CHAPTER 08

IDPS (침입탐지/방지시스템)

이현호 hyeonholee@korea.com

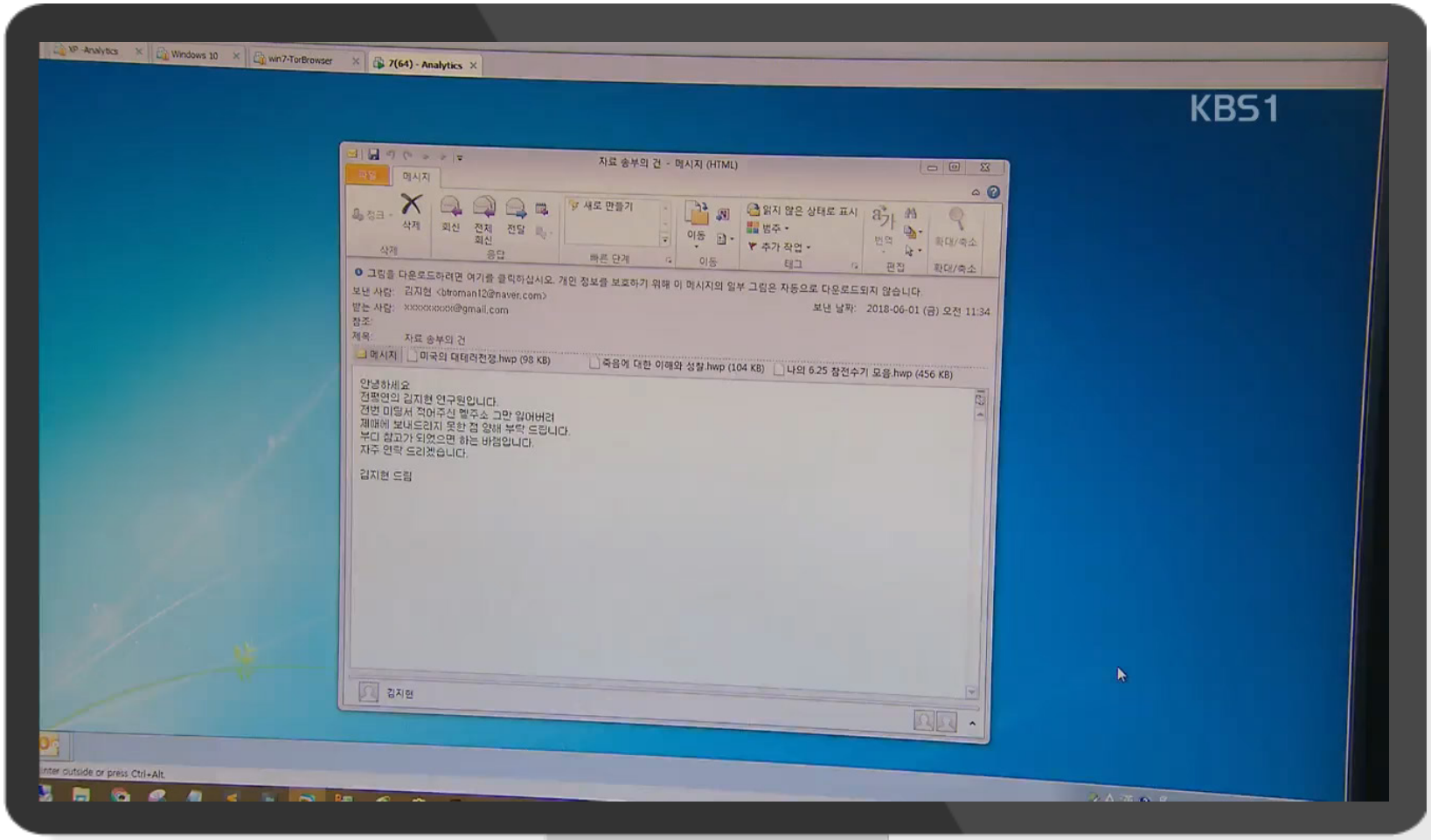
목차

I

IDPS의 이해

I IDPS의 이해

1 방화벽의 한계



출처 '빗썸' 해킹 징후 있었는데…"한국은 먹잇감", KBS(2018.06.21), https://www.youtube.com/watch?v=3MQzCDFQ-7Q

IDPS의 이해

1 방화벽의 한계

빗썸 고객들의 해킹메일 피해 사례

해킹 메일
무작위 전송

해킹메일

- 평범한 업무 메일로 위장하여 의심없이 열어볼 수 있게 유도
- 직원을 직접 겨냥한 이력서나 정부 문서를 사칭한 문서 파일을 가장한 악성코드 첨부

출처 '빗썸' 해킹 징후 있었는데…"한국은 먹잇감", KBS(2018.06.21), https://www.youtube.com/watch?v=3MQzCDFQ-7Q

IDPS의 이해

1 방화벽의 한계

빗썸 고객들의 해킹메일 피해 사례

아이디와 비밀번호를 절취하여
공격자에게 전송하는
명령어를 포함한 악성코드

첨부파일 오픈 시
악성코드에 감염

출처 '빗썸' 해킹 징후 있었는데…"한국은 먹잇감", KBS(2018.06.21), https://www.youtube.com/watch?v=3MQzCDFQ-7Q

I IDPS의 이해

1 방화벽의 한계

빗썸 고객들의 해킹메일 피해 사례

악성코드 일정 기간 잠복

↓

특정 시점에 ID/PW 절취

↓

사용자의 가상화폐까지 절취

악성코드를 예방하거나 대응하기에 방화벽 만으로 충분한 것일까?

출처 '빗썸' 해킹 징후 있었는데…"한국은 먹잇감", KBS(2018.06.21), https://www.youtube.com/watch?v=3MQzCDFQ-7Q

I IDPS의 이해

1 방화벽의 한계

- 방화벽(침입차단시스템)은 **전통적인 정보보호시스템**으로,
  무분별한 침해 시도로부터 일정 부분 대응할 수 있게끔 **1차 방어선을 구축**해주지만
  내용을 들여다볼 수 없다는 한계
  - 공격자의 행위가 발생되는 영역까지 확인하기 위해서는 본문 데이터까지 확인 필요
  - 공개 웹 서비스를 제공하기 위해 방화벽을 활용하여 HTTP(80), HTTPS(443) 통신을 누구에게나 허용하는 것은 IP, 포트(서비스) 만으로 누가 정상 사용자인지 공격자인지 구분할 수 없기 때문

2 IDPS

- **침입탐지시스템 (Intrusion Detection System, IDS)**

IDS

네트워크 간 전송되는 패킷을 수집하고 내용을 분석하여
침해 시도를 탐지하는 정보보호시스템

- 국가 · 공공에서 사용하는 공식 용어는 침입탐지시스템
- 실시간으로 탐지하지만 **사후분석 대응** 방식으로 활용
- **방화벽이 기 구성된 네트워크 경계 보호를 강화**하기 위한 목적으로 사용

2 IDPS

- **침입방지시스템 (Intrusion Prevention System, IPS)**

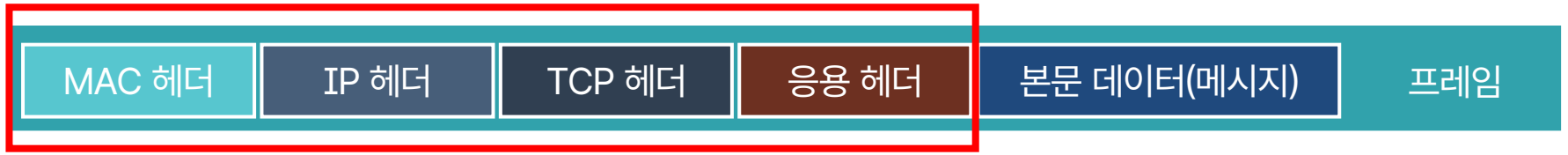
IPS

네트워크 간 전송되는 패킷을 수집하고 내용을 분석하여
침해 시도를 탐지하고 차단하는 정보보호시스템

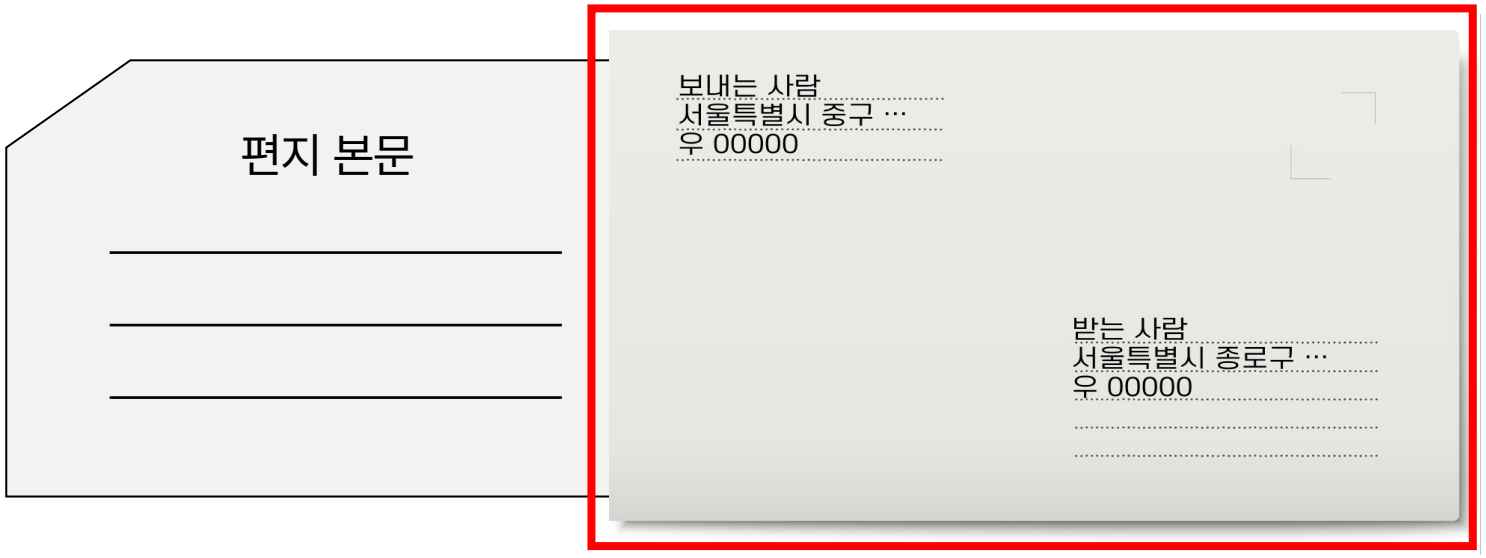
- 국가 · 공공에서 사용하는 공식 용어는 **침입방지시스템**
- 실시간으로 탐지할 뿐 아니라 **차단도 가능**하여, **실시간 대응 방식**으로 활용 가능
- **방화벽이 기 구성된 네트워크 경계 보호를 강화**하기 위한 목적으로 사용되며,
  근래에는 **IDS보다 IPS를 사용**하는 경향

2 IDPS

- 침입탐지시스템과 침입방지시스템을 묶어서 IDPS 또는 IDS/IPS라고 지칭
- IDPS는 방화벽이 확인하지 않는 응용 계층의 본문 데이터(메시지)까지 확인

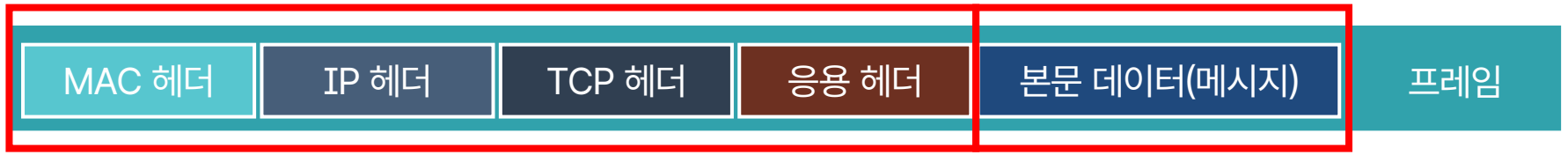


방화벽이 확인하는 영역

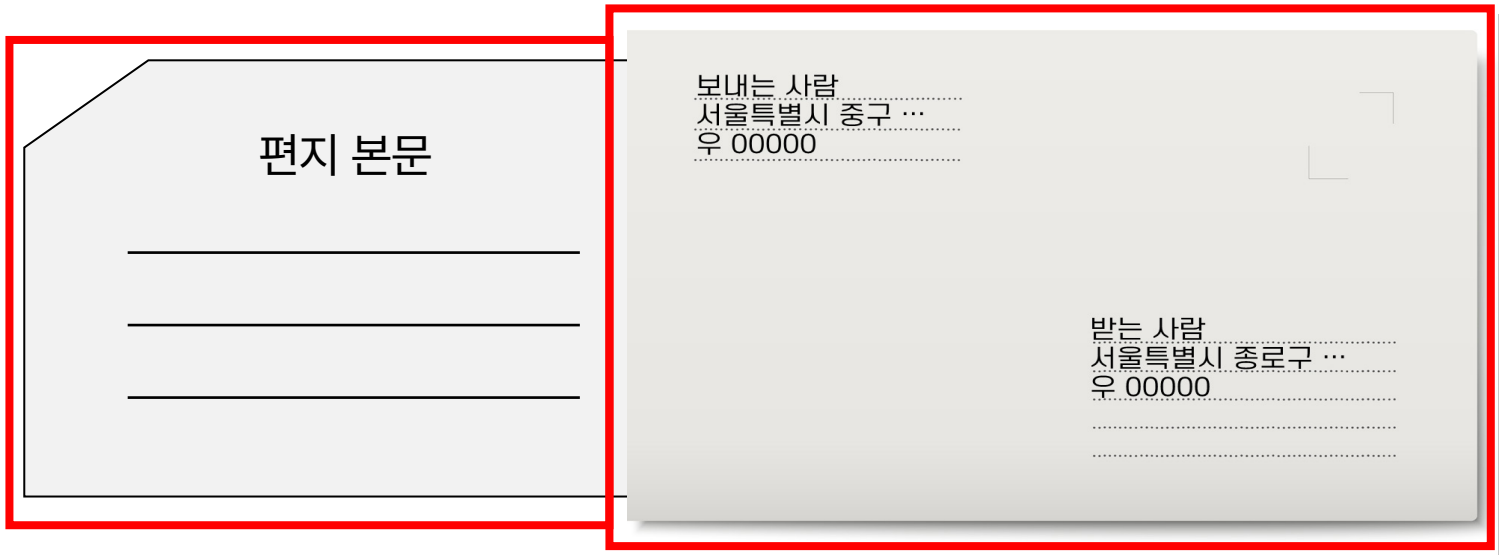


2 IDPS

- 침입탐지시스템과 침입방지시스템을 묶어서 IDPS 또는 IDS/IPS라고 지칭
- IDPS는 방화벽이 확인하지 않는 응용 계층의 본문 데이터(메시지)까지 확인



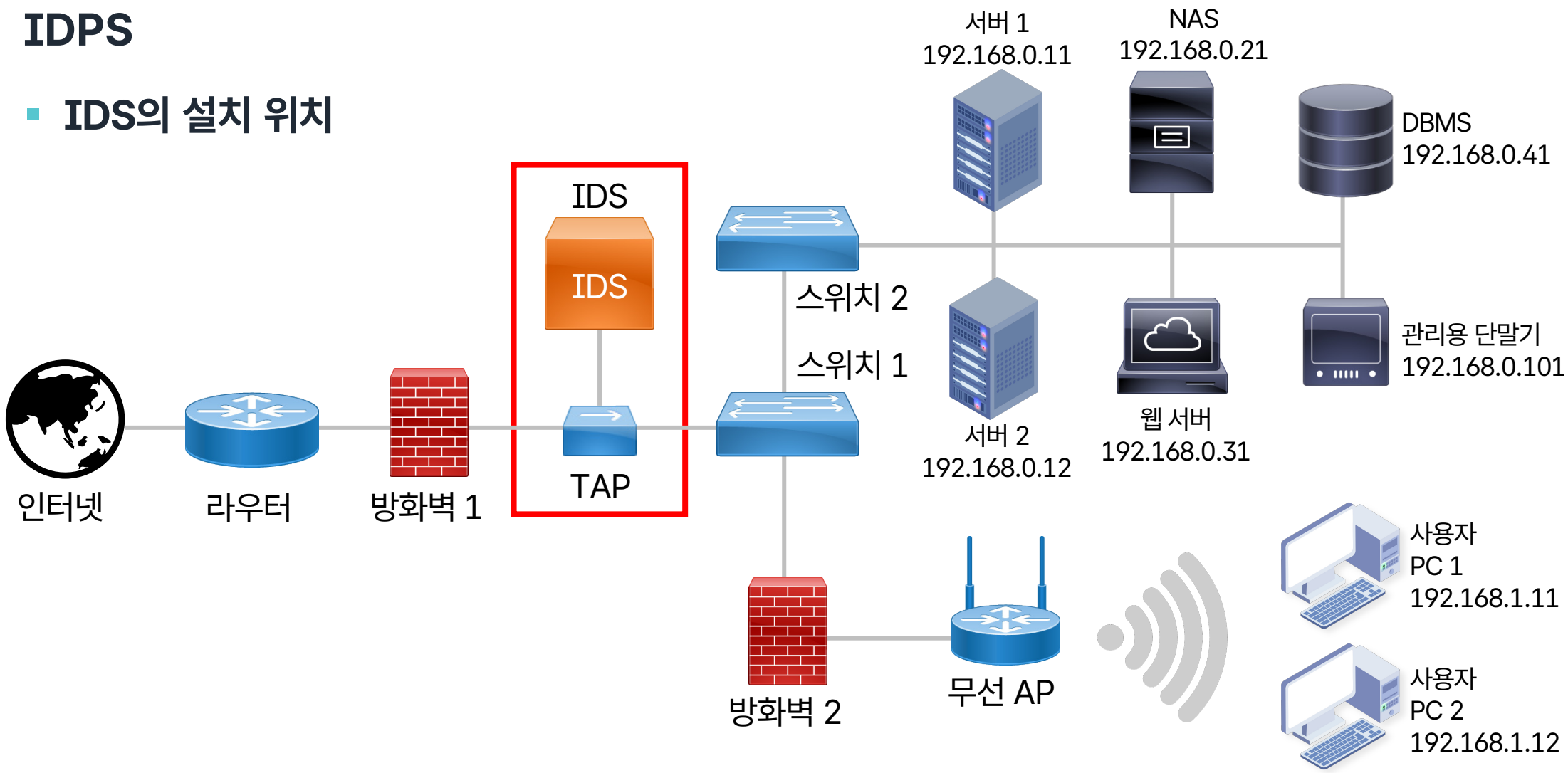
IDS/IPS가 확인하는 영역



IDPS의 이해

2 IDPS

- **IDS의 설치 위치**



2 IDPS

▪ IDS의 설치 위치

미러링(Mirroring) 모드

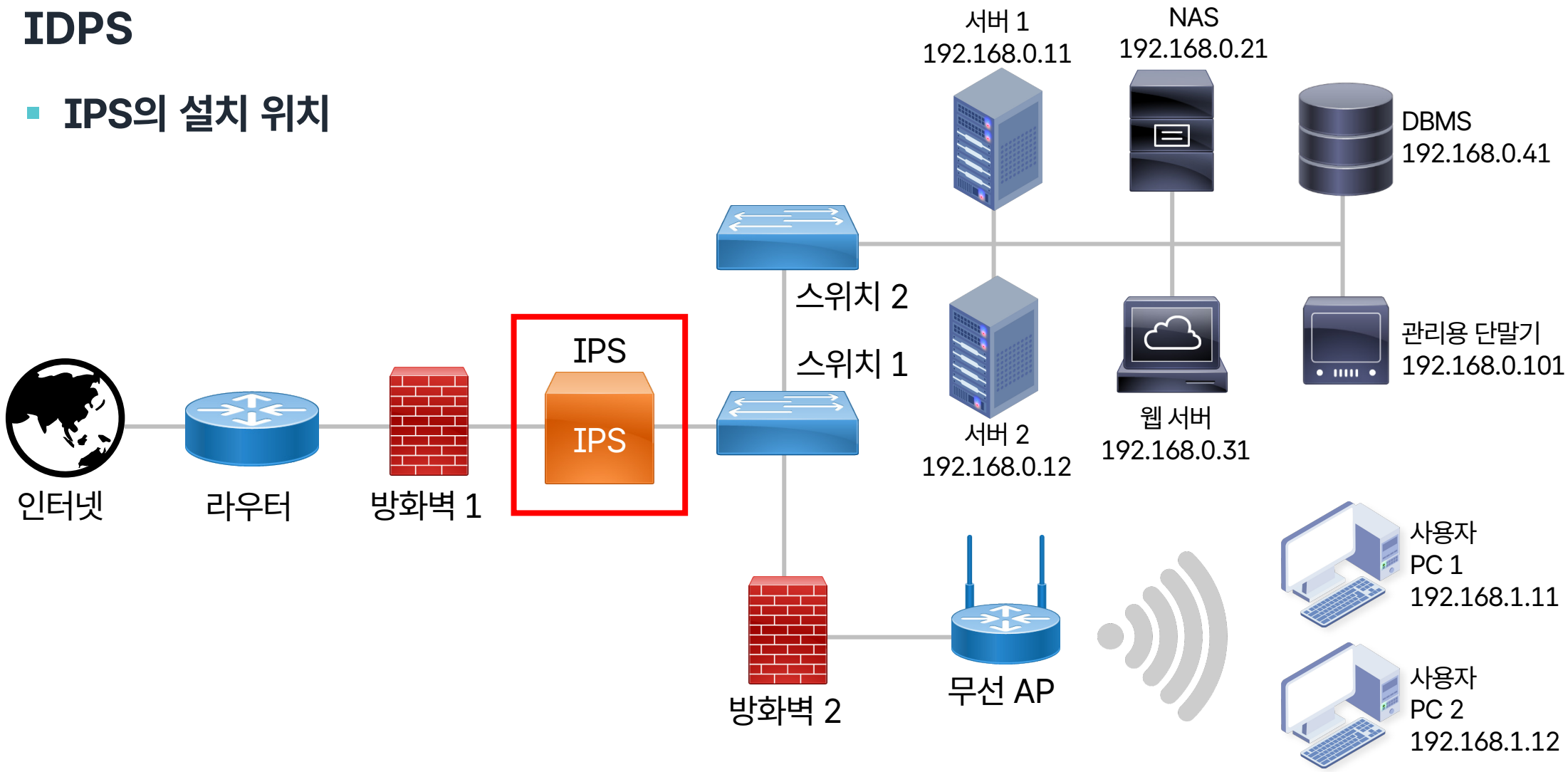
네트워크의 **모든 트래픽을 복제하여 복제된 트래픽이 정보보호시스템에 도달**하도록 구성하는 형태 → **IDS**는 미러링 모드로 구성

- 스위치의 포트 미러링 등의 기능을 활용하거나 별도의 TAP 장비를 사용하여 트래픽 복제
- 트래픽이 정보보호시스템을 경유하지 않아 네트워크에 대한 영향을 최소화할 수 있으나 실시간 대응(차단)은 불가

I IDPS의 이해

2 IDPS

- **IPS의 설치 위치**



2 IDPS

▪ IPS의 설치 위치

인라인(In-Line) 모드

네트워크의 **모든 트래픽이 반드시 정보보호시스템을 경유**하도록 구성하는 형태
→ **IPS**는 인라인 모드로 구성

- 규칙에 따라 패킷을 허용하거나 거부(차단) 가능
- 모든 패킷에 대한 판단이 요구되기 때문에 부하 발생 가능
  - 장애 발생 시 우회할 수 있게 구성하거나 아예 이중화 구성 필요

2 IDPS

▪ IDS의 활용

- 실시간으로 탐지할 뿐 아니라 차단까지 하면 좋겠지만, 과거에는 컴퓨터와 네트워크 성능이 열악했기 때문에 **차단 기능까지 구현하기에는 네트워크 성능을 저하시킬 우려**가 있었음
- IDS는 **실시간으로 탐지하고 사후적인 방식으로 대응**하기 위해 활용

2 IDPS

▪ IPS로의 전환

- 컴퓨터와 네트워크 성능의 발달로, IDS를 인라인으로 설치하여 실시간 차단 기능을 제공하더라도 **네트워크 성능을 과도하게 저하시키지 않을 수 있게 됨**
  - IPS로의 전환을 촉진하게 된 배경

    사후적인 방식으로 대응하기에 파급력이 지나치게 큼

    확산력이 빠른 공격이 증가함
- 다만, 초기의 IPS는 오탐률이 높아 정보통신망에 장애를 야기할 우려가 있었음
  - IPS를 도입했다 하더라도 차단 기능을 비활성화하고 IDS처럼 사용하는 경우도 많았음
  - 최근 몇 년 사이에 탐지 기술과 규칙들이 고도화되면서 차단 기능을 활성화(활용)하는 추세
- IPS는 **실시간으로 탐지하고 실시간으로 대응(차단)**하기 위해 활용

2 IDPS

▪ 주요 기능

- 침입탐지(Intrusion Detection)

오용탐지 기법	상태전이 기법	이상탐지 기법

전통적인 IDPS에서 기본적으로 채택하고 있는 기법으로,
알려진 공격 패턴을 미리 규칙으로 등록해두고 일치 여부를 탐지하는 방식

한계

- 알려진 공격 이외에는 탐지할 수 없음
- 대량의 데이터 분석에 적합하지 않고, 공격 순서를 추론하기 어려움

2 IDPS

▪ 주요 기능

- 침입탐지(Intrusion Detection)

오용탐지 기법	상태전이 기법	이상탐지 기법

공격 상황에 대한 시나리오를 작성하여 **각 상태에 따른 공격을 분석**하는 방식

한계

- 결과가 직관적이지만, 세밀한 시나리오 제작을 위해 고도의 기술과 노하우가 요구됨
- 추론 엔진이 포함되어 성능에 영향을 줄 수 있음

2 IDPS

▪ 주요 기능

- 침입탐지(Intrusion Detection)

오용탐지 기법	상태전이 기법	이상탐지 기법

급격한 변화의 발생이나 **발생 확률이 낮은 이벤트의 발생 여부를 탐지**하는 방식으로, 알려지지 않은 공격도 탐지할 수 있음

한계

인공지능 수준이 낮은 경우

- 오탐률이 높음
- 일정 기간 동안 학습이 필요함

2 IDPS

▪ 주요 기능

- 책임 추적성과 알림
  - 침입탐지 사실을 관제사들이 쉽게 인지할 수 있도록 실시간으로 표시하고 알리는 기능 제공
  - 기간별, 시간대별, 공격 유형별 등 필터링 및 분석 기능 제공
- 침입방지(Intrusion Prevention)
  - 탐지하고 알리는 데 그치지 않고 차단을 통해 능동적인 대응 수행

2 IDPS

▪ 방화벽과 IDPS의 비교

구분	방화벽 (침입차단시스템)	IDS (침입탐지시스템)	IPS (침입방지시스템)
목적	네트워크 경계의 보호 (헤더 기반 차단)	네트워크 경계 보호의 보강 (본문 데이터 기반 탐지)	네트워크 경계 보호의 보강 (본문 데이터 기반 차단)
차단 가능 여부	○	X	○
패킷 내용 분석	X	○	○
오용 탐지 (지정된 패턴)	-	○	○
오용 차단 (지정된 패턴)	-	X	○
이상 탐지 (지정된 패턴과 다른 패턴)	-	○	○
이상 차단 (지정된 패턴과 다른 패턴)	-	X	○

2 IDPS

▪ 방화벽과 IDPS의 비교

구분	방화벽 (침입차단시스템)	IDS (침입탐지시스템)	IPS (침입방지시스템)
특징	• 헤더만 검사하므로 속도가 빠름 • 본문 데이터는 검사 불가	• 본문 데이터도 실시간으로 검사하여 탐지 • 미러링 모드로 구성하여 네트워크 성능에 대한 영향 최소화 • 차단은 불가능하기 때문에 사후분석 대응 방식으로 활용	• 본문 데이터도 실시간으로 검사하여 탐지 • 인라인 모드로 구성하여 실시간 차단까지 가능 • 오탐 또는 장애 발생 시 네트워크 성능에 영향 • 성능이 좋은 경우 고가의 가격

II

정규표현식과 기본 문법

1 정규표현식(Regular Expression, Regex/Regexp)

정규표현식

어떤 문자열 내에서 '**특정한 형태나 규칙을 가진 문자열**'을 찾기 위해
그 **형태나 규칙을 나타내는 패턴을 정의**하는 식

1 정규표현식(Regular Expression, Regex/Regexp)

▪ 등장 배경

- Windows 등 GUI 운영체제가 대중화되기 전에는 방대한 양의 문자열을 편집하는 과정에서 문자열을 찾거나 선택하거나 교체하기 위해 명령어(식)을 입력

POSIX 정규식	vim 정규식	PCRE
• 이 때 사용된 명령어(식)는 POSIX 표준에 편입	• POSIX 정규식 중 표준식 (Basic Regular Expression, BRE)을 기본 골격으로 하여 vi/vim 편집기에 사용된 정규표현식	• Perl Compatible Regular Expression • Perl(프로그래밍 언어) 스크립트 언어에서 발전된 정규표현식 • IDPS에서 널리 사용

2 정규표현식의 필요성

```
In this example, we will explore various patterns within a text. The
text includes several repeated phrases like "data data data analysis"
and "data data data data analysis", numbers in sequences such as 123,
456, and 789, and patterns like 101-202-3030 and 404-505-6060. You
can find phone numbers formatted as (123) 456-7890, emails like
example@example.com, and dates in the format of 2023-02-20. The
purpose of "pattern recognition" in pattern recognition is to
illustrate how regex can be effectively used for data extraction and
text analysis. For more information, visit our website at
https://www.regex-example.com.
```

3 정규표현식의 문법

▪ 정규표현식의 시작과 끝

/패턴/패턴변경자

- 시작과 끝은 같은 구분자를 사용
- 일반적으로 /(슬래시, Slash)를 많이 사용하지만,
  정규표현식 내 슬래시가 포함되는 경우는 다른 문자를 사용할 수도 있음

3 정규표현식의 문법

- **리터럴 (Literal)**

/**패턴**/패턴변경자

- 문자 그대로의 값을 의미
- 이를테면 apple을 찾는 경우 apple을 그대로 기재

/**apple**/패턴변경자

3 정규표현식의 문법

- **메타 문자 (Meta Character)**

/**패턴**/패턴변경자

문자	의미	문자	의미
\	이스케이프 문자 (특별한 문자를 그대로 사용하고자 할 때)	[	클래스의 시작
		]	클래스의 끝
^	문자열(단어 등) 시작	(	그룹의 시작
$	문자열(단어 등) 끝	)	그룹의 끝
.	개행 문자를 제외한 모든 단일 문자	{	수량 한정자의 시작
|	또는(OR) 연산	}	수량 한정자의 끝

3 정규표현식의 문법

- **메타 문자 (Meta Character)**

/**패턴**/패턴변경자

문자	의미	문자	의미
[^]	(대괄호 안에서) ^ 이후의 문자열 패턴과 일치하지 않는 패턴	**\d**	모든 숫자에 대응하는 패턴 = [0-9]
\b	문자와 공백 사이를 구분하는 패턴	**\D**	\d 가 아닌 패턴 = [^0-9]
\B	\b 가 아닌 패턴	**\w**	단어를 만들 수 있는 영문 대소문자, 숫자, 밑줄을 포함하는 패턴 = [A-Za-z0-9_]
\s	모든 공백 문자에 대응하는 패턴	**\W**	\w 에 포함되지 않는 문자들의 패턴
\S	\s 가 아닌 패턴	**\n**	개행 문자 패턴

3 정규표현식의 문법

- **수량한정자 (Quantifier)**

/**패턴**/패턴변경자

문자	의미
`?`	바로 앞의 글자 또는 그룹이 1개 또는 0개인 경우
`*`	0개 이상인 경우
`+`	1개 이상인 경우
`{n}`	n개인 경우
`{n, m}`	n개 이상 m개 이하인 경우

3 정규표현식의 문법

- **탐색 (Look Ahead/Behind)**

/**패턴**/패턴변경자

문자	의미
?=	(전방 탐색) ?= 에 붙는 문자열을 기준으로 앞의 문자열을 추출
?<=	(후방 탐색) ?<= 에 붙는 문자열을 기준으로 뒤의 문자열을 추출

3 정규표현식의 문법

- **패턴변경자 (Flag)**

/패턴/**패턴변경자**

문자	의미
i	대소문자 구분하지 않고 검색
m	여러 줄에 걸쳐 검색
s	개행 문자를 문자로 포함하여 검색
x	대부분의 공백을 무시하고 검색
g	일치하는 모든 것들을 검색

4 정규표현식 활용 예제

```
In this example, we will explore various patterns within a text. The
text includes several repeated phrases like "data data data analysis"
and "data data data data analysis", numbers in sequences such as 123,
456, and 789, and patterns like 101-202-3030 and 404-505-6060. You
can find phone numbers formatted as (123) 456-7890, emails like
example@example.com, and dates in the format of 2023-02-20. The
purpose of "pattern recognition" in pattern recognition is to
illustrate how regex can be effectively used for data extraction and
text analysis. For more information, visit our website at
https://www.regex-example.com.
```

4 정규표현식 활용 예제

```
In this example, we will explore various patterns within a text. The
text includes several repeated phrases like "data data data analysis"
and "data data data data analysis", numbers in sequences such as 123,
456, and 789, and patterns like 101-202-3030 and 404-505-6060. You
can find phone numbers formatted as (123) 456-7890, emails like
example@example.com, and dates in the format of 2023-02-20. The
purpose of "pattern recognition" in pattern recognition is to
illustrate how regex can be effectively used for data extraction and
text analysis. For more information, visit our website at
https://www.regex-example.com.
```

- **특정 단어 찾기**

  예 `/data/g`

4 정규표현식 활용 예제

```
In this example, we will explore various patterns within a text. The
text includes several repeated phrases like "data data data analysis"
and "data data data data analysis", numbers in sequences such as 123,
456, and 789, and patterns like 101-202-3030 and 404-505-6060. You
can find phone numbers formatted as (123) 456-7890, emails like
example@example.com, and dates in the format of 2023-02-20. The
purpose of "pattern recognition" in pattern recognition is to
illustrate how regex can be effectively used for data extraction and
text analysis. For more information, visit our website at
https://www.regex-example.com.
```

- **숫자 찾기**

  예 `/\d/g`

4 정규표현식 활용 예제

```
In this example, we will explore various patterns within a text. The
text includes several repeated phrases like "data data data analysis"
and "data data data data analysis", numbers in sequences such as 123,
456, and 789, and patterns like 101-202-3030 and 404-505-6060. You
can find phone numbers formatted as (123) 456-7890, emails like
example@example.com, and dates in the format of 2023-02-20. The
purpose of "pattern recognition" in pattern recognition is to
illustrate how regex can be effectively used for data extraction and
text analysis. For more information, visit our website at
https://www.regex-example.com.
```

- **전화번호 찾기**

  예 `/\(\d{3}\)\s\d{3}-\d{4}/g`

4 정규표현식 활용 예제

```
In this example, we will explore various patterns within a text. The
text includes several repeated phrases like "data data data analysis"
and "data data data data analysis", numbers in sequences such as 123,
456, and 789, and patterns like 101-202-3030 and 404-505-6060. You
can find phone numbers formatted as (123) 456-7890, emails like
example@example.com, and dates in the format of 2023-02-20. The
purpose of "pattern recognition" in pattern recognition is to
illustrate how regex can be effectively used for data extraction and
text analysis. For more information, visit our website at
https://www.regex-example.com.
```

- **여러 형식의 전화번호 찾기 ('또는' 연산자 사용)**

  예 `/(\(\d{3}\)\s\d{3}-\d{4})|(\d{3}-\d{3}-\d{4})/g`

4 정규표현식 활용 예제

```
In this example, we will explore various patterns within a text. The
text includes several repeated phrases like "data data data analysis"
and "data data data data analysis", numbers in sequences such as 123,
456, and 789, and patterns like 101-202-3030 and 404-505-6060. You
can find phone numbers formatted as (123) 456-7890, emails like
example@example.com, and dates in the format of 2023-02-20. The
purpose of "pattern recognition" in pattern recognition is to
illustrate how regex can be effectively used for data extraction and
text analysis. For more information, visit our website at
https://www.regex-example.com.
```

- **이메일주소 찾기**

  예 `/[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}/g`

4 정규표현식 활용 예제

```
In this example, we will explore various patterns within a text. The
text includes several repeated phrases like "data data data analysis"
and "data data data data analysis", numbers in sequences such as 123,
456, and 789, and patterns like 101-202-3030 and 404-505-6060. You
can find phone numbers formatted as (123) 456-7890, emails like
example@example.com, and dates in the format of 2023-02-20. The
purpose of "pattern recognition" in pattern recognition is to
illustrate how regex can be effectively used for data extraction and
text analysis. For more information, visit our website at
https://www.regex-example.com.
```

- **날짜 찾기**

  예 `/\d{4}-\d{2}-\d{2}/g`

4 정규표현식 활용 예제

```
In this example, we will explore various patterns within a text. The
text includes several repeated phrases like "data data data analysis"
and "data data data data analysis", numbers in sequences such as 123,
456, and 789, and patterns like 101-202-3030 and 404-505-6060. You
can find phone numbers formatted as (123) 456-7890, emails like
example@example.com, and dates in the format of 2023-02-20. The
purpose of "pattern recognition" in pattern recognition is to
illustrate how regex can be effectively used for data extraction and
text analysis. For more information, visit our website at
https://www.regex-example.com.
```

- **URL 찾기**

  예 `/https?://[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}(?:/[a-zA-Z0-9._%+-]*)*/g`

III

IDPS 정책 · 규칙 구성

IDPS 정책 · 규칙 구성

1 IDPS의 탐지/차단 원리

- **IDPS의 특성상 블랙리스트 방식으로 동작**
  - IDPS를 설치하더라도 적절한 탐지/차단 규칙을 등록하지 않으면 설치하지 않은 것과 다르지 않은 상태에 불과

III IDPS 정책 · 규칙 구성

1 IDPS의 탐지/차단 원리

방화벽	IDPS
헤더를 검사하기 때문에 IP와 포트(서비스)와 같은 항목을 표 형태로 구성하여 차단 규칙을 관리	본문 데이터(메시지)까지 검사하기 때문에 검사하고자 하는 문자열이나 값에 대한 사항을 구성하여 탐지/차단 규칙을 관리

- **천차만별인 본문 데이터에서 어떤 내용을 검사할 지 정의해줘야 함**
  - 검사할 내용이 매번 동일한 경우도 있겠지만, 규칙성을 갖고 변화하는 경우도 있음
- **내용을 검사하는 것은 컴퓨팅 자원을 많이 활용하여 네트워크 성능에 영향이 있으므로, 빠르고 정확하게 검사할 수 있는 기술과 엔진이 요구됨**

IDPS 정책 · 규칙 구성

2 IDPS의 탐지/차단 규칙

- 대부분의 IDPS는 PCRE 정규표현식 규격을 적용한 오픈소스 IDS인 Snort를 널리 활용하고 있기 때문에 IDPS 탐지/차단 규칙을 **Snort 규칙(Snort Rule)**이라고도 함

Snort Rule	동작	프로토콜	출발지 IP	출발지 포트	방향	목적지 IP	목적지 포트	내용

IDPS 정책 · 규칙 구성

2 IDPS의 탐지/차단 규칙

Snort Rule	동작	프로토콜	출발지 IP	출발지 포트	방향	목적지 IP	목적지 포트	내용

- **동작**

alert	규칙과 일치하는 경우 경고를 발생시키고 로그 파일에 기록
log	로그 파일에 기록
pass	패킷을 무시
drop	패킷을 차단하고 로그 파일에 기록
reject	패킷을 차단하고 로그 파일에 기록하며 프로토콜에 따라 대응 • TCP 패킷 : RST(리셋) 응답 • UDP 패킷 : ICMP Unreachable 패킷 응답
sdrop	패킷을 차단하되 로그 파일에 기록하지는 않음

IDPS 정책 · 규칙 구성

2 IDPS의 탐지/차단 규칙

- **프로토콜**

IDPS 정책 · 규칙 구성

2 IDPS의 탐지/차단 규칙

- **IP 주소**

any	모두 • 부정 연산자(!) 사용 가능
[]	여러 IP 주소들을 지정하는 경우 사용하며 콤마(,)로 구분

- IP 대역을 지정하는 경우 'IP 주소(네트워크 주소)/비트수' 형태로 표시

IDPS 정책 · 규칙 구성

2 IDPS의 탐지/차단 규칙

- **포트 번호**

n:m	n ~ m
:n	n 이하
n:	n 이상
!n:m	n ~ m을 제외한 나머지 (부정 연산자 사용)
[]	여러 포트 번호들을 지정하는 경우 사용하며 콤마(,)로 구분

IDPS 정책 · 규칙 구성

2 IDPS의 탐지/차단 규칙

Snort Rule	동작	프로토콜	출발지 IP	출발지 포트	방향	목적지 IP	목적지 포트	내용

- **방향**

->	출발지에서 목적지까지의 방향
<>	출발지와 목적지 사이의 모든 방향
<-	(존재하지 않음)

2 IDPS의 탐지/차단 규칙

- **내용**
  - 내용은 괄호로 둘러싸며, 각 항목 사이를 세미콜론(;)으로 구분
  - 항목은 '항목명: 값' 형태로 구성

    예 (msg: "SQL Injection Type 1"; content: "-- 1 or 1;"; nocase; sid: 1000001;)

IDPS 정책 · 규칙 구성

2 IDPS의 탐지/차단 규칙

- **내용**
  - 옵션

msg	액션이 alert인 경우 표시할 내용 (관제사가 확인하는 탐지명)
sid	규칙 ID • ~99 : 시스템 예약 ID • 100~1,000,000 : Snort 자체 지정 SID • 1,000,001~ : 사용자 정의
rev	규칙 수정 횟수(버전)

2 IDPS의 탐지/차단 규칙

- **내용**
  - 탐지 범위와 세부 내용

dsize	상한 범위 또는 하한 범위 (바이트 단위)
content	정적 문자열 또는 HEX 값
offset	검색을 건너뛸 바이트 수
depth	offset을 기점으로 검색할 바이트 수
nocase	대소문자를 구별하지 않음
flags	TCP 제어 플래그
pcre	정규표현식 (동적 문자열, 동적 값 등)

IDPS 정책 · 규칙 구성

2 IDPS의 탐지/차단 규칙

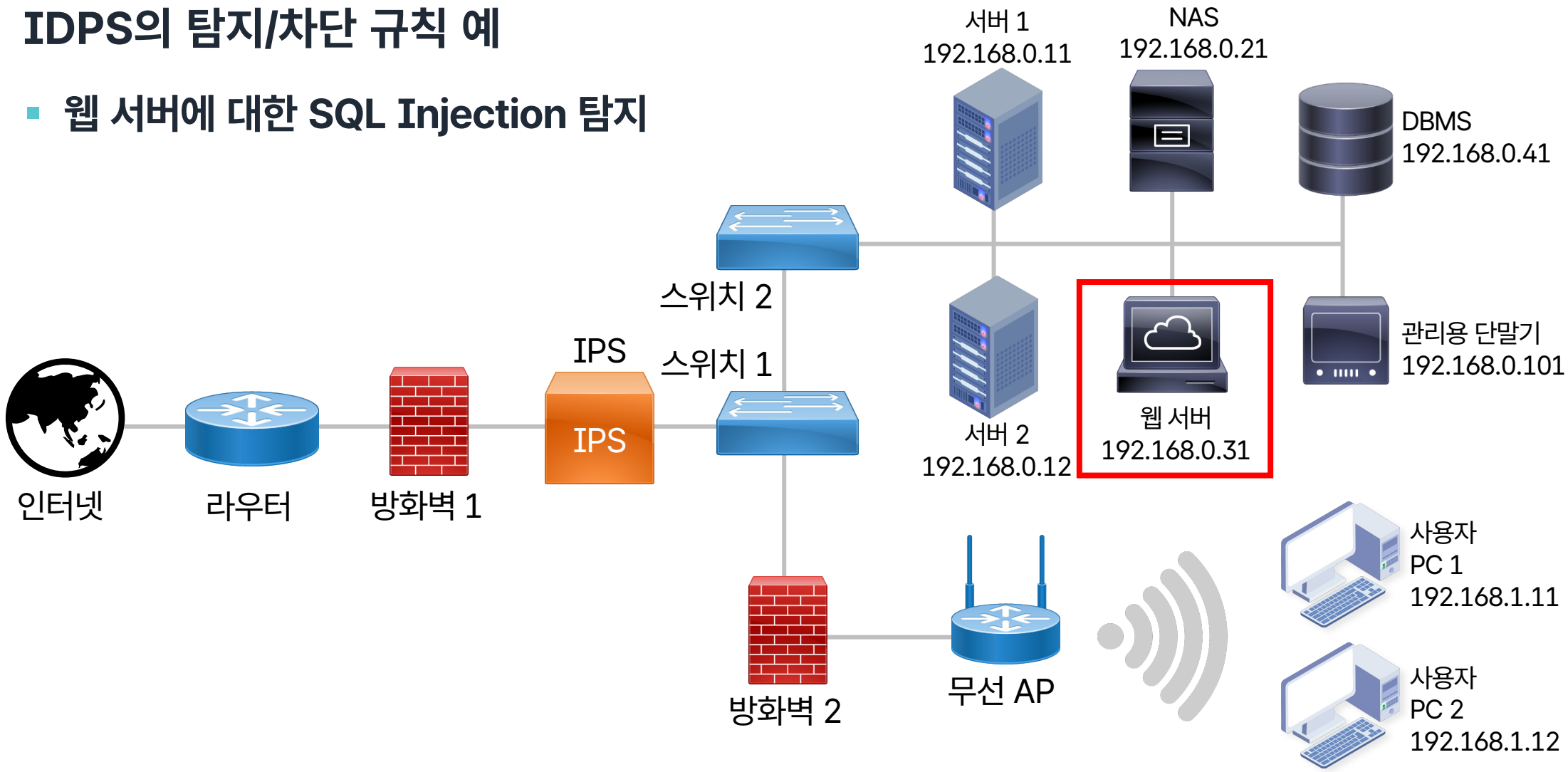
- **내용**
  - 탐지 범위와 세부 내용

threshold	발생량 기반 탐지 • type limit(임계값 기준) / threshold(패킷량 기준) / both(IP 기준) • track by_src(출발지 IP 기준 추적) / by_dst(목적지 IP 기준 추적) • count n : 횟수 • seconds m : 초

III IDPS 정책 · 규칙 구성

3 IDPS의 탐지/차단 규칙 예

- 웹 서버에 대한 SQL Injection 탐지



3 IDPS의 탐지/차단 규칙 예

- **웹 서버에 대한 SQL Injection 탐지**
  - 공격 페이로드

```
' OR 1 = 1; #
```

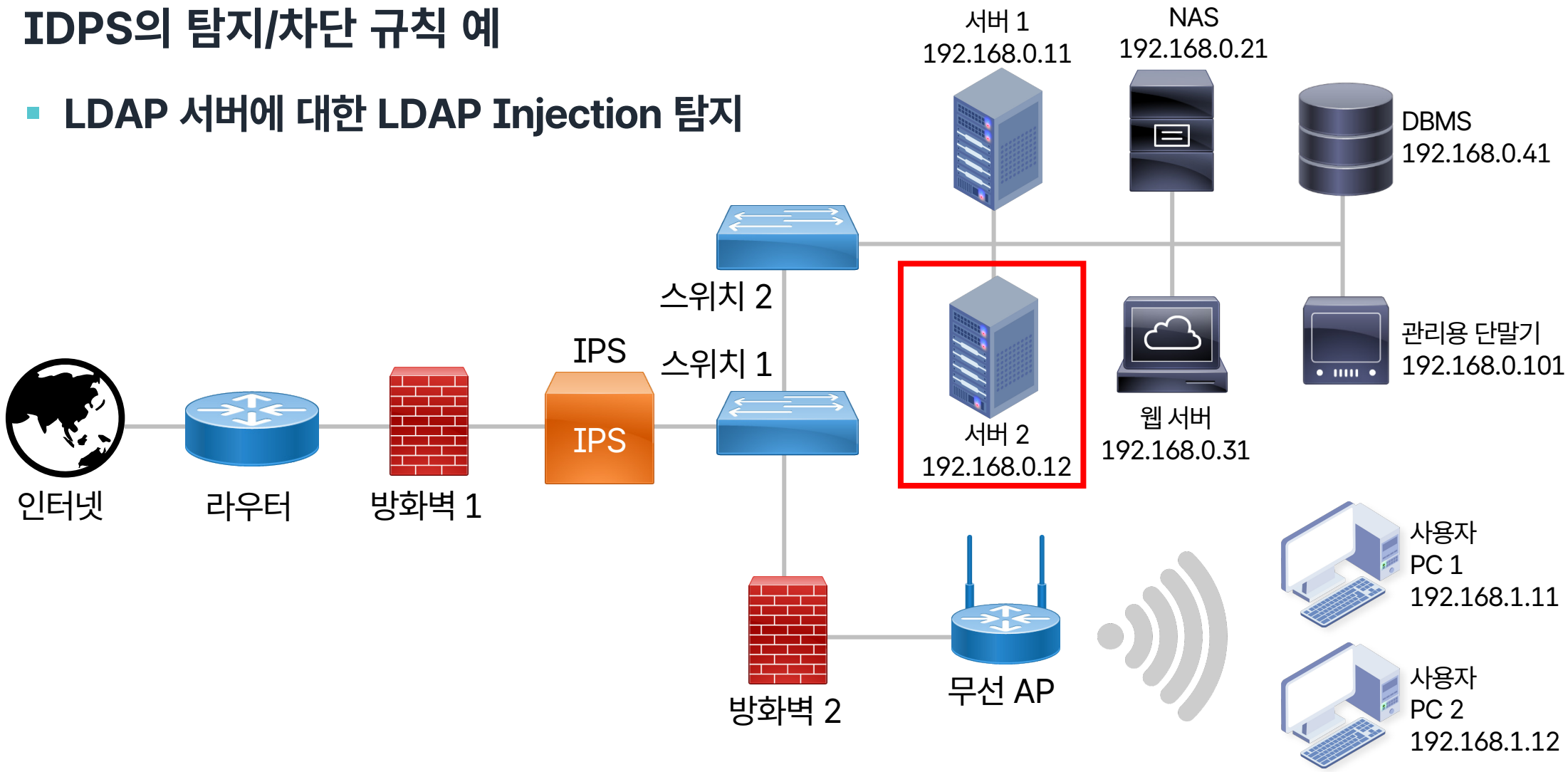
  - 대응 규칙 작성 예

```
alert tcp any any -> 192.168.0.31 [80,443] (msg: "SQL Injection -
OR"; pcre: "/'\s*OR\s*1=1\s*;?\s*\#/i"; sid: 1000001;)
```

IDPS 정책 · 규칙 구성

3 IDPS의 탐지/차단 규칙 예

- LDAP 서버에 대한 LDAP Injection 탐지



3 IDPS의 탐지/차단 규칙 예

- **LDAP 서버에 대한 LDAP Injection 탐지**
  - 공격 페이로드

```
(|(userPassword=*))
```

```
(&(objectClass=*))
```

```
(&(uid=admin)(userPassword=*))
```

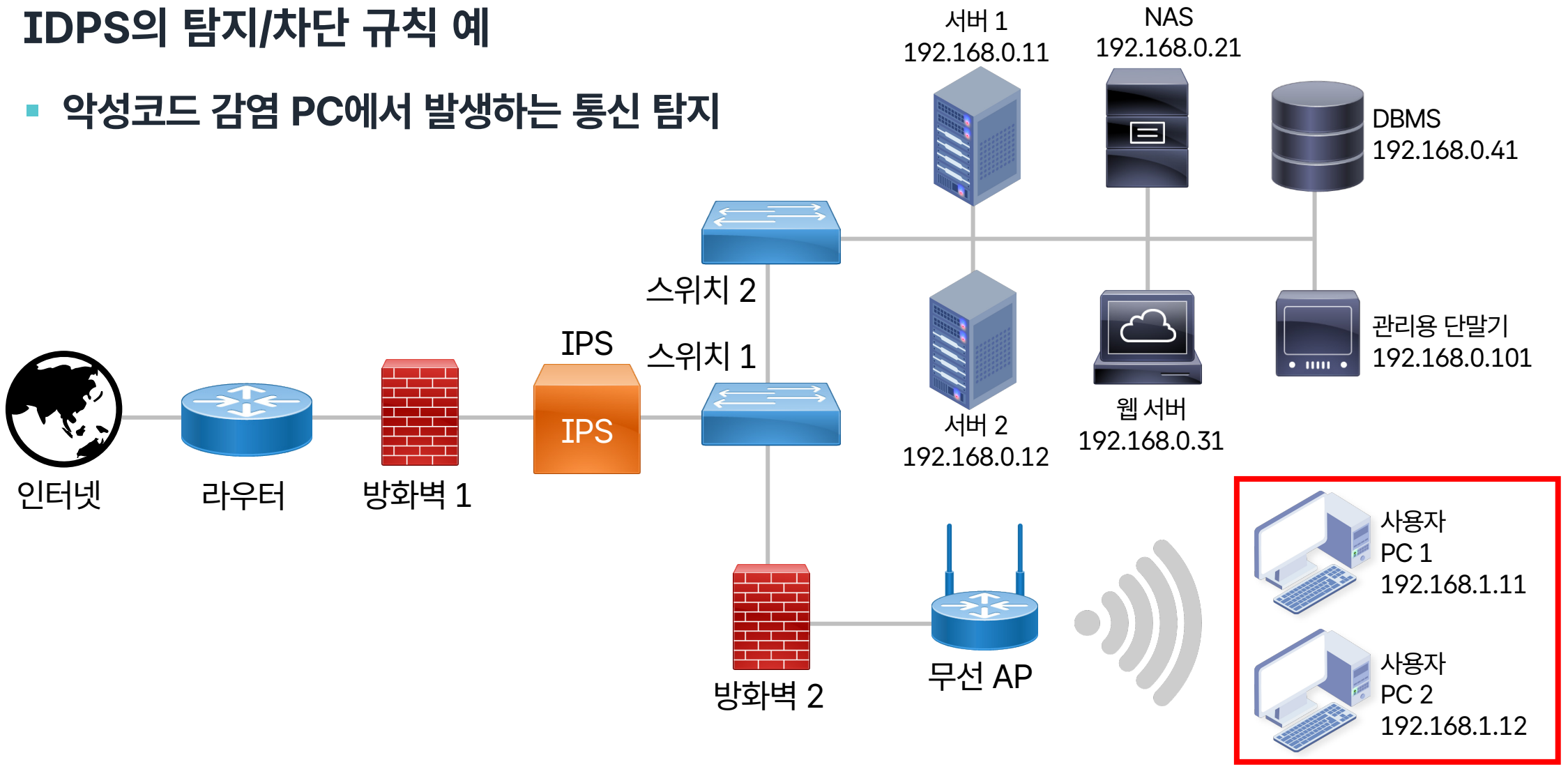
  - 대응 규칙 작성 예

```
alert tcp any any -> 192.168.0.31 [389] (msg: "LDAP Injection";
content:"(|"; pcre: "/\(|\&\)\((objectClass|userPassword|uid)=\*.
*\)/i"; sid: 1000002;)
```

IDPS 정책 · 규칙 구성

3 IDPS의 탐지/차단 규칙 예

- 악성코드 감염 PC에서 발생하는 통신 탐지



3 IDPS의 탐지/차단 규칙 예

- **악성코드 감염 PC에서 발생하는 통신 탐지**
  - 공격 페이로드

```
Mal0Day SEND ALIVE
```

```
Mal0Day SEND ANY UPDATE
```

```
Mal0Day GET https://x.com/status/000000000000
```

  - 대응 규칙 작성 예

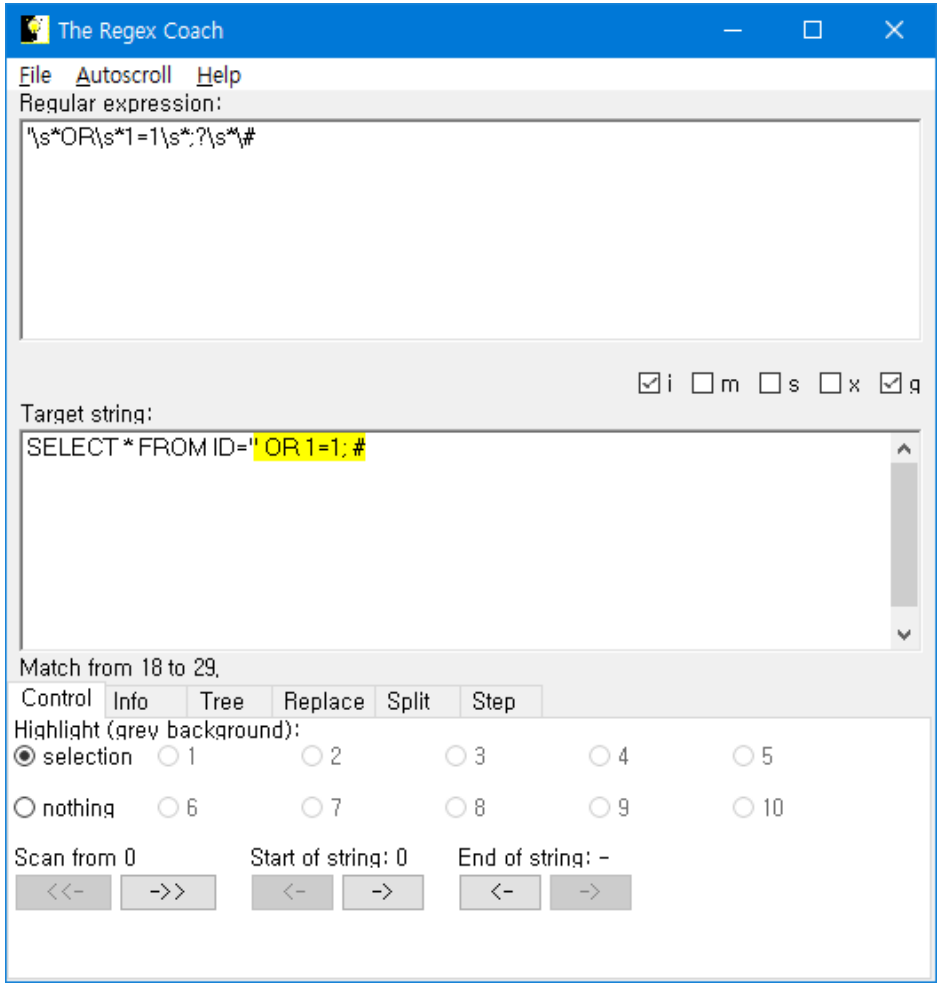
```
alert tcp 192.168.1.0/24 any -> any any (msg: "Mal0Day Malware C2
Signature"; content:"Mal0Day"; pcre:"/^Mal0Day\s/"; sid: 1000003;)
```

PCRE 기반 IDPS 규칙 작성

IV PCRE 기반 IDPS 규칙 작성

1 실습 도구 안내

- **The Regex Coach**
  - 2003부터 2008년까지 Edmund Weitz 박사가 개발하여 공개한 교육용 실습 도구
  - 하단의 Target string에 대상 문자열을 넣고 상단의 Regular expression에 검색할 내용을 PCRE로 작성하면 대화식으로 결과를 확인 가능



출처 The Regex Coach - interactive regular expressions, http://www.weitz.de/regex-coach/

PCRE 기반 IDPS 규칙 작성

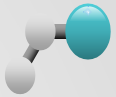
2 실습

- **The Regex Coach**

요약 정리

- 지금까지 학습한 내용을 정리해보겠습니다.

요약정리



- **IDPS의 이해**
  - **IDS (Intrusion Detection System)**
    - 네트워크간 전송되는 패킷을 수집하고 내용을 분석하여 침해시도를 탐지
      - 미러링 모드로 구성하여 네트워크 성능에 대한 영향 최소화
    - 차단은 불가능하기 때문에 사후분석 대응 방식으로 활용
  - **IPS (Intrusion Prevention System)**
    - 네트워크간 전송되는 패킷을 수집하고 내용을 분석하여 침해시도를 탐지하고 차단
      - 인라인 모드로 구성하여 실시간 차단
    - 차단도 가능하지만 오탐 또는 장애 발생 시 네트워크 성능에 영향 가능성
  - **방화벽(침입차단시스템)과의 차이**
    - 방화벽은 1차 방어선을 구축해주지만 본문 데이터(메시지)까지 들여다볼 수는 없다는 한계
    - 방화벽을 설치한 상태에서 IDPS를 추가 설치함으로써 네트워크 경계 보호 보강

요약정리

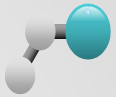
정규표현식과 기본 문법

정규표현식 (Regular Expression, Regex/Regexp)

- 어떤 문자열 내에서 '특정한 형태나 규칙을 가진 문자열'을 찾기 위해 그 패턴을 정의하는 식
- **PCRE(Perl Compatible Regular Expression)** : Perl 스크립트 언어에서 발전된 정규표현식
  - IDPS에서 널리 사용

기본 문법

- 시작과 끝 : 시작과 끝은 같은 구분자를 사용
- 리터럴 (Literal) : 문자 그대로의 값
- 메타 문자 (Meta Character) : 이스케이프 문자, OR 연산, 개행 문자, 클래스, 그룹, 수량한정자 등
- 수량한정자 (Quantifier) : 개수의 범위를 지정
- 탐색 (Look Ahead/Behind) : 전방 또는 후방 탐색 범위를 지정
- 패턴변경자 (Flag) : 검색 조건을 지정



IDPS 정책 · 규칙 작성

Snort 규칙

- 대부분의 IDPS는 PCRE 규격을 적용한 오픈소스 IDS인 Snort를 널리 활용하고 있기 때문에 IDPS 탐지/차단 규칙을 Snort 규칙(Snort Rule)이라고도 함.
- 동작, 프로토콜, 출발지 IP, 출발지 포트, 방향, 목적지 IP, 목적지 포트, 내용 순으로 구성
  - 동작 : alert, log, pass, drop, reject, sdrop
  - 프로토콜 : TCP, UDP, ICMP, IP
  - IP 주소 : 단일 IP 주소, IP 주소 대역(클래스 표기), 여러 IP 주소(대괄호와 콤마(,) 사용)
  - 포트 번호 : 단일 포트 번호, 포트 번호 범위(콜론(:) 사용), 여러 포트 번호(대괄호와 콤마(,) 사용)
  - 방향 : ->(단일 방향), <>(양방향)
  - 내용 : 내용은 괄호로 둘러싸며, 각 항목 사이를 세미콜론(;)으로 구분하고, 항목은 '항목명: 값' 형태로 구성
    옵션 : msg, sid, rev
    탐지 범위와 세부 내용 : dsize, content, offset, depth, nocase, flags, pcre, threshold

참고문헌

- 정보통신기반보호법 (법률)
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (법률)
- 사이버안보 업무규정 (대통령령)
- 국가사이버안전관리규정 (대통령훈령)
- 국가 정보보안 기본지침 (국가정보원 지침)
- 보안관제학, 2014, 안성진 등 공저, 이한미디어
- 2023 국가정보보호백서, 2023, 국가정보원 등 관계기관 합동
- 국가사이버안보센터 웹 사이트, http://www.ncsc.go.kr
- 한국인터넷진흥원 웹 사이트, http://www.kisa.or.kr
- KISA 보호나라 & KrCERT/CC 웹 사이트, http://www.krcert.or.kr
- Common Criteria 웹 사이트, http://commoncriteriaportal.org

참고문헌

- IT보안인증사무국 웹 사이트, http://itscc.kr
- '빗썸' 해킹 징후 있었는데…"한국은 먹잇감", KBS, 2018.06.21, https://www.youtube.com/watch?v=3MQzCDFQ-7Q
- The Regex Coach - interactive regular expressions, http://www.weitz.de/regex-coach/

수고하셨습니다