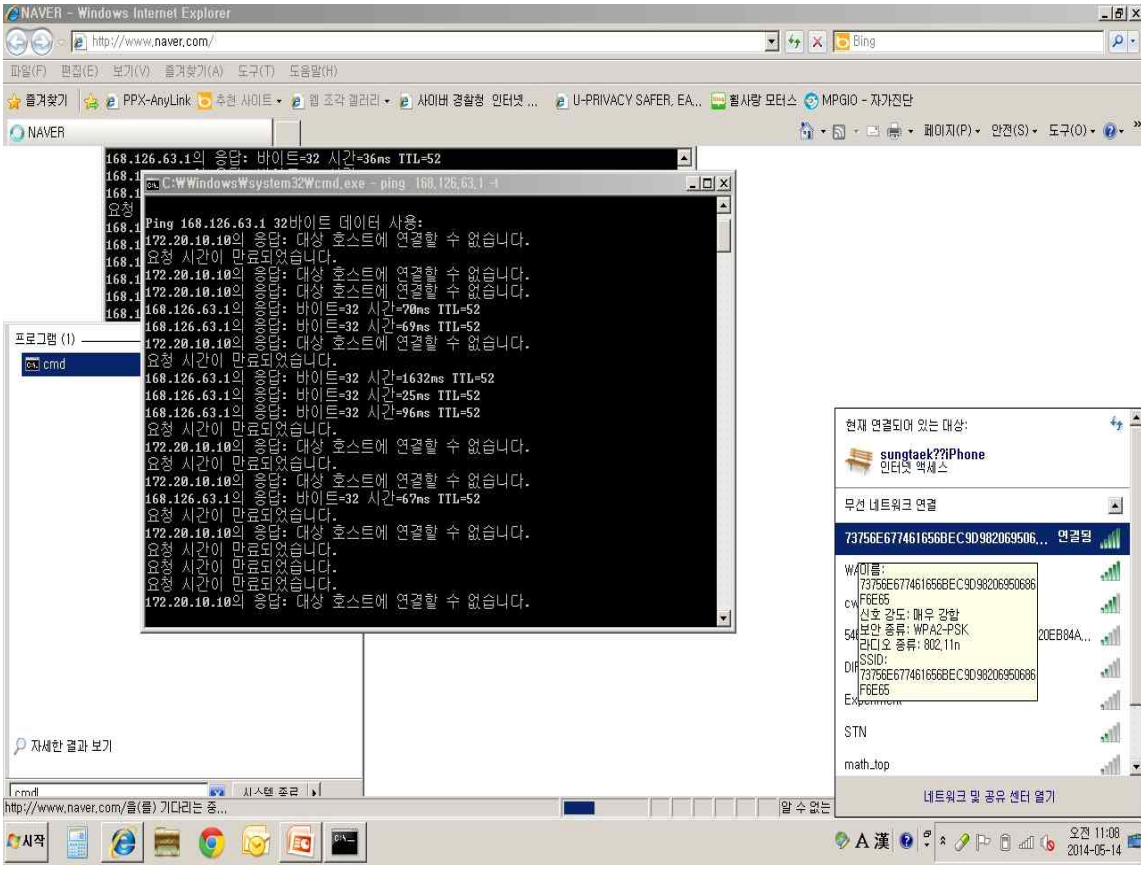
3. 원내 불법 AP 차단 방법 및 테스트 수행 분석

□ 불법 AP 탐지 및 차단 방법

- 서로 다른 위치에 있는 센서 AP의 무선 주파수 스캔을 통해 불법 AP를 검사하고, 불법 AP 의 가장 근접해 있는 AP 센서가 차단을 하는 방식이다

□ 원내 불법 AP 차단 테스트

- 일시 : 2014. 05. 14
- 장소 : 한국과학기술정보연구원 6층 회의실
- 구성 : 테더링용 핸드폰 및 노트북



<그림 18> 원내 불법AP 차단 테스트 화면

- 위 테스트 화면을 보면 핸드폰과 노트북이 연결은 되어 있으나 센서

□ 원내 불법 AP 차단 방법 관련 문제점 및 해결방안

- 현재 원내 Access Point는 분원을 포함하여 총69대 이며, 원내 불법AP는
  Access Point를 통해 차단되는 점에서 연구원 면적에 비하여 그 수량이
  부족한 문제점이 존재한다.

- 연구원내 층별로 1대 혹은 2대의 Access Point를 통해 서비스지
  이루어 지고 불법AP를 탐지 및 차단 하고 있기에, Access Point의
  센서가 미치지 않는 사각지대가 존재 하게 되며, 향후 Access Poin
  수량 보충을 통한 보안강화가 필요할 것으로 보여진다.

Ⅳ 종합분석 및 성능향상 방안

○ 2014년 8월 원내 통합UTM 장비의 도입과 함께 허가 받은 외부 접근만을 허용 함으로써 원내망의 보안이 한층 강화 되었다. 이와 더불어 업무 외 사이트 및 불법 사이트에 대한 차단 정책이 시행됨으로써 원내 네트워크 사용자의 보안이 한층 강화 되었다.

이에 날로 중요성이 강조되어 가는 네트워크 보안에 대한 강화 방안으로 통합UTM 장비를 이용한 원내망의 성능향상 테스트 수행 분석을 실시하였다. 1차 원내망 테스트 수행현황을 살펴보면 가상 공격용 PC 10대로 미리 구축 해둔 웹서버를 대상으로 공격을 수행하였고, 첫 번째 수행 테스트 결과 원내망의 네트워크가 단절된 것을 알 수 있다. http세션수/초 1000 트래픽 발생 에서는 원내 네트워크가 정상 작동하였으나 http세션수/초 5000 이상의 트래픽 발생에서는 원내 네트워크가 단절 되는 것을 확인 할 수 있었다.

이에 보다 정확한 원인 파악 및 분석을 위해 2차 원내망 테스트를 수행하였다. 2차 원내망 테스트에서는 기존의 구성도에서 통합UTM 장비를 배제하고, 공격 장비와 스위치간 직접 연결을 통해 테스트를 진행하였다. 그 결과 2차 원내망 테스트 수행표에서 보듯이 http세션수/초 1000 ~ 25000 까지의 트래픽 발생 공격에서 원내 네트워크는 정상 작동 하였다. 앞선 1차 원내망 테스트와 2차 원내망 테스트를 종합한 결과 통합UTM 장비를 트래픽이 통과 하였을때 문제가 발생되는 것으로 분석되었다.

1, 2차 원내망 테스트 결과 분석을 바탕으로 확실한 원인파악을 위한 통합UTM 장비 제조사인 WatchGuard사의 계측기를 이용하여 3차 원내망 테스트를 진행 하였다. 3차 원내망 테스트 수행 시 원내 네트워크 단절 현상이 발생하였던 1차 원내망 테스트 구성도와 동일하게 구성하여 진행 하였으며, 공격용 DDoS 장비 대신 제조사측의 계측기를 이용하여 테스트를 수행 하였다. 결과적으로 1차 원내망 테스트 시 발생 하였던 네트워크 단절 현상이 동일하게 발생 하였으며, 계측기를 통한 분석결과 동일구간에서 트래픽이 막히는 것을 확인 할 수 있었다.

1, 2, 3차 원내망 테스트 수행 결과를 바탕으로 원내망으로 가는 트래픽이 막히는 시점이 통합UTM 보안 장비로 추정 되어, 장비 설정 간 문제점이 존재 하는지 확인 작업을 수행 하였다. 그 결과 통합UTM 장비와 원내 백본장비 간 Link Aggregation 모두 구성이 불일치 되는 현상을 확인 하였다. 모두 구성 불일치 현상에 대한 해결 방안으로 통합UTM 보안 장비와 Cisco 백본 장비 간 해당 표준 프로토콜 구성 방안을 정확하게 확인하여 최적의 적용 방안으로 변경 구성 적용을 계획 하고 있으며, 향후 DDoS 공격 등의 과다 트래픽 발생으로 인한 원내망 보안사고 예방 향상에 도움이 될 것으로 판단된다.

○ 2009년 상반기부터 원내 불법AP 차단 및 원내 사용자 인증을 통한 무선AP 사용을 위해 무선 인터넷 보안장비를 도입하여 원내 무선AP를 관리하고 있다. 무선 인터넷 보안장비의 도입으로 기존의 무분별한 불법AP 사용으로 인해 발생 할 수 있는 원내 무선망 보안사고를 예방 강화하는 효과를 보이고 있으며, 2014년 12월 현재 총69대의 Access Point를 통해 원내에 무선AP 서비스를 실시하고 있다.

2009년 도입부터 2014년 현재까지 스마트폰 등 휴대용 기기의 대량 공급과 함께 무선인터넷의 수요가 폭발적으로 늘어나게 됨에 따라 원내 사용자 무선망의 수요도 비약적으로 증가 하였다. 이에 불법AP 점검을 통해 원내의 불법AP 사용 형태와 현재 불법AP 차단 방법 및 문제점 그리고 향후 원내 무선망 보안강화와 관련된 성능향상 방안에 대해 분석을 실시 하였다.

그 결과 무선인터넷 보안장비를 통한 사용자 인증이 완료된 무선AP 외에 총 460건의 불법AP 가 탐지 및 차단 되는 것을 확인 할 수 있었다. 특히 사용자들의 무분별한 무선공유기 사용 외 에 통신사의 AP 또한 연구원 내에 많은 수가 보급 되어 있는 것을 볼 수 있었다. 이는 무선인터넷의 광범위한 보급과 함께 사용자들의 접근성 및 편의성은 대폭 향상 되었지만 그에 반해 무선망 보안사고에 대한 보안의식은 낮아 지고 있는 것을 반증하는 것으로 판단된다. 460건의 불법AP 탐지 중 무선공유기 사용이 200건으로 절반 가까이 비중을 차지 하고 있으며 특히 지원은 110건으로 본원 및 분원을 포함하여 과반수 이상을 차지하고 있었다. 이는 지원의 특성상 근접해 있는 주변 사무실의 불법AP가 다수 탐지 된 것으로 여겨지며, 향후 보안사고에 심각하게 노출되어 있는 지원 무선망에 대한 보안이 대폭 강화 되어야 할 것 이다.

연구원의 무선망 점검과 더불어 탐지된 불법AP에 대한 차단 및 방법에 대해서도 분석을 진행하였다. 현재 원내에 무선인터넷 보안장비를 통해 사용자 인증이 완료된 무선AP 외에는 모두 불법AP로 간주 되고 있으며, 원내 모든 불법AP는 Access Point를 통해 접속이 차단 되고 있다. 하지만 Access Point를 이용한 불법AP 차단 특성상 Access Point의 센서가 닿지 않는 사각지대가 존재 하기에 향후 연구원 면적 대비 Access Point의 수량

V 결론

○ 2009년 7 · 7 DDoS 공격, 2011년 3 · 3 DDoS 공격 등 IT 산업의 발달과 더불어 그에 대한 보안 취약점이 여과 없이 드러나고 있다. 또한 최근들어 대규모의 개인정보 유출 사건이 발생 하며 국민모두가 보안에 대한 인식변화가 필요한 시점이 되었다. 국민 개개인 뿐만 아니라 기업 더 나아가 정부까지 보안에 대한 중요성을 인식하고 보안에 대한 철저한 대책 강구가 필요하다. 2014년 8월부터 진행된 원내망 성능향상 테스트 분석을 통해 원내망의 보안 문제를 확인 할 수 있었고, 그에 따른 해결책을 마련 함으로써 원내망의 보안성을 강화 할 수 있었다. 향후, 발생 할 수 있는 원내망 보안사고에 대해 더욱더 철저한 대비를 위해 정기적인 성능향상 테스트 및 점검 이 필요할 것으로 판단 된다.

또한, 원내 무선망 점검 수행 분석을 보면 최근 모바일 기기의 폭발적 증가와 함께 유선망에 비해 네트워크 구축이 용이하고 운용비용이 저렴한 무선망의 사용 비중이 비약적으로 늘고 있는 것을 확인 할 수 있었다. 유선망에 비해 특히 보안이 취약한 무선망의 점검 수행 분석을 통해 원내 무선망 사용자들의 무분별한 불법AP 사용 실태를 확인 할 수 있었고, 보안의식 또한 현저히 낮다는 것을 알 수 있었다. 무선인터넷 보안장비를 통한 1차적인 원내 불법AP의 차단조치와 더불어 무선망 사용자 들의 보안의식 제고를 통해 무선공유기, 테더링 등의 불법AP 사용의 근절과 통신사에서 설치한 무선AP 철거 등 근본적인 보안 대책이 필요할 것으로 판단 된다.

향후 지속적인 원내망 및 무선망 점검 수행을 바탕으로 KISTI 원내망 의