

중소기업형 스마트 팩토리 IDS/ IPS 솔루션 개발

스마트팩토리 1조

RIP (Raspberry / Router IPS Solution)

INDEX

01 프로젝트 개요

- 팀 소개
- 프로젝트 주제
- 시장 동향 및 현황 | 보안
- 프로젝트 배경 및 목적

02 IDS / IPS 설계

- IDS / IPS Inline mirroring
- 개발 도구 및 형상 관리 도구
- 기술 설명
- DB 설계

03 프로젝트 구현

- 하드웨어 구현 환경
- 산업용 프로토콜 보안 취약성 분석
- IDS / IPS Control 프로그램 구현
- Packet Generator 프로그램 구현
- 시연 영상

04 기대효과

- 기대 효과

A blue-tinted background image showing a group of people in a meeting. One person is pointing at a document that features a bar chart. The scene is focused on collaboration and data analysis.

01

프로젝트 개요

- 팀원 소개
- 프로젝트 주제
- 시장 동향 및 현황
- 프로젝트 목적 및 필요성

RIP 팀을 소개합니다

멘토



최병욱

○(주)탐텍 - 대표이사

팀장



박동

- 정보통신공학과
- Snort 구축 및 Rules 구성
- 패킷 분석
- Packet Generater 개발
- OpenWrt 구축



이경재

- 정보통신공학과
- IDS/IPS Control C# 프로그램 개발
- Rule 수정 기능 및 Log 모니터링 기능 구현
- Oracle DB 구축 및 연동



구교원

- 컴퓨터공학과
- Suricata 구축 및 Rules 구성
- Packet Generater 개발
- OpenWrt 구축

IDS / IPS Solution, 왜 중요할까요?

사물인터넷(IoT)·스마트팩토리의 확산으로 기업의 제조 및 운영시설(OT)에 대한 보안위협이 커지고 있습니다. 과거에는 OT 환경이 폐쇄적이어서 외부 해커의 침입이 불가능했지만, 이제는 외부 네트워크와 연결되는 시스템이 하나둘씩 생기면서 해커들의 타깃이 됐습니다.

문제는 기존 OT 시스템들이 보안에 취약한 구조를 가지고 있다는 점입니다. 보안패치조차 잘 되지 않은 경우가 많고, OT 환경을 위한 보안기술도 부족합니다.



출처 : 중소벤처기업부, 중소기업 스마트 제조혁신 전략 보고회



출처 : 중소벤처기업부

IDS / IPS Solution, 왜 중요할까요?

사물인터넷(IoT)·스마트팩토리의 확산으로 기업의 제조 및 운영시설(OT)에 대한 보안위협이 커지고 있습니다. 과거에는 OT 환경이 폐쇄적이어서 외부 해커의 침입이 불가능했지만, 이제는 외부 네트워크와 연결되는 시스템이 하나둘씩 생기면서 해커들의 타깃이 됐습니다. 문제는 기존 OT 시스템들이 보안에 취약한 구조를 가지고 있다는 점입니다. 보안패치조차 잘 되지 않은 경우가 많고, OT 환경을 위한 보안기술도 부족합니다.



제조업체 61% 사이버위협 노출...시스템 중단으로 이어져

스마트팩토리 지키는 OT 보안, 신규 먹거리로 떠올라

지난해 사이버공격 중 23% 제조업에 몰려
OT 영역 신규 취약점 매년 50% 증가세

2025년 글로벌 OT 보안 시장 '102억 달러' 규모로 전망

IDS / IPS Solution, 왜 중요할까요?

사물인터넷(IoT)·스마트팩토리의 확산으로 기업의 제조 및 운영시설(OT)에 대한 보안위협이 커지고 있습니다. 과거에는 OT 환경이 폐쇄적이어서 외부 해커의 침입이 불가능했지만, 이제는 외부 네트워크와 연결되는 시스템이 하나둘씩 생기면서 해커들의 타깃이 됐습니다. 문제는 기존 OT 시스템들이 보안에 취약한 구조를 가지고 있다는 점입니다. 보안패치조차 잘 되지 않은 경우가 많고, OT 환경을 위한 보안기술도 부족합니다.



제조업체 61% 사이버위협 노출...시스템 중단으로 이어져

지원조건	
구분	지원내용
기초	- 최대 0.7억원, 총 사업비의 50% 이내 지원
고도화1	- 최대 2억원, 총 사업비의 50% 이내 지원 * 중간 1 이상 구축 기업은 보안솔루션 구축 또는 연동 필수
고도화2	- 기업당 최대 4억원, 총 사업비의 50% 이내 지원 * 보안솔루션 구축 또는 연동 필수

먹거리로 떠올라

출처:<https://www.smart-factory.kr/bsnsIntrcn/intrcnView?bsnsClCodeSe=0000002A>

2025년 글로벌 OT 보안 시장 ‘102억 달러’ 규모로 전망

시장 동향 및 현황

IDS/IPS 장비 시장 현황

| 침입 차단 시스템 임대

[단위: 원/월 VAT별도]

구분	네트워크 지원 대역폭	월 비용
IPS	~100Mbps	1,300,000원/월
	100~500Mbps	2,350,000원/월
	500~1000Mbps	4,000,000원/월
	1000Mbps이상	별도협의

(출처 :<https://www.siidc.com/security/ips/index.php>)

- 기존의 IDS / IPS 장비는 대체로 높은 가격으로 형성
- IDS / IPS 장비는 최소 200만원 이상부터 1억원까지의 가격대로 형성되어있다
- 저가형 모델의 경우 IP, Port 정도만 지정하여 감시할 수 있는 아주 단순한 기능만 제공

시장 동향 및 현황

IDS/IPS 장비 시장 현황

CISCO GPL 2022

Check Cisco Price - Cisco Global Price List Tool
Cisco Router, Switch, Firewall, Wireless AP, IP Phone Price List

Cisco

HP / HPE

Huawei

Dell

Fortinet

Juniper

More

Q ISA-3000

Search GPL

Bulk Search

Top Searched Parts By Brands

Cisco Price Changed?

What are Cisco's Hot Products?

Partner with Router-switch.com

Join An IT Community Designed to Foster Business Growth.

Apply Now

Cisco Released: May 11, 2022

#No	Product	Description	List Price (USD)	Our Price		Quote Sheet
1	ISA-3000-ENCR-K9	Industrial Security Appliance - Encryption (3DES/AES)	\$0.00		<div>Get Discount</div>	<input type="checkbox"/>
2	ISA-3000-2C2F-K9=	Industrial Security Appliance 3000 2 copper 2 fiber ports.	\$5,343.55		<div>Get Discount</div>	<input type="checkbox"/>
3	ISA-3000-2C2F-K9	Industrial Security Appliance 3000 2 copper 2 fiber ports.	\$5,343.55		<div>Get Discount</div>	<input type="checkbox"/>
4	ISA-3000-4C-K9=	Industrial Security Appliance 3000 4 copper ports.	\$5,343.55		<div>Get Discount</div>	<input type="checkbox"/>
5	ISA-3000-4C-K9	Industrial Security Appliance 3000 4 copper ports.	\$5,402.41		<div>Get Discount</div>	<input type="checkbox"/>
6	ISA-3000-4C-FTD	ISA 3000 4 copper ports FTD Unified image.	\$5,357.68		<div>Get Discount</div>	<input type="checkbox"/>
7	ISA-3000-2C2F-FTD	ISA 3000 2 copper 2 fiber ports FTD Firepower Unified Image.	\$4,725.63		<div>Get Discount</div>	<div>Live Chat</div>



Add Access Rule

Order	Title	Action
2	Inside_DMZ	Allow

Source/Destination

Applications

URLs

Users

Intrusion Policy

File policy

Logging

SOURCE

Zones

+

Networks

+

Ports

+

Inside_zone

ANY

ANY

DESTINATION

Zones

+

Networks

+

Ports/Protocols

+

dmz-zone

ANY

ANY

(출처 : <https://itprice.com/cisco-gpl/isa-3000>)

(출처 : ISA3000 User Manual)

프로젝트 목적 및 필요성

스타트업 및 중소기업용 보급형 IDS/IPS 통합 솔루션 제작



스마트팩토리 전용 IDS/IPS

- Switch와 RaspberryPi에 Snort와 Suricata를 구축
- 스마트팩토리 프로토콜 전용 Rule을 설정하여 차단 및 탐지

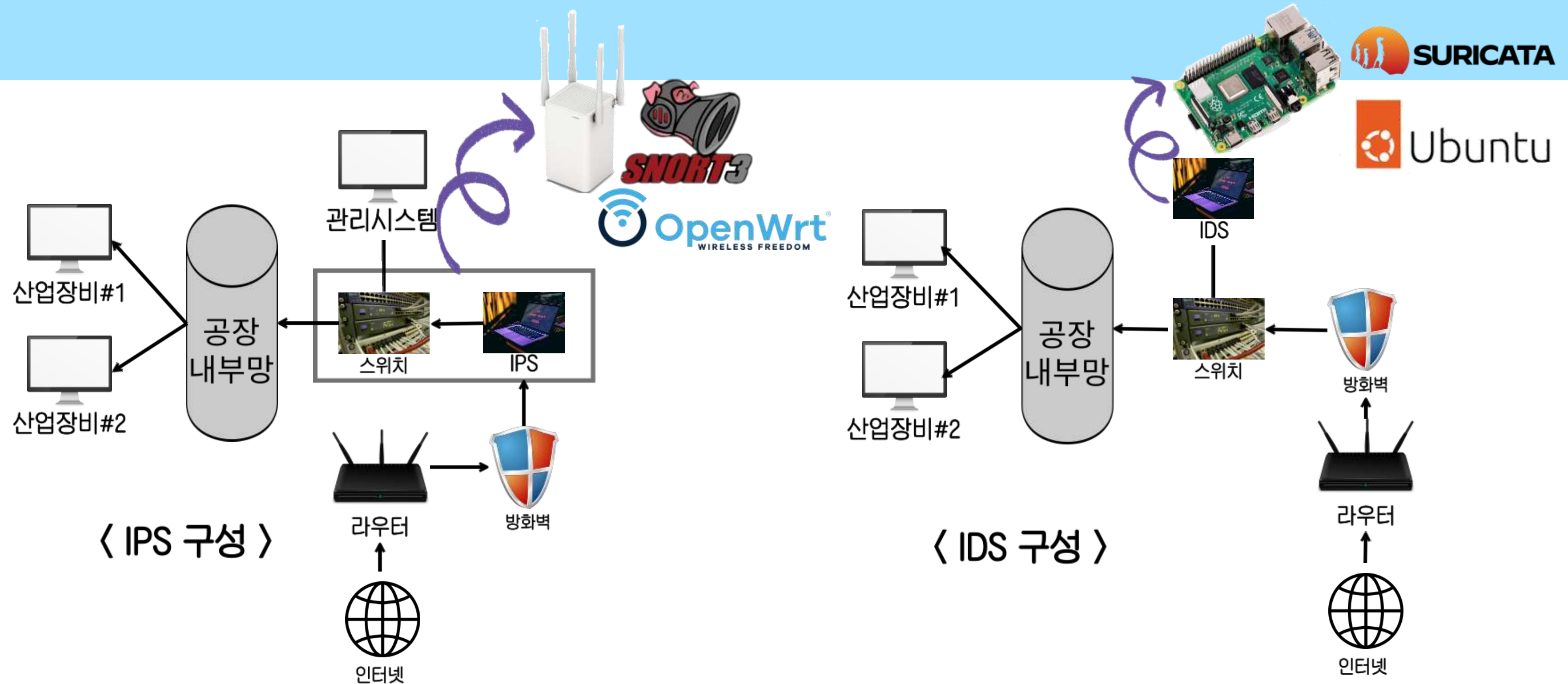
02

IPS / IDS 설계

- IPS / IDS Inline mirroring
- 개발 도구 및 형상 관리 도구
- 기술 설명
- DB 설계

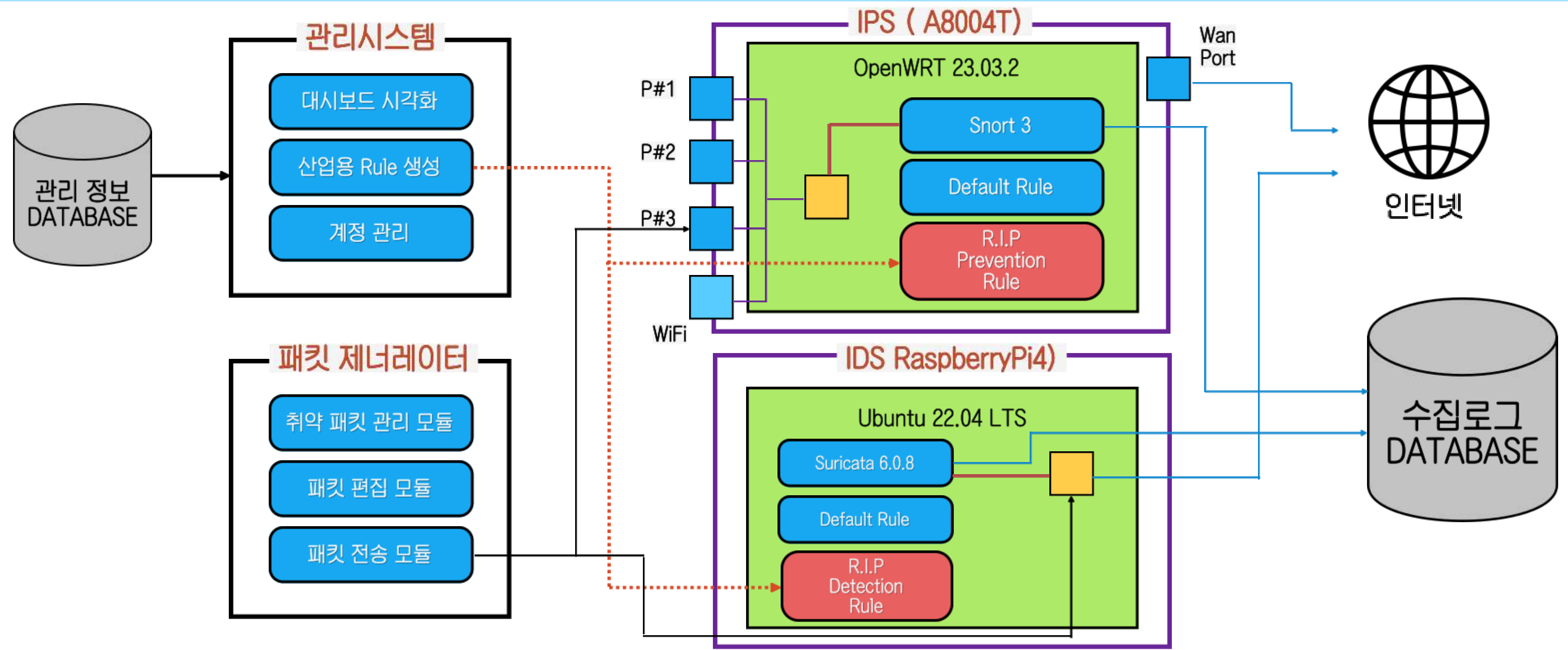
IDS / IPS 적용 네트워크 구성도

IPS / IDS



R.I.P IDS / IPS 시스템 구성도

R.I.P IDS / IPS



개발 도구 및 형상 관리 도구

형상 관리 도구

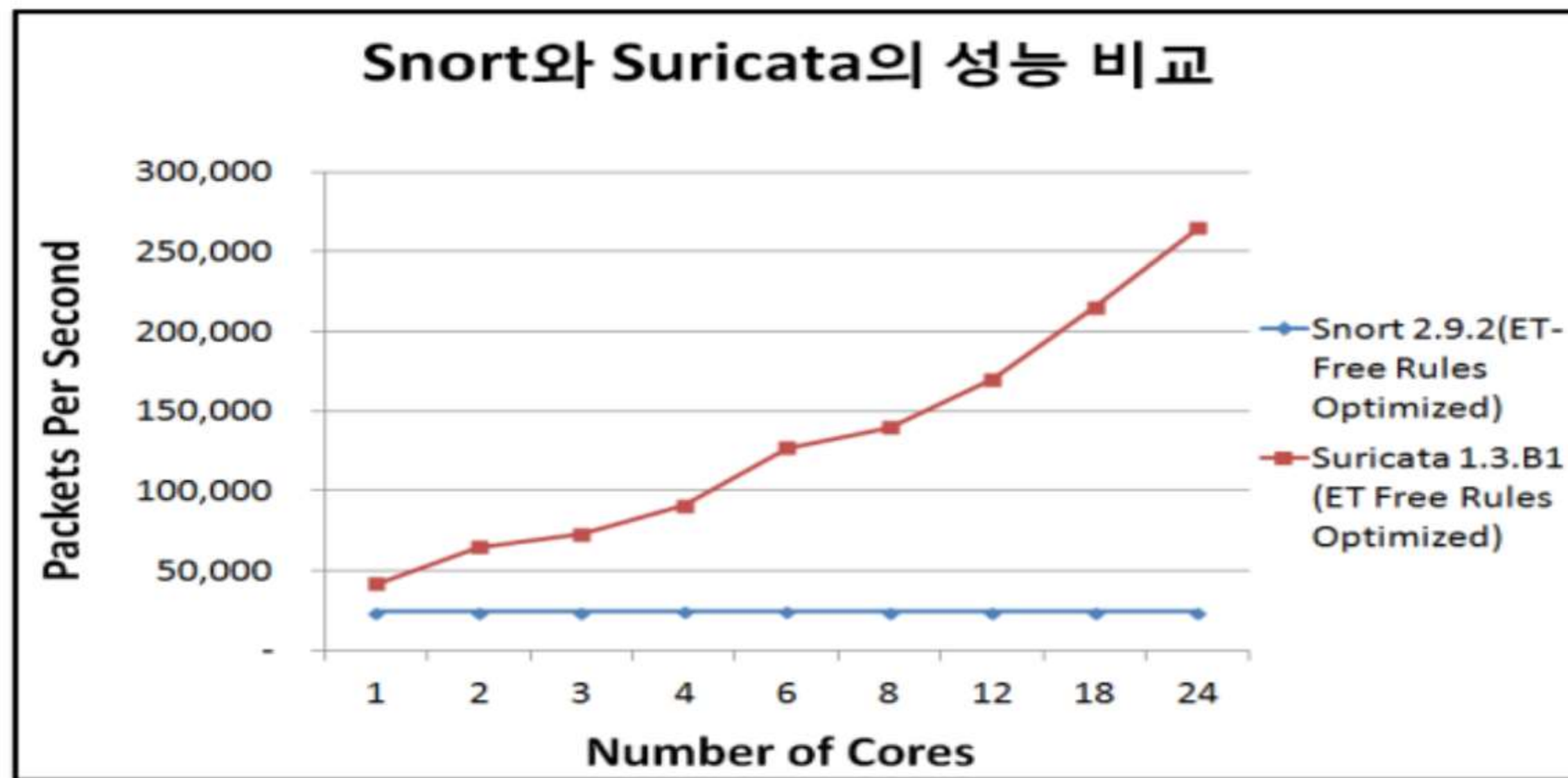


ORACLE



SURICATA / SNORT

위의 기술들 설명



출처: <https://koreascience.kr/article/JAKO201435640763049.pdf>



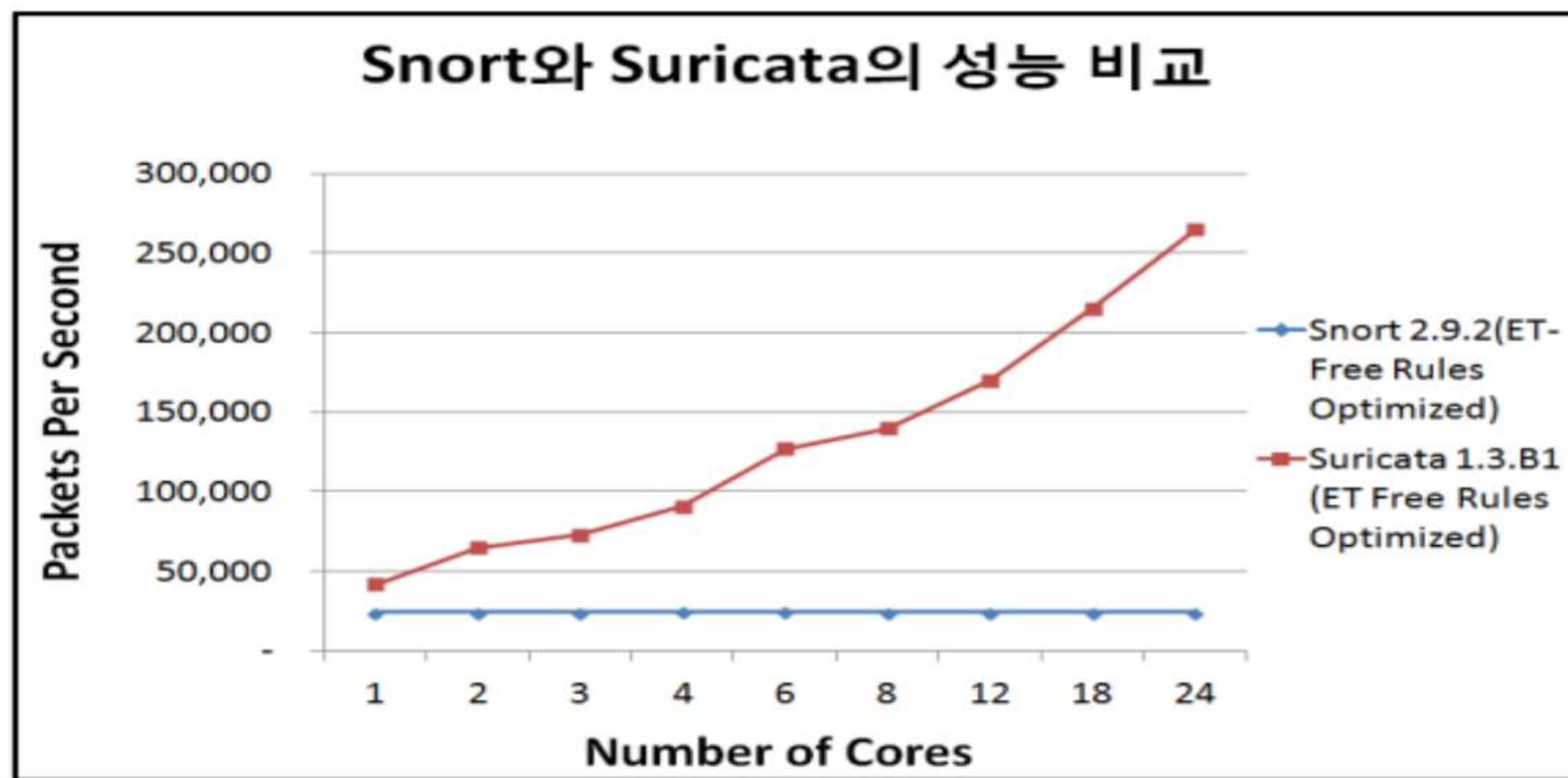
<특징>

-snort의 발전된 형태로,
멀티프로세싱에 적합한 구조로서
멀티 프로세싱에 효과적

따라서, IDS에는 **미니서버에 적합한**
suricata를 선택

SURICATA / SNORT

위의 기술들 설명



출처: <https://koreascience.kr/article/JAKO201435640763049.pdf>



Switch에서는 리소스 자체가 최소화되어있어, 오히려 **멀티스레딩방식이 비효율적**

따라서 CPU, Memory, Flash Memory 등 하드웨어 사양이 낮지만 멀티 네트워크 인터페이스를 제공하는 공유기에는 Minimal Single Processing 구조의 snort 적용

DB 설계

회원가입 / 로그인 / 로그 저장 / 룰 DB / 시퀀스

```
CREATE TABLE create_User(  
  ID VARCHAR2(300) PRIMARY KEY,  
  PASSWORD VARCHAR2(300) NOT NULL,  
  NAME VARCHAR2(30),  
  PHONENUM VARCHAR2(50),  
  AUTHORITY VARCHAR2(30) DEFAULT '-'  
);
```

```
create table maked_rule(  
  sid      VARCHAR2(20) primary key,  
  msg      VARCHAR2(100),  
  rule     VARCHAR2(500)  
);
```

```
CREATE SEQUENCE sid_seq  
  INCREMENT BY 1  
  START WITH 1000001  
  MINVALUE 1000000  
  MAXVALUE 1001000  
  NOCYCLE  
  NOCACHE;
```

```
CREATE TABLE Threats(  
  time      VARCHAR2(50),  
  message   VARCHAR2(200),  
  priority  VARCHAR2(50),  
  src_ip    VARCHAR2(20),  
  src_port  VARCHAR2(20),  
  dst_ip    VARCHAR2(20),  
  dst_port  VARCHAR2(20)  
);
```

```
CREATE TABLE DropThreats(  
  time      VARCHAR2(50),  
  isdrop    VARCHAR2(10),  
  message   VARCHAR2(200),  
  priority  VARCHAR2(50),  
  src_ip    VARCHAR2(20),  
  src_port  VARCHAR2(20),  
  dst_ip    VARCHAR2(20),  
  dst_port  VARCHAR2(20)  
);
```

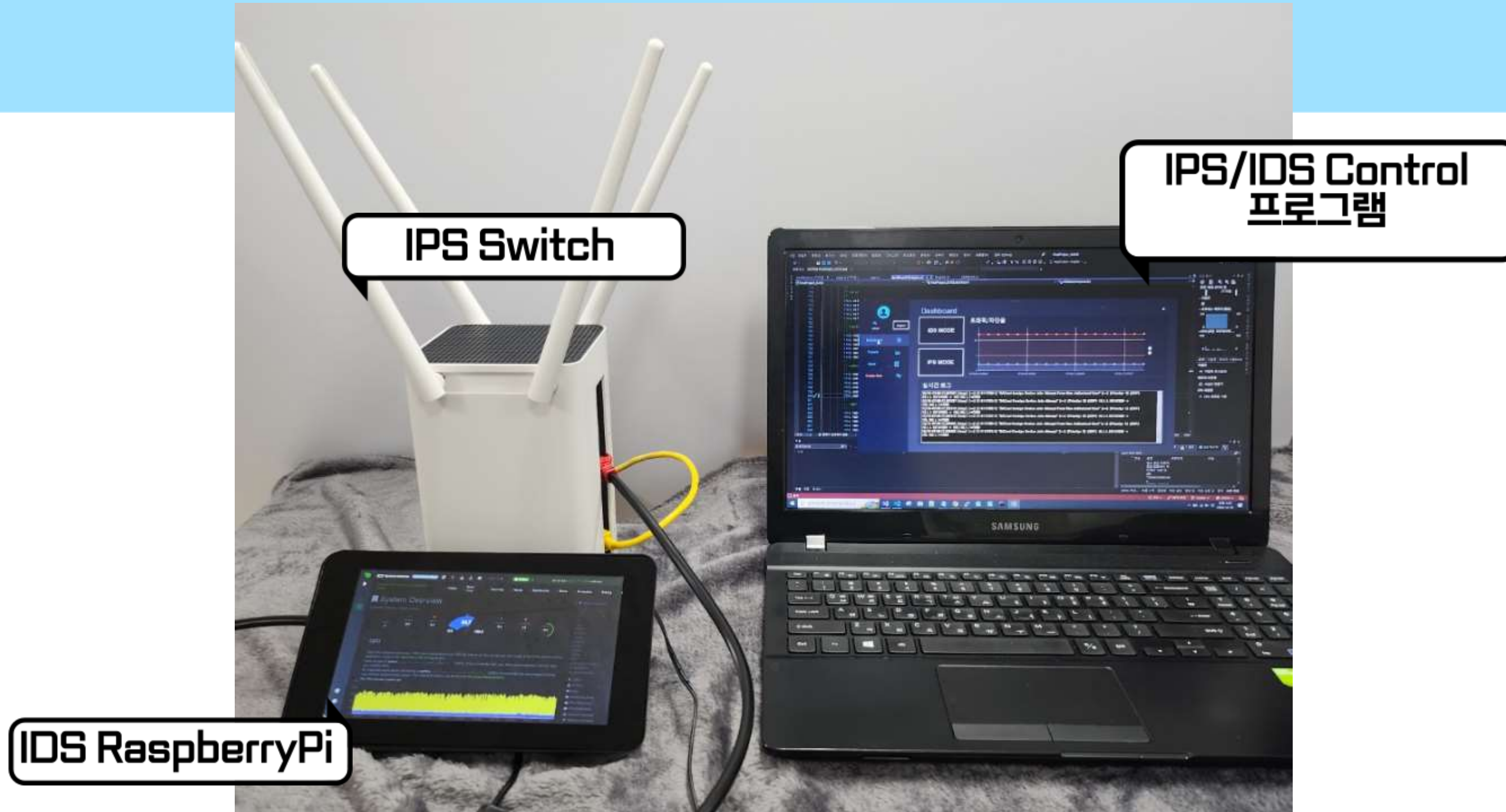

03

프로젝트 구현

- 하드웨어 구현 환경
- IPS / IDS Control 프로그램 구현
- Packet Generator 프로그램 구현
- 시연 영상

R.I.P Hardware

Implementation Environment



IDS / IPS Control 프로그램 구현

회원가입 및 로그인

IPS CONTROL CREATE USER

아이디

비밀번호

이름

전화번호

생성

나가기

IPS CONTROL CREATE USER

아이디

비밀번호

전화번호

생성

나가기

빈칸에 공백이 존재합니다. 모든 항목을 작성해 주십시오.

확인

IPS CONTROL CREATE USER

아이디

비밀번호

이름

전화번호

생성

나가기

아이디가 생성되었습니다.

확인

IPS CONTROL LOGIN

아이디

비밀번호

Insert ID/PASSWORD

회원가입

확인

나가기

IPS CONTROL LOGIN

아이디

비밀번호

아이디/비밀번호가 틀립니다.


회원가입

확인

나가기


admin권한으로 로그인 성공. 메인화면으로 갑니다.

확인



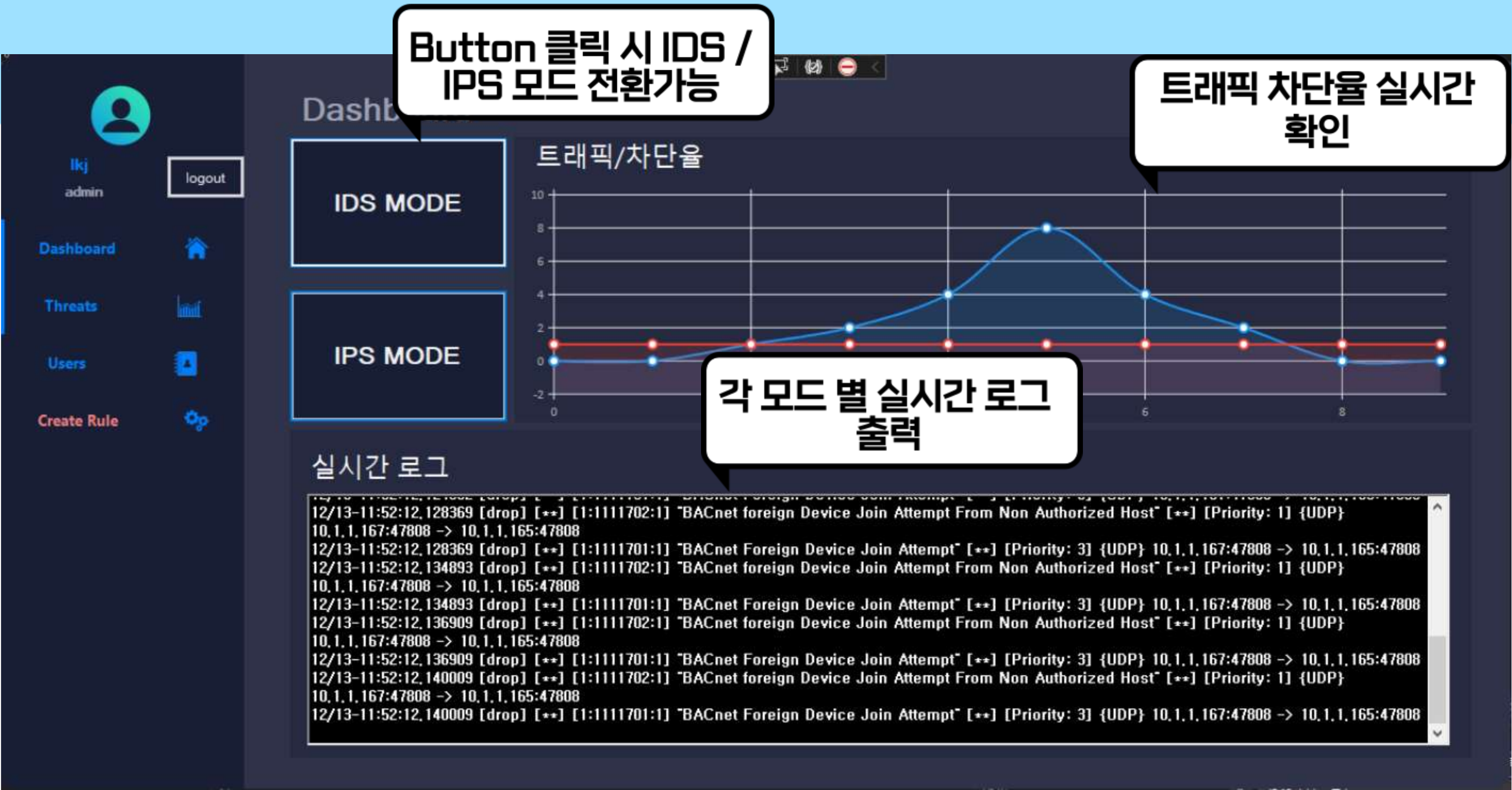
lkj
admin

logout

Dashboard

IDS / IPS Control 프로그램 구현

Dashboard Form



IDS / IPS Control 프로그램 구현

Threats Form


lkj
admin

logout

Dashboard

Threats

Users

Create Rule

Threats

총 이벤트 발생 건수와
최다 공격 IP, 횟수

발생건수 : 10 최다 공격 IP : 10.1.1.167 최다 공격 횟수 : 10

IDS 로그 새로고침

IPS 로그 새로고침

TIME	ISDROP	MESSAGE	PRIORITY	SRC_IP	SRC_PORT	DST_IP	DST_PORT
12/13-11:52:12.1...	drop	"BACnet Foreign...	3	10.1.1.167	47808	10.1.1.165	47808
12/13-11:52:12.1...	drop	"BACnet foreign...	1	10.1.1.167	47808	10.1.1.165	47808
12/13-11:52:12.1...	drop	"BACnet foreign...	1	10.1.1.167	47808	10.1.1.165	47808
12/13-11:52:12.1...	drop	"BACnet Foreign...	3	10.1.1.167	47808	10.1.1.165	47808
12/13-11:52:12.1...	drop	"BACnet Foreign...	3	10.1.1.167	47808	10.1.1.165	47808
12/13-11:52:12.1...	drop	"BACnet foreign...	1	10.1.1.167	47808	10.1.1.165	47808
12/13-11:52:12.1...	drop	"BACnet foreign...	1	10.1.1.167	47808	10.1.1.165	47808
12/13-11:52:12.1...	drop	"BACnet Foreign...	3	10.1.1.167	47808	10.1.1.165	47808
12/13-11:52:12.1...	drop	"BACnet foreign...	1	10.1.1.167	47808	10.1.1.165	47808
12/13-11:52:12.1...	drop	"BACnet Foreign...	3	10.1.1.167	47808	10.1.1.165	47808

Button 클릭 시 로그
새로 고침

모드별 로그 출력

IDS / IPS Control 프로그램 구현

User Form

Admin 권한만
사용 가능

lkj
admin

logout

Dashboard

Threats

Users

Create Rule

Users

회원가입 신청목록

ID	PASSWORD	NAME	PHONENUM	AUTHORITY	ACCEPT
test	1234	홍길동	010-1111-1111	user	X
test1	12345	홍길순	010-1111-1112	user	O
aa	123	llkk	111-1111-1111	user	X
qwerty	1234	qwerty	010-1111-2222	admin	O
test2	123456	Lion	111-1111-2222	user	X

유저 목록

ID	PASSWORD	AUTHORITY
lkj	1234	admin
qwerty	1234	admin
test1	12345	user

회원 가입 신청 목록 확인

권한 설정

qwerty

관리자 권한 부여

사용자 권한 부여

권한 회수

가입 승인

회원 삭제

취약점 분석 대상 프로토콜

프로토콜 정의 및 취약점 분석

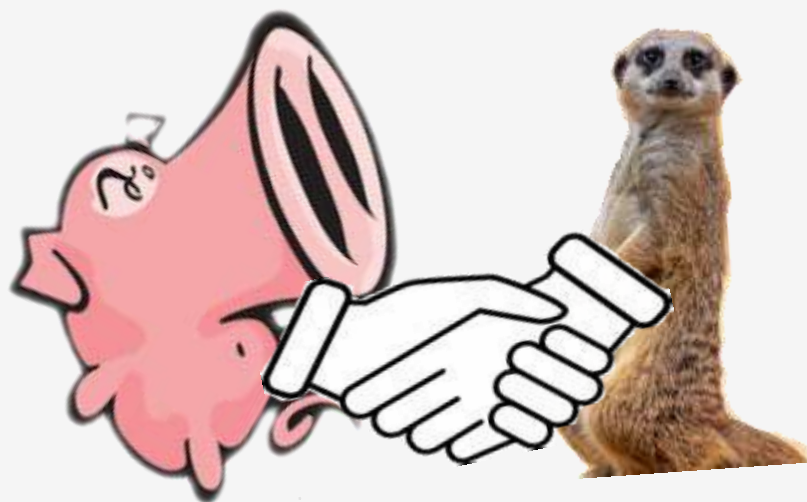
우리는 총 8종의 산업용 프로토콜을 대상으로 보안취약성을 분석하여, 58개의 탐지 룰을 생성했다.

대상 프로토콜	정의	취약점 분석
BACnet	- 빌딩 자동제어 및 제어 네트워크의 표준 프로토콜 (A Data Communication Protocol for Building Automation and Control Networks) - 미국 및 유럽의 표준이며 30여개국 이상에서 표준으로 채택	• 총 9종 - 외부 장치 가입 시도 / 속성 읽기 시도 / Broadcast-Distribution 테이블 읽기 시도 / Read-Broadcast-Distribution-Table NAK, 디바이스에서 BDT 읽기에 대한 액세스가 거부
DNP3	DNP3(IEEE Std 1815)는 컴퓨터 간의 통신 규칙을 정의하는 종합적인 프로토콜 표준	• 총 22종 - 승인되지 않은 클라이언트의 브로드캐스트 요청 / 클라이언트에서 콜드 재시작 / 요청하지 않은 응답 비활성화 / 애플리케이션 중지 / PLC에 대한 무단 읽기 요청 / 요청하지 않은 많은 양의 응답 / 원 부팅
Enip	이더넷/IP(EtherNet/IP, IP = Industrial Protocol)는 산업 네트워크 프로토콜. 미국 주도적인 산업 프로토콜 가운데 하나이며 공장, 하이브리드 및 공정을 포함한 다양한 산업 부문에 널리 사용	• 총 2종 Redpoint Nmap NSE를 통해 전송된 Request Identity 명령
Fox	Niagara Fox Protocol은 Tridium의 Niagara 소프트웨어 시스템 간에 사용되는 빌딩 자동화 프로토콜	• 총 2종 - TCP/1911의 Redpoint Nmap NSE를 통해 발생한 명령
Modbus	- 시리얼 통신 프로토콜. 제조공장이나 놀이공원의 기계들을 자동화하고 제어하는 목적으로 사용되는 프로그래머블 로직 컨트롤러(Programmable Logic Controller, PLC)들과의 통신에 사용할 목적. - 프로토콜이 단순하지만, 장비 제어와 모니터링에 필요한 기능들을 수행할 수 있기에 사실상의 표준 프로토콜로서, 현재까지 산업용 전자 장치들을 서로 연결하는 목적으로 널리 사용	• 총 14종 -카운터 및 진단 레지스터 지우기 명령 / 강제 수신 전용 모드 / 장치 식별 읽기 / 서버 정보 보고 / 통신 옵션 재시작
Modicon	- Modbus 프로토콜을 정의한 회사(Modicon)의 전용 컨트롤러 제어 프로토콜	• 총 3종 ladder Logic download / upload
Omron	- PLC 및 기타 장비와의 통신 프로토콜 - ASCII 기반 프로토콜이며, RS232 또는 RS422/RS485를 통해 사용 - 산업 현장에서 PLC, 온도 컨트롤러, 패널 미터 등을 제어	• 총 4종 -OMRON FIN TCP 읽기 컨트롤러 시도 / OMRON FIN UDP 읽기 컨트롤러 시도
S7	S7comm(S7 Communication)은 Siemens S7-300/400 제품군의 프로그래밍 가능 논리 컨트롤러 (PLC) 간에 실행되는 Siemens 독점 프로토콜	• 총 2종 - TCP/102에서 s7-enumerate Redpoint Nmap NSE를 통한 명령

IDS / IPS Control 프로그램 구현

Rule 생성

snort Rule과 suricata Rule은 동일하게 호환되며, 상용 IPS, IDS는 거의 모든 모델에서 snort Rule을 지원하고 있는 장점이 있다. 우리는 복잡한 Rule 생성에 대해 일반 관리자가 GUI를 통해 쉽게 Rule을 생성할 수 있도록 룰 자동 생성 기능도 구현했다



IDS / IPS Control 프로그램 구현

Create Rule Form - 자동 룰 생성

lkj
admin

logout

Dashboard

Threats

Users

Create Rule

Create Rule

<스마트팩토리 유해 모델>

BACnet Foreign Device Join Attempt

Header

Action

Protocol

Src IP

Src Port

Direction

Dst IP

Dst Port

Option

option	value
> Meta Data	
> payload	
> Non-Payload	

Server : 192.168.0.13
Type : RIP-IPS
Status : Running

고유번호 생성

서버 룰 추가

서버 적용

alert udp any any -> any 47808 (content: W"105|W"; depth: 1; offset: 1; msg:W"BACnet Foreign Device Join AttemptW"; priority: 3; rev: 1; sid: 1000004;)

Admin 권한만
사용 가능

스마트팩토리 보안
유해 모델

작동 환경

설정한 룰 Preview

IDS / IPS Control 프로그램 구현


Create Rule Form - 자동 룰 생성

Admin 권한만
사용 가능

적용 된 룰 확인

각 노드에 값 입력시 자
동으로 룰 생성

룰 추가 및 서버 적용,
자동 sid 부여



lkj
admin

logout

Dashboard

Threats

Users

Create Rule

Create Rules

<스마트팩토리 유해 모델>

Header

Action

alert

Protocol

udp

Src IP

any

Src Port

47808

Direction

->

Dst IP

any

Dst Port

any

Option

option	value
Meta Data	
msg	BACnet Register-Forel...
priority	3
rev	1
payload	
content	[00 30]
nocase	
rawbytes	
depth	2
offset	4
distance	
within	
isdataat	

Server :

Type :

Status :

고유번호 생성

서버 룰 추가

서버 적용

alert udp any 47808 -> any any (content: W"100 30|W"; depth: 2; offset: 4;msg:W"BACnet Register-Foreign-Device NAKW"; priority: 3; rev: 1; sid: 1000005;)

확인

```
root@kyowon-desktop: /home/kyowon
alert udp any any -> any 47808 (content: "|02|"; offset: 1; depth: 1; msg: "BAC
net Read-Broadcast-Distribution-Table Attempt";sid:1111708;priority:3;rev:1;)
... is a Read-Broadcast-Distribution-Table NAK
... 08 -> any any (content: "|00 20|"; offset: 4; depth: 2; msg:
lcast-Distribution-Table NAK, Device was denied access to read
... 1111709;priority:3;rev:1;)
alert udp any any -> any 47808 ( content: "|05|"; depth: 1; offset: 1;msg:"BAC
net Foreign Device Join Attempt"; priority: 3; rev: 1; sid: 1000001; )
alert udp any any -> any 47808 ( content: "|05|"; depth: 1; offset: 1;msg:"BAC
net Foreign Device Join Attempt"; priority: 3; rev: 1; sid: 1000003; )
alert udp any 47808 -> any any ( content: "|00 30|"; depth: 2; offset: 4;msg:"
BACnet Register-Foreign-Device NAK"; priority: 3; rev: 1; sid: 1000005; )
```



```
08:57:19.969468 IP6 fe80::577:98a6:e7db:c091:60579 > ff02::1:3.5355: UDP, length 22
08:57:19.969467 IP6 fe80::577:98a6:e7db:c091:62607 > ff02::1:3.5355: UDP, length 22
08:57:19.969908 IP 192.168.1.236.62607 > 224.0.0.252.5355: UDP, length 22
08:57:19.969905 IP 192.168.1.236.60579 > 224.0.0.252.5355: UDP, length 22
08:57:20.313673 IP 192.168.1.236.137 > 192.168.1.255.137: UDP, length 50
08:57:20.548034 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
08:57:20.548740 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
08:57:20.560631 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
08:57:20.561303 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
08:57:20.562287 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 AAAA (QM)? wpad.local. (28)
08:57:20.562875 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 AAAA (QM)? wpad.local. (28)
08:57:20.563659 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 AAAA (QM)? wpad.local. (28)
08:57:20.564295 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 AAAA (QM)? wpad.local. (28)
08:57:21.074792 IP 192.168.1.236.137 > 192.168.1.255.137: UDP, length 50
```


Packet Generator 프로그램

공격 수행

공격 수행 가능

스마트팩토리 프로토콜 패킷 제너레이터

산업용 프로토콜 취약성 모음

☒ bacnet_Foreign Device Join Attempt.pcap

☐ bacnet_Read Property Attempt.pcap

☐ bacnet_Read-Broadcast-Distribution-Table Attempt.pcap

☐ bacnet_Read-Broadcast-Distribution-Table NAK.pcap

☐ bacnet_Register-Foreign-Device NAK.pcap

☐ dnp3_Broadcast Request from Authorized Client.pcap

☐ dnp3_Cold Restart From Authorized Client.pcap

☐ dnp3_Disable Unsolicited Responses.pcap

☐ dnp3_Stop Application.pcap

☐ dnp3_Unauthorized Read Request to a PLC.pcap

☐ dnp3_Unsolicited Response Storm.pcap

* BACnet Protocol

1. 정의

BACnet은 빌딩 자동제어 및 제어 네트워크의 표준 프로토콜로서 말 그대로 "A Data Communication Protocol for Building Automation and Control Networks"의 약자이다.

BACnet은 미국의 냉동 공조 학회인 ASHRAE(American Society of Heating, Refrigerating and Air-Conditioning Engineers)의 주도로 만들어졌으며, 미국 및 유럽의 표준이며 30여개국 이상에서 표준으로 채택되었다.

2. 프로토콜 취약성

외부 장비의 인증없는 등록 요청 취약성

3. 차단 정책 추천

alert udp !\$BACNET_CLIENT any -> any 47808 (content: "[05]"; offset:1; depth:1; msg:"BACnet foreign Device Join Attempt From Non Authorized Host"; sid:1111702;priority:1;rev:1;)

공격 완료!

19번째 공격 수행 중...

공격 완료!

20번째 공격 수행 중...

공격 완료!

-- 패킷 대기열 해제

설정 및 수행

공격 대상 IP : Port : 공격횟수 : 20

모니터링 서버 : 192.168.1.1 ID : root Password : ***** Interface : br-lan

공격 수행

로거 연결

공격 로그

Original Eth packet: [EthernetPacket: SourceHardwareAddress=3c:a9:f4:21:22:fb, DestinationHardwareAddress=00:19:07:24:3c:ca, Type=IPv4][IPv4Packet: SourceAddress=10.1.1.167, DestinationAddress=10.1.1.165, HeaderLength=5, Protocol=Udp, TimeToLive=128][UDPPacket: SourcePort=47808, DestinationPort=47808]

Original IP packet: [IPv4Packet: SourceAddress=10.1.1.167, DestinationAddress=10.1.1.165, HeaderLength=5, Protocol=Udp, TimeToLive=128][UDPPacket: SourcePort=47808, DestinationPort=47808]

Original UDP packet: [UDPPacket: SourcePort=47808, DestinationPort=47808]

Manipulated Eth packet: [EthernetPacket: SourceHardwareAddress=3c:a9:f4:21:22:fb, DestinationHardwareAddress=00:19:07:24:3c:ca, Type=IPv4][IPv4Packet: SourceAddress=10.1.1.167, DestinationAddress=10.1.1.165, HeaderLength=5, Protocol=Udp, TimeToLive=128][UDPPacket: SourcePort=47808, DestinationPort=47808]

서버 로그

08:57:19.969468 IP6 fe80::577:98a6:e7db:c091:60579 > ff02::1:3.5355: UDP, length 22

08:57:19.969467 IP6 fe80::577:98a6:e7db:c091:62607 > ff02::1:3.5355: UDP, length 22

08:57:19.969908 IP 192.168.1.236.62607 > 224.0.0.252.5355: UDP, length 22

08:57:19.969905 IP 192.168.1.236.60579 > 224.0.0.252.5355: UDP, length 22

08:57:20.313673 IP 192.168.1.236.137 > 192.168.1.255.137: UDP, length 50

08:57:20.548034 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)

08:57:20.548740 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)

08:57:20.560631 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)

08:57:20.561303 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)

08:57:20.562287 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 AAAA (QM)? wpad.local. (28)

08:57:20.562875 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 AAAA (QM)? wpad.local. (28)

08:57:20.563659 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 AAAA (QM)? wpad.local. (28)

08:57:20.564295 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 AAAA (QM)? wpad.local. (28)

08:57:21.074792 IP 192.168.1.236.137 > 192.168.1.255.137: UDP, length 50

Packet Generator 프로그램

로거 연결

로거 연결

스마트팩토리 프로토콜 패킷 제너레이터

산업용 프로토콜 취약성 모음

☒ bacnet_Foreign Device Join Attempt.pcap

☐ bacnet_Read Property Attempt.pcap

☐ bacnet_Read-Broadcast-Distribution-Table Attempt.pcap

☐ bacnet_Read-Broadcast-Distribution-Table NAK.pcap

☐ bacnet_Register-Foreign-Device NAK.pcap

☐ dnp3_Broadcast Request from Authorized Client.pcap

☐ dnp3_Cold Restart From Authorized Client.pcap

☐ dnp3_Disable Unsolicited Responses.pcap

☐ dnp3_Stop Application.pcap

☐ dnp3_Unauthorized Read Request to a PLC.pcap

☐ dnp3_Unsolicited Response Storm.pcap

* BACnet Protocol

1. 정의

BACnet은 빌딩 자동제어 및 제어 네트워크의 표준 프로토콜로서 말 그대로 "A Data Communication Protocol for Building Automation and Control Networks"의 약자이다.

BACnet은 미국의 냉동 공조 학회인 ASHRAE(American Society of Heating, Refrigerating and Air-Conditioning Engineers)의 주도로 만들어졌으며, 미국 및 유럽의 표준이며 30여개국 이상에서 표준으로 채택되었다.

2. 프로토콜 취약성

외부 장비의 인증없는 등록 요청 취약성

3. 차단 정책 추천

alert udp !\$BACNET_CLIENT any -> any 47808 (content: "[05]"; offset:1; depth:1; msg:"BACnet foreign Device Join Attempt From Non Authorized Host"; sid:1111702;priority:1;rev:1;)

공격 완료!

19번째 공격 수행 중...

공격 완료!

20번째 공격 수행 중...

공격 완료!

-- 패킷 대기열 해제

설정 및 수행

공격 대상 IP : Port : 공격횟수 : 20 공격 수행

모니터링 서버 : 192.168.1.1 ID : root Password : ***** Interface : br-lan 로거 연결

공격 로그

Original Eth packet: [EthernetPacket: SourceHardwareAddress=3c:a9:f4:21:22:fb, DestinationHardwareAddress=00:19:07:24:3c:ca, Type=IPv4][IPv4Packet: SourceAddress=10.1.1.167, DestinationAddress=10.1.1.165, HeaderLength=5, Protocol=Udp, TimeToLive=128][UDPPacket: SourcePort=47808, DestinationPort=47808]

Original IP packet: [IPv4Packet: SourceAddress=10.1.1.167, DestinationAddress=10.1.1.165, HeaderLength=5, Protocol=Udp, TimeToLive=128][UDPPacket: SourcePort=47808, DestinationPort=47808]

Original UDP packet: [UDPPacket: SourcePort=47808, DestinationPort=47808]

Manipulated Eth packet: [EthernetPacket: SourceHardwareAddress=3c:a9:f4:21:22:fb, DestinationHardwareAddress=00:19:07:24:3c:ca, Type=IPv4][IPv4Packet: SourceAddress=10.1.1.167, DestinationAddress=10.1.1.165, HeaderLength=5, Protocol=Udp, TimeToLive=128][UDPPacket: SourcePort=47808, DestinationPort=47808]

서버 로그

08:57:19.969468 IP6 fe80::577:98a6:e7db:c091:60579 > ff02::1:3.5355: UDP, length 22

08:57:19.969467 IP6 fe80::577:98a6:e7db:c091:62607 > ff02::1:3.5355: UDP, length 22

08:57:19.969908 IP 192.168.1.236.62607 > 224.0.0.252.5355: UDP, length 22

08:57:19.969905 IP 192.168.1.236.60579 > 224.0.0.252.5355: UDP, length 22

08:57:20.313673 IP 192.168.1.236.137 > 192.168.1.255.137: UDP, length 50

08:57:20.548034 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)

08:57:20.548740 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)

08:57:20.560631 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)

08:57:20.561303 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)

08:57:20.562287 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 AAAA (QM)? wpad.local. (28)

08:57:20.562875 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 AAAA (QM)? wpad.local. (28)

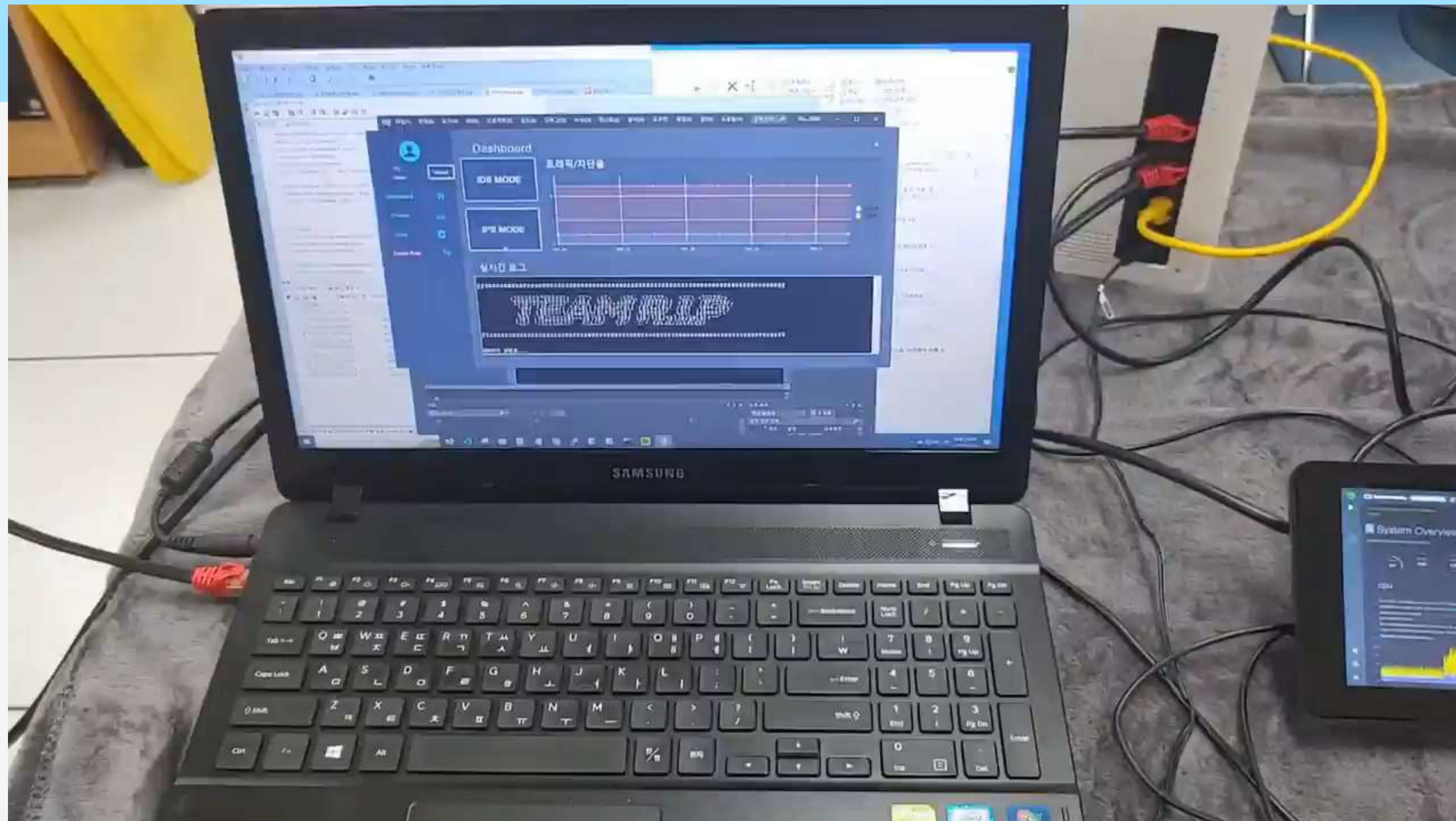
08:57:20.563659 IP 192.168.1.236.5353 > 224.0.0.251.5353: 0 AAAA (QM)? wpad.local. (28)

08:57:20.564295 IP6 fe80::577:98a6:e7db:c091:5353 > ff02::fb.5353: 0 AAAA (QM)? wpad.local. (28)

08:57:21.074792 IP 192.168.1.236.137 > 192.168.1.255.137: UDP, length 50

Tcpdump를 log로 확인

시연 영상





03

기대효과

기대 효과

전문가가 따로 필요 없이 rules 생성가능

저렴한 비용으로 보안구축

신규 취약성에 대한 빠른 Rule
업데이트 가능

기존 방화벽에서 탐지 못하는
스마트팩토리 취약 패킷 탐지
가능

감사합니다.