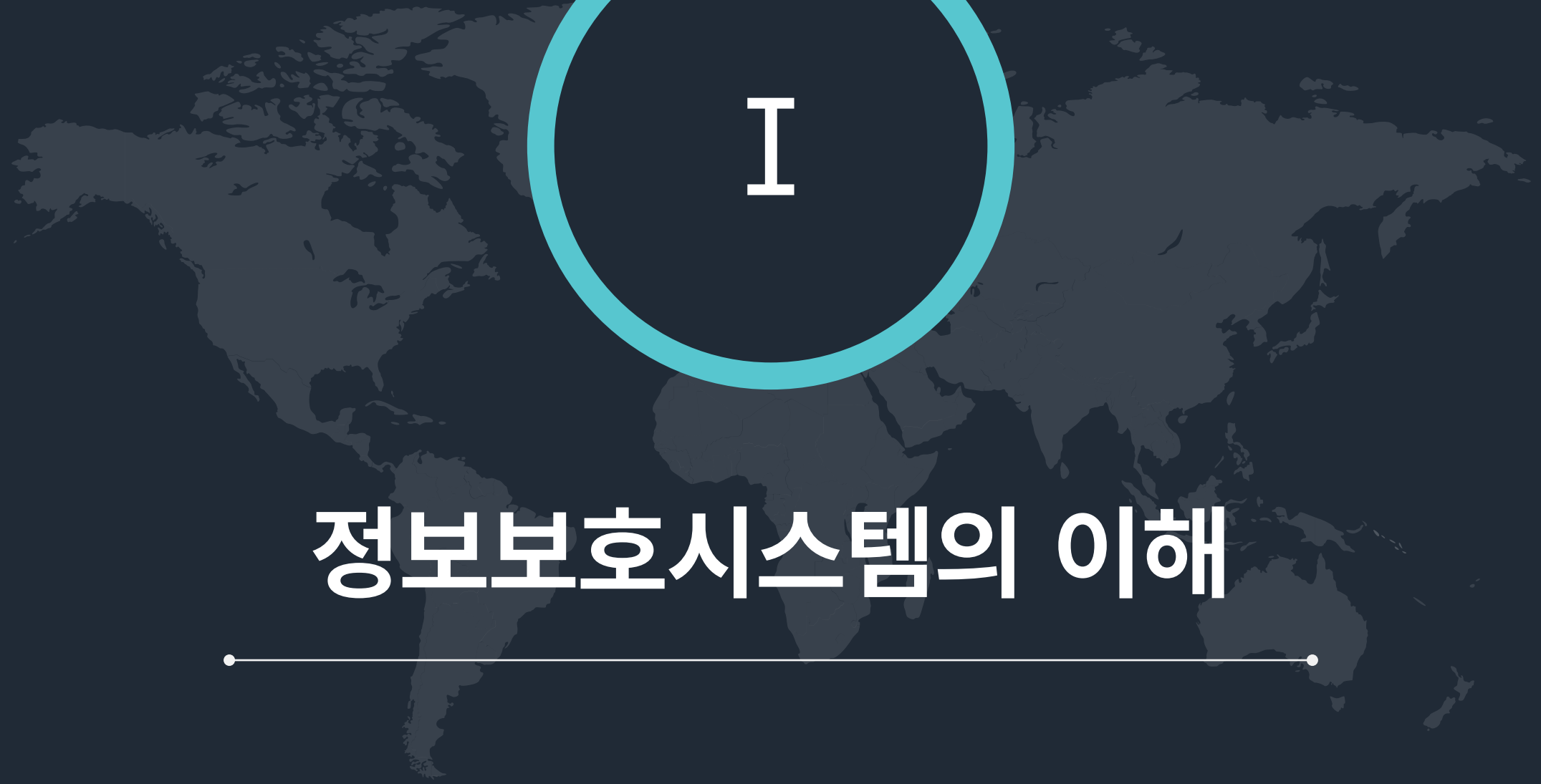
CHAPTER 07

방화벽 (침입차단시스템)

이현호 hyeonholee@korea.com

목차



I

정보보호시스템의 이해

I 정보보호시스템의 이해

1 정보보호시스템의 필요성

▪ 정보보호시스템

- 정보의 접근통제 등을 위해 사용하는 어플라이언스 또는 소프트웨어

어플라이언스

소프트웨어를 내장한 하드웨어 형태(하드웨어 + 소프트웨어)

소프트웨어

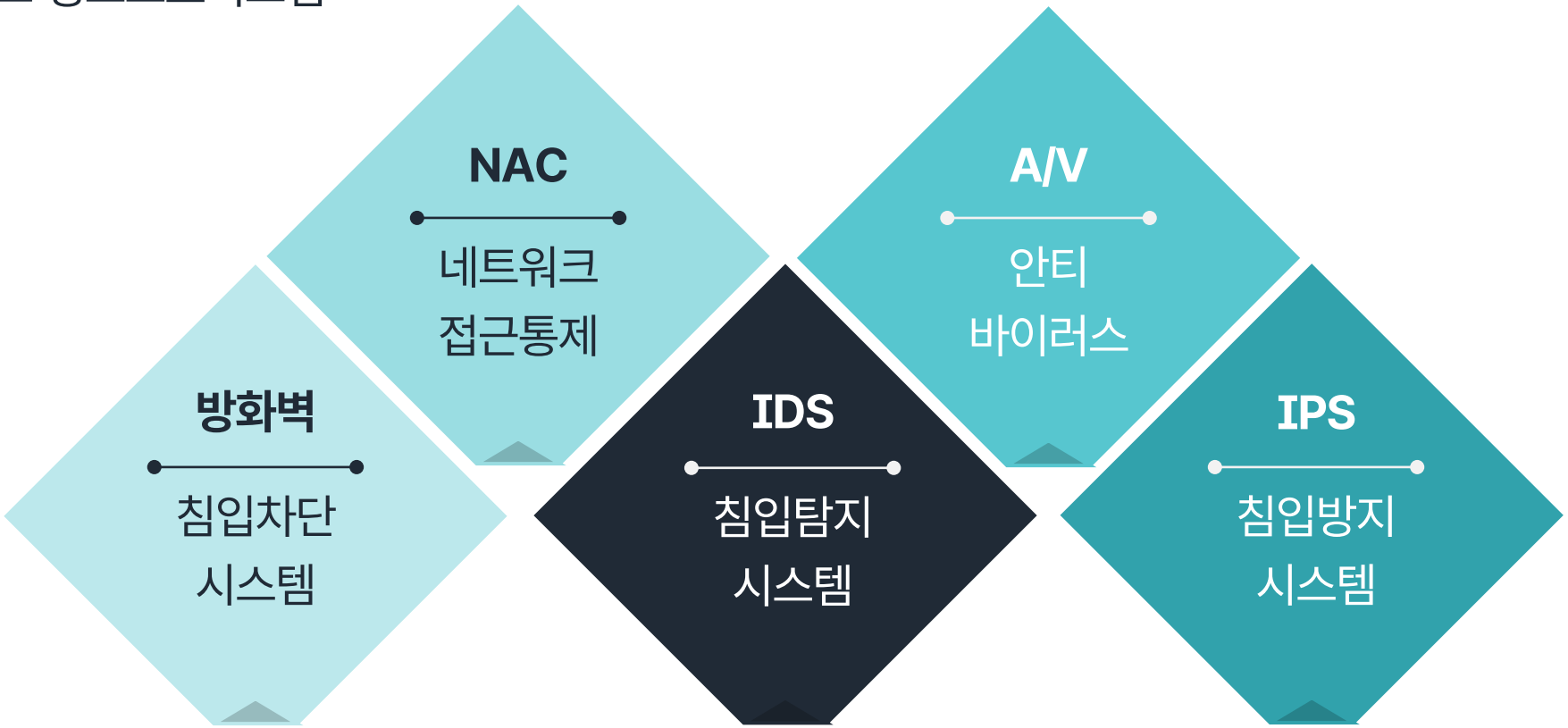
호스트에 설치할 수 있는 컴퓨터 프로그램 형태

- 사이버공격 및 침해시도를 탐지하거나 차단하고 보안 정보 및 이벤트로 보관
- 과거에는 보안관제사가 개별 정보보호시스템을 각각 들여다보는 방식으로 관제 업무 수행

정보보호시스템의 이해

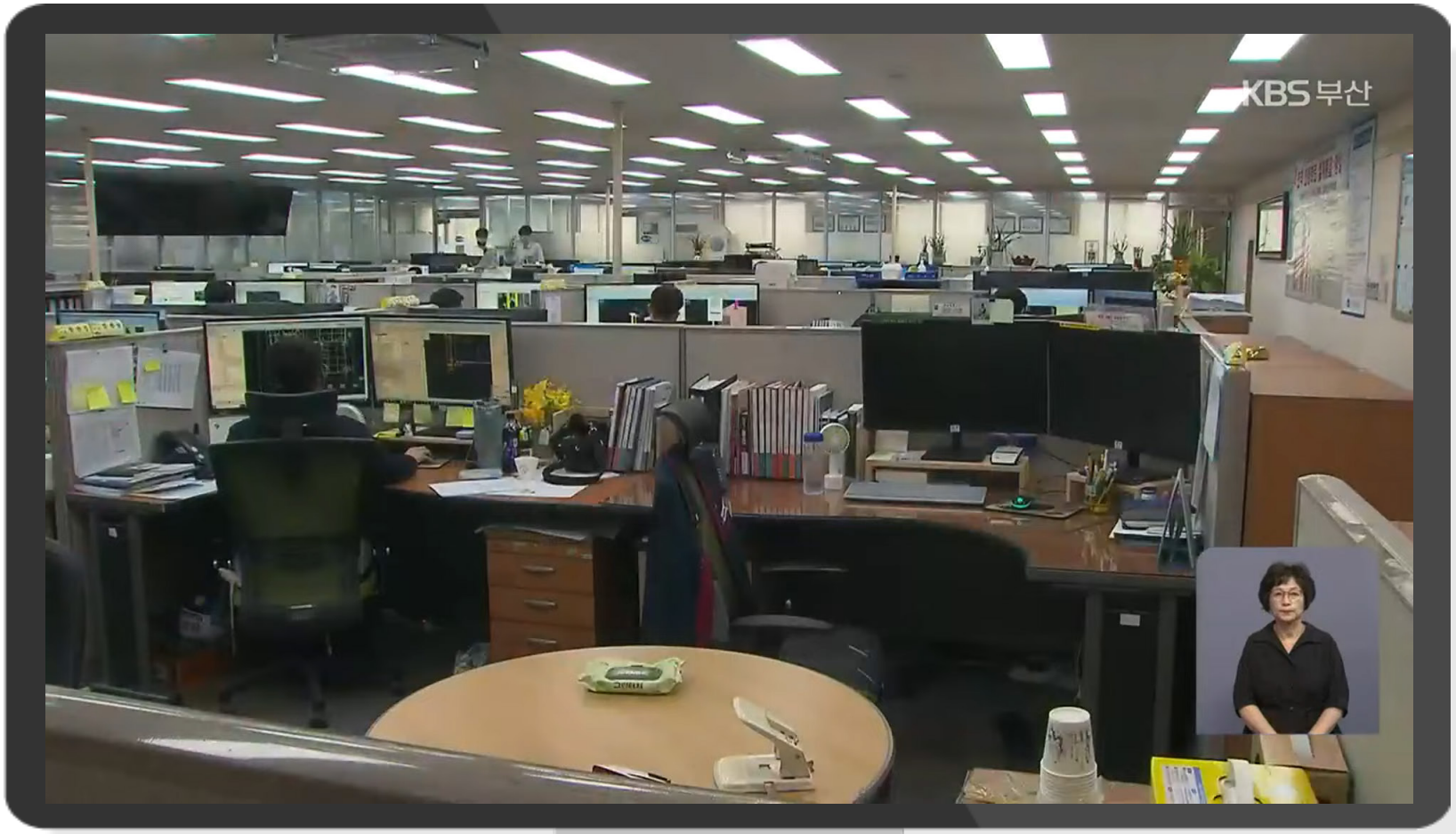
1 정보보호시스템의 필요성

- **정보보호시스템**
  - 주요 정보보호시스템



I 정보보호시스템의 이해

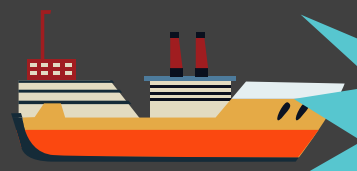
1 정보보호시스템의 필요성



출처 지역 기업 사이버 보안 '취약'…투자계획도 없어, KBS(2023.09.07), https://www.youtube.com/watch?v=_teCTriqgjM

1 정보보호시스템의 필요성

부산의 한 조선기자재 업체의 랜섬웨어 피해 사례



조선기자재 업체
계열사 2곳

랜섬웨어 피해

설계도면 & 파일 손실

↓

방화벽 설치

소 잃고 외양간 고쳤지만 사이버보안 강화

출처 지역 기업 사이버 보안 '취약'…투자계획도 없어, KBS(2023.09.07), https://www.youtube.com/watch?v=_teCTriqgjM

I 정보보호시스템의 이해

1 정보보호시스템의 필요성

부산의 한 조선기자재 업체의 랜섬웨어 피해 사례

방화벽과 같은
정보보호시스템
구비 ✕

정보통신망 및 정보시스템이
무분별하게 외부에 노출

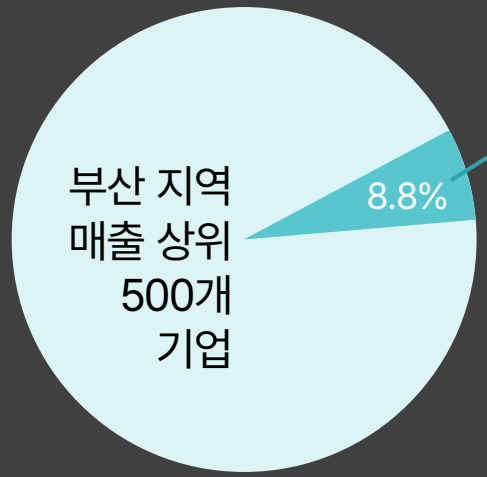
↓

침해사고 발생 가능성 ↑

출처 지역 기업 사이버 보안 '취약'…투자계획도 없어, KBS(2023.09.07), https://www.youtube.com/watch?v=_teCTriqgjM

1 정보보호시스템의 필요성

부산의 한 조선기자재 업체의 랜섬웨어 피해 사례



설문조사 결과

- 해킹과 랜섬웨어 같은 침해사고 경험이 있음
- 사이버보안에 취약한 기업은 거의 절반에 달하는 수준
- 대다수의 기업들이 비용 부담 등의 이유로 사이버보안에 대한 투자계획이 전무

침해사고는 **중요한 기업기밀의 유출과 손실 등 심각한 위험**으로 이어질 수 있는 만큼 이를 예방하기 위해 **기본적인 정보보호시스템을 갖추는 것**이 중요

출처 지역 기업 사이버 보안 '취약'…투자계획도 없어, KBS(2023.09.07), https://www.youtube.com/watch?v=_teCTriqgjM

I 정보보호시스템의 이해

1 정보보호시스템의 필요성

인터넷 공간

수많은 침해 시도가
끊임없이 발생되고 있는
매우 위험한 공간

정보보호시스템이
구비되지 않은 경우
해킹 공격, 내부자 위협 등
침해사고 위험에 상시 노출 상태

* 도둑에게 집에 들어오라고 문을 활짝 열어둔 격

I 정보보호시스템의 이해

1 정보보호시스템의 필요성

- **네트워크 정보보호시스템**
  - 사이버 공격이 들어오는 경계 또는 통로에서 침해 시도를 탐지하여 차단하기 위해 네트워크 정보보호시스템이 마련되어야 할 필요
- **호스트 정보보호시스템**
  - 네트워크 보호에 실패한 경우 호스트 자체에서 침해시도를 탐지하여 차단 가능
  - 호스트 보호에도 실패한 경우 호스트 정보보호시스템은 호스트를 신속히 격리하고 원인 규명을 지원 가능

2 네트워크 정보보호시스템

- **방화벽 (침입차단시스템)**
  - 네트워크 간 전송되는 패킷들을 정해진 규칙에 따라 통과시키거나 차단시켜,
    공격자로부터 내부 정보자산을 보호하기 위한 목적으로 사용되는 가장 기본적인 정보보호시스템
- **IDS (침입탐지시스템)**
  - 네트워크 간 전송되는 패킷을 수집하고 내용을 분석하여 침해 시도를 탐지하는 정보보호시스템
- **IPS (침입방지시스템)**
  - 네트워크 간 전송되는 패킷을 수집하고 내용을 분석하여 침해 시도를 탐지 · 차단하는 정보보호시스템

방화벽, IDPS는 각 해당 차시에서 자세하게 다룰 예정

2 네트워크 정보보호시스템

▪ 네트워크 접근통제 (Network Access Control, NAC)

내부에 위치한 컴퓨팅 장치의 **정보통신망 접근을 통제**하는 정보보호시스템

- 국가 · 공공에서 사용하는 공식 용어도 네트워크 접근통제

비인가 컴퓨팅 장치의 정보통신망 연결을 통제

- 등록되지 않은 MAC 주소를 가진 컴퓨팅 장치는 비인가 컴퓨팅 장치로 간주

예 개인 랩톱 PC, 개인 스마트폰, 개인 태블릿 PC 등

2 네트워크 정보보호시스템

▪ 네트워크 접근통제 (Network Access Control, NAC)

인가된 컴퓨팅 장치라 하더라도 **내부 보안 정책의 준수 여부**에 따라
정보통신망 연결을 허용하거나 통제

- ID와 비밀번호를 통해 실제 내부 사용자인지 아닌지 확인
- 각 PC에 에이전트(프로그램)를 설치하게 하고, 에이전트를 통해
  내부 보안 정책의 준수 여부를 확인

예 운영체제 비밀번호 설정 및 최신화 여부,화면보호기 설정 및 비밀번호 지정 여부,
최신 보안 업데이트 적용 여부 등

2 네트워크 정보보호시스템

▪ 웹 방화벽 (Web Application Firewall, WAF)

방화벽 (침입차단시스템)	네트워크 경계를 보호하거나 내부 통신을 통제하기 위한 목적으로 사용되므로, 응용 계층의 헤더(응용서비스 유형)까지만 확인
웹 방화벽	웹 응용프로그램에 대한 웹 해킹을 방어하기 위해 응용 계층의 본문 내용(메시지)까지 확인 • **주요 웹 해킹 유발 취약점** – 파일 업로드, 파일 다운로드, SQL 인젝션, 크로스 사이트 스크립팅(XSS) 등

웹 방화벽의 설치 위치

웹 응용프로그램이 탑재된 **웹 서버의 앞 단**에 구성

* 단, 웹 서버 내 설치하는 웹 방화벽(소프트웨어)의 경우 호스트 정보보호시스템으로 분류

2 네트워크 정보보호시스템

▪ 통합위협관리 (Unified Threat Management, UTM)

정보통신망의 규모가 큰 경우	정보통신망의 규모가 작은 중·소 조직
• 방화벽(침입차단시스템), IDPS(침입탐지/방지시스템), 웹 방화벽 등을 **별도 설치하여 운용**하는 것이 유리 * 각각의 정보보호시스템을 거치면서 트래픽이 필터링되는 효과가 있어 정보보호시스템의 가용성과 생존성 보장	• 개별 정보보호시스템을 도입하는 것이 **경제적으로 부담**이 될 수 있음 • 최근 정보통신 기술의 발전으로 컴퓨팅 능력이 증가되어 하나의 어플라이언스에 여러 기능을 통합하는 **UTM의 개념이 보편화** 예 UTM= 방화벽 + IDS/IPS + 웹 방화벽 + …

2 네트워크 정보보호시스템

- **무선침입방지 (Wireless Intrusion Prevention System, WIPS)**
  - 와이파이 등 무선 환경에서의 비인가 컴퓨팅 장치의 **정보통신망 접근을 통제**하는 정보보호시스템
    - 네트워크 접근통제(NAC)와 유사한 기능도 포함하지만, **무선 환경에 특화**된 기능 제공

IPS의 특성과 NAC의 특성 보유

- 조직 내 무선 AP에 대한 공격 **트래픽 차단**
- 조직 내 무선 AP에 연결을 시도하는 경우
  인가된 컴퓨팅 장치인지 여부와 **인가된 사용자인지 여부**를 확인
- 인가되지 않은 핫스팟/테더링 등 **비인가 무선 신호의 발생** 또는 **접속 차단(인증 해제)**

2 네트워크 정보보호시스템

▪ NDR (Network Detection and Response)

과거에는 정보통신 기술의 한계로 인해,
전통적인 네트워크 정보보호시스템은 **모든 트래픽을 보관하지 않는 형태**로 설계

- 즉, 탐지되거나 차단된 이벤트를 중심으로 보관하고, 이외의 이벤트는 보관하지 않는 방식

컴퓨팅 능력과 저장장치의 용량 증가 덕분에 **모든 트래픽을 장기간 보관**해두었다가 **심층 분석**할 수 있게 하는 NDR의 필요성 대두

- 탐지/차단되지 못한 이벤트라 하더라도 유의한 침해시도/침해사고였을 가능성 존재
- NDR은 모든 트래픽을 보관하고 재현하며 심층 분석할 수 있게 지원

한계점

- 모든 트래픽을 통째로 보관하기 때문에 **개인정보 논란**이 있을 수 있음
- **막대한 용량의 저장장치**가 필요함

3 호스트 정보보호시스템

- **안티 바이러스 (Anti-Virus, A/V)**
  - 컴퓨터 바이러스와 악성코드를 탐지하고 방어하는 호스트 기반 정보보호시스템

안티 바이러스는 해당 차시에서 자세하게 다룰 예정

Antivirus

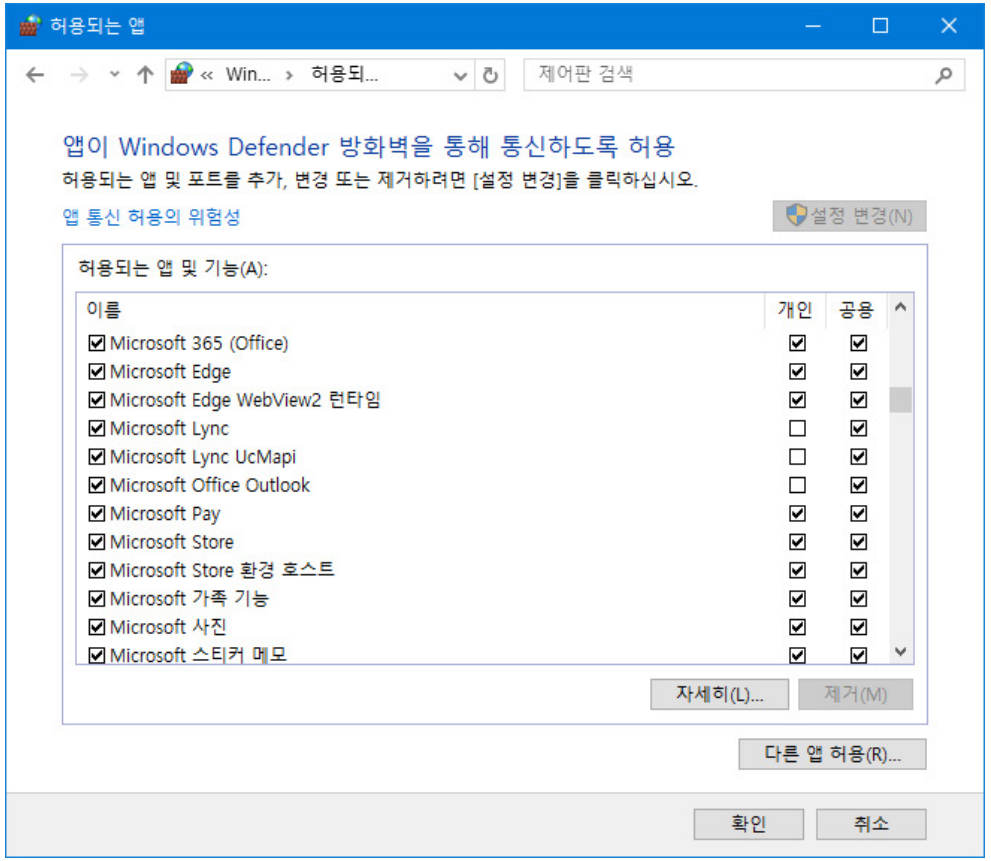
3 호스트 정보보호시스템

▪ 호스트 방화벽 (Host Firewall)

- 일반적으로 지칭하는 방화벽(침입차단시스템)은 네트워크 정보보호시스템으로, **네트워크 경계를 보호**하거나 **내부 통신을 통제하기 위한 목적**으로 사용되는 네트워크 방화벽을 의미
- 정보통신망 환경의 발달에 따라 현대적인 운영체제는 개별 호스트를 보호하기 위해 **호스트 방화벽 기능을 내장**하는 경향
  - 네트워크 방화벽과 유사한 방식으로 규칙을 지정/관리
- 일부 안티 바이러스는 **네트워크 보호의 일환**으로 호스트 방화벽 기능 제공

3 호스트 정보보호시스템

- **호스트 방화벽 (Host Firewall)**



Windows 방화벽 화면

3 호스트 정보보호시스템

- **자료유출방지 (Data Loss Prevention, DLP)**
  - 오늘날 내부자에 의한 정보유출 및 훼손 등 **내부자 위협(Insider Threat)이 증가**하고 있는 추세
    - 내부자 감시·통제가 중요한 정보수사기관 등 일부 조직에서는 정보보호 기능을 감사/감찰 기능에 통합하여 내부자 위협을 관리하기도 함

3 호스트 정보보호시스템

- **자료유출방지 (Data Loss Prevention, DLP)**
  - 내부 자료의 **외부 반출을 통제**하고, **자료/정보의 흐름을 모두 기록으로 보존**하여 감사/모니터링 지원

저장매체 통제 기능	USB, CD/DVD 등으로 파일을 복사할 때 **승인 절차를 요구**하는 기능
출력물 통제 기능	모니터 화면이나 프린터 출력 시 **워터마크를 표시**하며, 프린터 출력의 경우 **승인 절차를 요구**하는 기능
감사 기능	파일 이동/복사 및 출력 등의 **이벤트 발생 내역을 기록으로 보존**

3 호스트 정보보호시스템

- **디지털저작권관리 (Digital Rights Management, DRM)**

자료유출방지는 자료/정보의 흐름을 감시할 수 있으나, 이를 우회하여 유출된 자료/정보를 보호하기에는 **충분하지 않음**

디지털저작권관리 기술을 응용하면, 조직에서 생산되는 파일에 **디지털 서명**을 하고 **암호화** 함으로써 조직 외부로 자료/정보가 유출되더라도 열 수 없게 조치 가능

- 디지털저작권관리 기술은 당초 저작물을 관리하기 위해 고안된 기술
- 파일을 외부에 반출하기 위해서는 승인 절차를 통해 복호화 필요
  - 복호화 되지 않은 파일은 외부에서 열 수 없음

자료유출방지를 도입할 때 같이 도입함으로써 **상호 보완적**으로 활용하는 경향

3 호스트 정보보호시스템

- **EDR (Endpoint Detection and Response)**

NDR과 마찬가지로, 각 호스트에서 발생되는 **모든 이벤트를 실시간으로 모니터링**하며
수집 · 분석할 수 있는 EDR의 필요성 대두

- 안티 바이러스에서 진단하지 못하는 **신종 바이러스/악성코드**가 존재할 수 있고,
  이외에도 사용자가 **악의적인 목적으로 내부 정보를 유출**하는 등의 행위 가능성 존재
- 컴퓨터 운영체제 내 모든 이벤트와 네트워크 연결에 관한 정보를 모니터링

한계점

- 호스트 내 모든 이벤트를 통째로 보관하기 때문에 **개인정보 논란**이 있을 수 있음
- **막대한 용량의 저장장치**가 필요함

II

정보보호시스템 인증 · 평가 제도

II 정보보호시스템 인증 · 평가 제도

1 정보보호시스템 인증 · 평가의 필요성

- 정보보호시스템의 주 기능 : **보안**
- 국가안보에 영향을 미칠 수 있기 때문에 일정 수준 이상의 **보안 기능 품질이 담보**되어야 함

> 신뢰할 수 있는 평가기관을 통해 정보보호시스템의 **보안 기능 수준을 객관적으로 측정하고 보증**해야 할 필요

> 국가 · 공공 분야에 도입되는 정보보호시스템의 경우 **보안 기능 수준의 적합성을 보다 엄정하게 검증**하는 기준과 절차 필요

- 우리나라를 비롯한 각국에서는 **정보보호시스템의 성능과 보안 기능의 안전성 및 신뢰성 등을 평가 · 인증**하기 위한 제도를 마련하여 운영 중

2 우리나라의 정보보호시스템 인증 · 평가 제도

3 CC 평가 · 인증 (과학기술정보통신부)

- 정보보호시스템에 대한 **국제적인 신뢰도를 확보**하고 **경쟁력을 강화**하기 위해 **정보보호시스템의 안전성 및 신뢰성을 평가 · 인증**하는 제도

우리나라의 정보보호시스템(제품)	VS	**미국**의 정보보호시스템(제품)

- **국제적인 공통평가기준과 공통평가방법론**을 평가기준 및 평가방법론으로 적용

- 관련 근거
  - 지능정보화 기본법 제58조(정보보호시스템에 관한 기준 고시 등)
  - 지능정보화 기본법 시행령 제51조(정보보호시스템에 관한 기준 고시 등)
  - 정보보호시스템 공통평가기준(미래창조과학부)
  - 정보보호시스템 평가 · 인증 등에 관한 고시(과학기술정보통신부)
  - 정보보호제품 평가 · 인증 수행규정(과학기술정보통신부 · IT보안인증사무국)

3 CC 평가 · 인증 (과학기술정보통신부)

- 일반적인 CC 평가 · 인증은 **국제 CC인증**을 의미
  - 국제상호인정협정(Common Criteria Recognition Arrangement, CCRA) 회원국이 공통으로 사용하는 **공통평가기준**(Common Criteria, CC)과 **공통평가방법론**(Common Evaluation Methodology, CEM) 적용
- 우리나라는 휴전 국가로 전쟁 위험이 항상 상존하고 있다는 특성상 국제 CC를 준용하여 **우리나라에서만 적용되는 국내용 CC**를 별도 운영중

국내용 CC	
	• **국제 CC에 비해 간소화**되어 있어 국제 CC로는 인정 불가 – 국내용 CC인증을 받은 정보보호시스템(제품)의 수출을 위해서는 별도 국제 CC인증 필요 • **국가정보원이 인정한 국가용 보호 프로파일**(Protection Profile, PP)을 활용하게끔 강제되어 국내용 CC인증을 받은 경우 국가 · 공공용으로 도입 가능 – 국가용 PP를 준수하여 국제 CC인증을 받은 경우는 국가 · 공공용으로 도입 가능

3 CC 평가 · 인증 (과학기술정보통신부)

- **정책**기관 : 과학기술정보통신부

관련 법령 제·개정	**관련 제도** 수립	**관련 제도 예산** 확보

- **인증**기관 : 국가보안기술연구소(NSR)의 IT보안인증사무국(ITSCC)

평가결과 승인 및 인증서 발급	**평가기관 관리** 및 **CC인증 정책수립** 지원
발급 국제상호인정협정(CCRA)관련 국제 활동	제품 목록, 보호프로파일 등 **관련 자료 제공**

- **평가**기관 : 한국인터넷진흥원(KISA) 등 7개 기관(업체)

한국인정기구(KOLAS)에서 승인한 **공인시험기관 품질메뉴얼**에 따른 평가기관 운영	제출물 조사 및 시험 · 취약성 분석 등 **제품 평가**
평가자 교육 훈련	신청기관 개발환경 **보안점검**

4 정보보호제품 성능평가 (과학기술정보통신부)

- 정보보호시스템이 운영환경에서 **네트워크 트래픽에 얼마나 적절히 대응**하는지 성능을 평가하여 결과를 제공하는 제도
- 안전성이나 신뢰성 등 보안성을 고려하는 것이 아닌 **성능 위주의 지표를 고려**

  예 분당 처리할 수 있는 **네트워크 트래픽이 어느 정도**인가,
  단시간에 들어오는 **네트워크 트래픽을 얼마나 감당**할 수 있는가 등

- 관련 근거
  - 정보보호산업의 진흥에 관한 법률 제17조(성능평가 지원)
  - 정보보호산업의 진흥에 관한 법률 시행령 제10조(성능평가의 방법 및 성능평가기관의 지정)

정보보호시스템 인증 · 평가 제도

4 정보보호제품 성능평가 (과학기술정보통신부)

- **정책**기관 : 과학기술정보통신부

법·제도 개선 및 정책 결정	**성능평가기관** 지정 및 취소

- **심의·관리**기관 : 한국인터넷진흥원(KISA)

성능평가기관 관리	**성능평가자** 양성 및 자격 관리	**기술심의위원회** 운영

* 성능평가의 세부기준 및 결과 등을 심의·의결

- **성능평가**기관 : 한국정보통신협회(TTA) 등 5개 기관(업체)

성능평가 수행

5 보안 기능 시험 (국가정보원)

- CC 평가 · 인증은 국제적인 공통평가기준과 공통평가방법론을 적용하고 있는 만큼 **안전성과 신뢰성이 담보**
- **하지만 많은 시간과 비용이 투입**되는 한계점도 존재

  예 국외 수출을 하지 않고 **국가 · 공공 분야에 납품하기 위한 목적 만**으로 국내용 CC 평가·인증을 받는 것은 과도한 노력 투입 가능성

- 보안 기능 시험 제도는 정보보호시스템, 네트워크장비, 양자암호통신장비 등 **보안 기능이 탑재된 IT제품에 대한 국가용 보안요구사항 만족 여부를 시험하여 안전성을 확인**하는 제도
- 관련 근거
  - 전자정부법 제56조(정보통신망 등의 보안대책 수립·시행)
  - 사이버안보 업무규정 제9조(사이버공격·위협 예방 조치 등)
  - 국가 정보보안 기본지침 제19조의2(보안 기능 시험)

정보보호시스템 인증 · 평가 제도

5 보안 기능 시험 (국가정보원)

- **정책**기관 : 국가정보원

보안 기능 시험 관련 제도·정책 총괄	**검증기준 승인 및 시험성적서** 발급대상 제품 보정	**시험결과서** 현황 관리

- **검증**기관 : 국가보안기술연구소

검증기준 작성 및 검토	**보안 기능 시험결과서** 검토

- **공인시험**기관 : 한국정보통신협회(TTA) 등 6개 기관(업체)

보안 기능 시험 수행

6 보안적합성 검증 (국가정보원)

- 국가 · 공공 분야에 도입되는 정보보호시스템, 네트워크장비, 양자암호통신장비 등 **보안기능이 탑재된 IT제품의 안전성을 검증**하는 제도
  - 디지털 복합기에 탑재되는 저장자료 완전 삭제 제품 포함
- **CC 평가 · 인증**(국내용 CC, 국가용 PP를 준수하여 받은 국제 CC)을 받았거나 **보안 기능 시험을 통과한 검증필 제품**은 검증절차 생략(간소화) 가능
- 국방 분야는 **국방부 장관에게 위탁**(위임) 하고 있어 국군방첩사령부에서 **軍** 보안적합성 검증 업무 통제
- 관련 근거
  - 전자정부법 제56조(정보통신망 등의 보안대책 수립·시행)
  - 사이버안보 업무규정 제9조(사이버공격·위협 예방 조치 등)
  - 국가 정보보안 기본지침 제20조의(정보통신제품 도입), 제5절(보안적합성 검증)

6 보안적합성 검증 (국가정보원)

- **국가 · 공공 분야**

정책기관	검증 · 시험기관
국가정보원	국가보안기술연구소

- **국방 분야 위임 (軍 보안적합성 검증)**

정책기관	검증기관	시험기관
국방정보본부	국군방첩사령부	국군방첩사령부 정보보호단 (정보보호인증센터)

7 암호모듈 검증 (국가정보원)

- 비밀이 아닌 **비공개 업무자료를 보호**하기 위해 국가 · 공공 분야에서 도입하는 **상용 암호모듈의 안전성과 구현 적합성을 검증**하는 제도
  - 비밀(국가비밀, 군사비밀)은 국가용 보안시스템(암호장비)만 적용 가능
- 1995년 미국과 캐나다가 공동으로 개발한 **암호모듈 검증 제도**(Cryptographic Module Validation Program, CMVP)를 벤치마킹하여 **우리나라의 실정에 부합되도록 구성**한 제도
  - 단, 우리나라의 암호모듈 검증 제도와 CMVP는 상호 호환되지 않음
- 관련 근거
  - 전자정부법 시행령 제69조(전자문서의 보관·유통 관련 보안조치)
  - 사이버안보 업무규정 제9조(사이버공격·위협 예방 조치 등)
  - 국가 정보보안 기본지침 제65조(대외비의 전자적 처리), 제66절(비공개 업무자료 처리)

7 암호모듈 검증 (국가정보원)

- **국가 · 공공 분야**

정책기관	검증 · 시험기관
국가정보원	국가보안기술연구소, 한국인터넷진흥원(KISA)

- **국방 분야 추가 검증 제도 (상용암호모듈 보안적합성 검증)**
  - 국방정보시스템 및 무기체계의 경우 검증필 암호모듈을 적절한 방식으로 적용했는지 여부를 추가로 확인

정책기관	검증기관	시험기관
국방정보본부	국군방첩사령부	국군방첩사령부 정보보호단 (암호보호지원센터)

8 인증 · 평가 제도에 따른 정보보호시스템 분류

- **CC 평가 · 인증에 따른 분류**

침입차단시스템(FW)	침입방지시스템(IPS)	네트워크 접근통제
무선랜 인증	무선침입방지	문서 암호화
서버 접근통제	스마트카드	스마트폰 보안관리
웹 방화벽	자료유출방지	통합보안관리
통합인증	DB 암호화	DB 접근통제
VoIP 방화벽	VPN	

8 인증 · 평가 제도에 따른 정보보호시스템 분류

- **보안적합성 검증 및 보안 기능 시험 제도에 따른 분류**

침입차단 제품군

- 침입차단시스템(FW)
- 웹 방화벽(WAF)
- DDoS 대응장비
- 인터넷전화 보안제품 등

침입방지 제품군

- 침입방지시스템(IPS·IDS)
- 무선침입방지제품(WIPS) 등

구간보안 제품군

- 가상사설망(VPN)
- 네트워크 접근통제제품(NAC)
- 망간 자료전송제품
- 무선랜 인증제품
- 구간 암호화제품 등

8 인증 · 평가 제도에 따른 정보보호시스템 분류

- **보안적합성 검증 및 보안 기능 시험 제도에 따른 분류**

전송자료보안 제품군	보안관리 제품군		가상화 제품군
• 스팸메일 차단시스템	• 스마트카드(COS 포함)	• DB 접근통제제품	• 가상화 관리제품 등
• 소프트웨어 기반 보안USB제품	• 통합보안 관리제품	• 시스템 접근관리제품	
• 호스트 자료유출방지 제품	• (ESM, UTM, 통합로그관리)	• 패스워드 관리제품	
• 네트워크 자료유출방지 제품	• 소스코드 보안약점 분석도구	• 통합인증제품(SSO) 등	
• 메일 암호화제품 등	• 패치관리시스템		

8 인증 · 평가 제도에 따른 정보보호시스템 분류

- **보안적합성 검증 및 보안 기능 시험 제도에 따른 분류**

엔드포인트 보안제품군

- 디지털 복합기
- 안티바이러스제품 (Windows/Linux)
- 스마트폰 보안관리제품
- 운영체제(서버) 접근통제제품
- EDR제품
- APT대응제품
- 문서암호화제품(DRM)
- DB 암호화제품 등

저장자료 완전삭제 제품군

- 저장자료 완전삭제 제품(SSD 제외)

III

방화벽 (침입차단시스템)

방화벽 (침입차단시스템)

1 방화벽 (Firewall)

방화벽

네트워크 간 전송되는 패킷들을 정해진 규칙에 따라 통과시키거나 차단시켜,
공격자로부터 내부 정보자산을 보호하기 위한 목적으로 사용되는 가장 기본적인 정보보호시스템

- 국가·공공에서 사용하는 공식 용어는 침입차단시스템
- 네트워크 경계를 보호하거나 내부 통신을 통제하기 위한 목적으로 사용

패킷 필터링 기능

IP 주소와 포트 번호를 토대로 패킷을 허용하거나 차단하는 기능

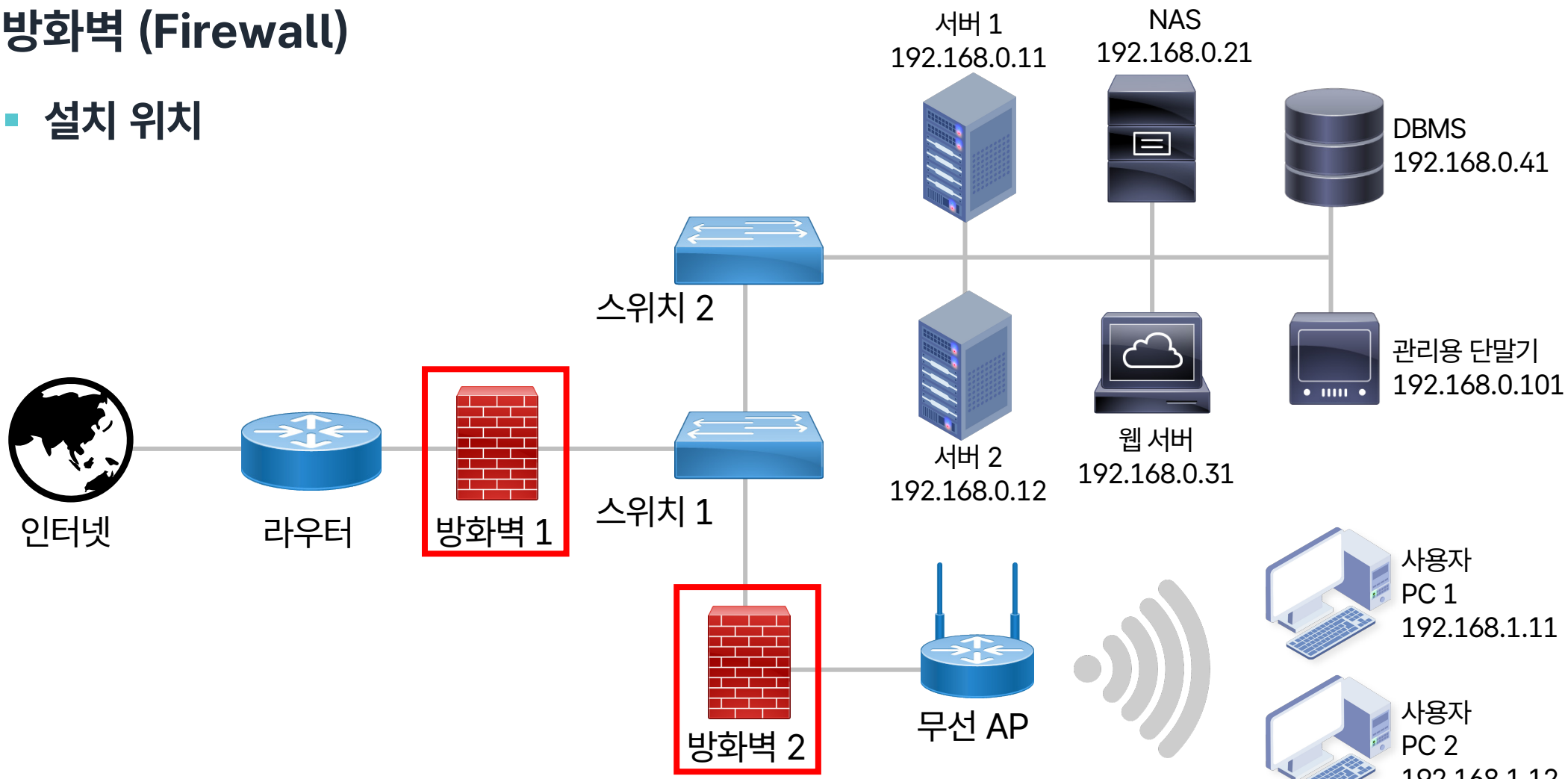
상태기반 패킷 검사 기능

프로토콜 및 TCP 연결 상태 정보 등을 이용하여 패킷을 허용하거나 차단하는 기능

방화벽 (침입차단시스템)

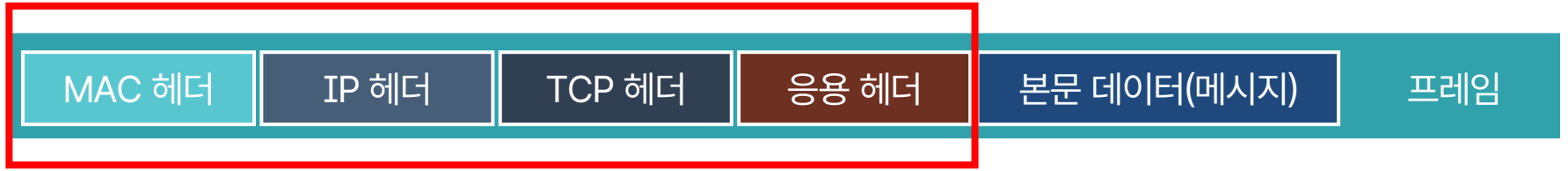
1 방화벽 (Firewall)

- 설치 위치

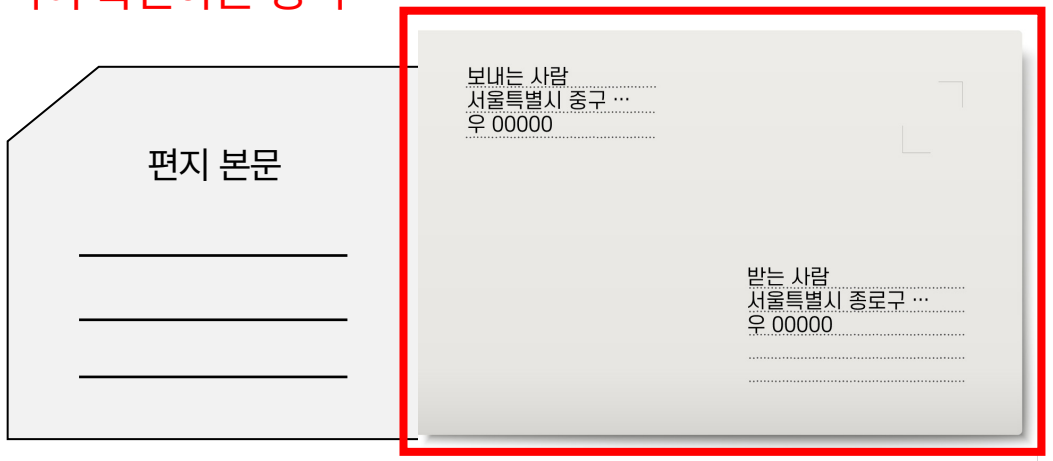


1 방화벽 (Firewall)

- **특성**
  - 방화벽은 1980년대부터 존재했던 **전통적인 정보보호시스템**
  - 빠른 탐지 · 차단 처리를 위해 **헤더만 확인**



방화벽이 확인하는 영역



2 방화벽 정책 · 규칙의 이해

- 방화벽은 기본적으로 **화이트리스트 방식**으로 동작하는 정보보호체계

블랙리스트 방식	기본적으로 **모두 허용(allow)하고 차단(deny)**할 것들만 규칙에 등록
화이트리스트 방식	기본적으로 **모두 차단(deny)하고 허용(allow)**할 것들만 규칙에 등록

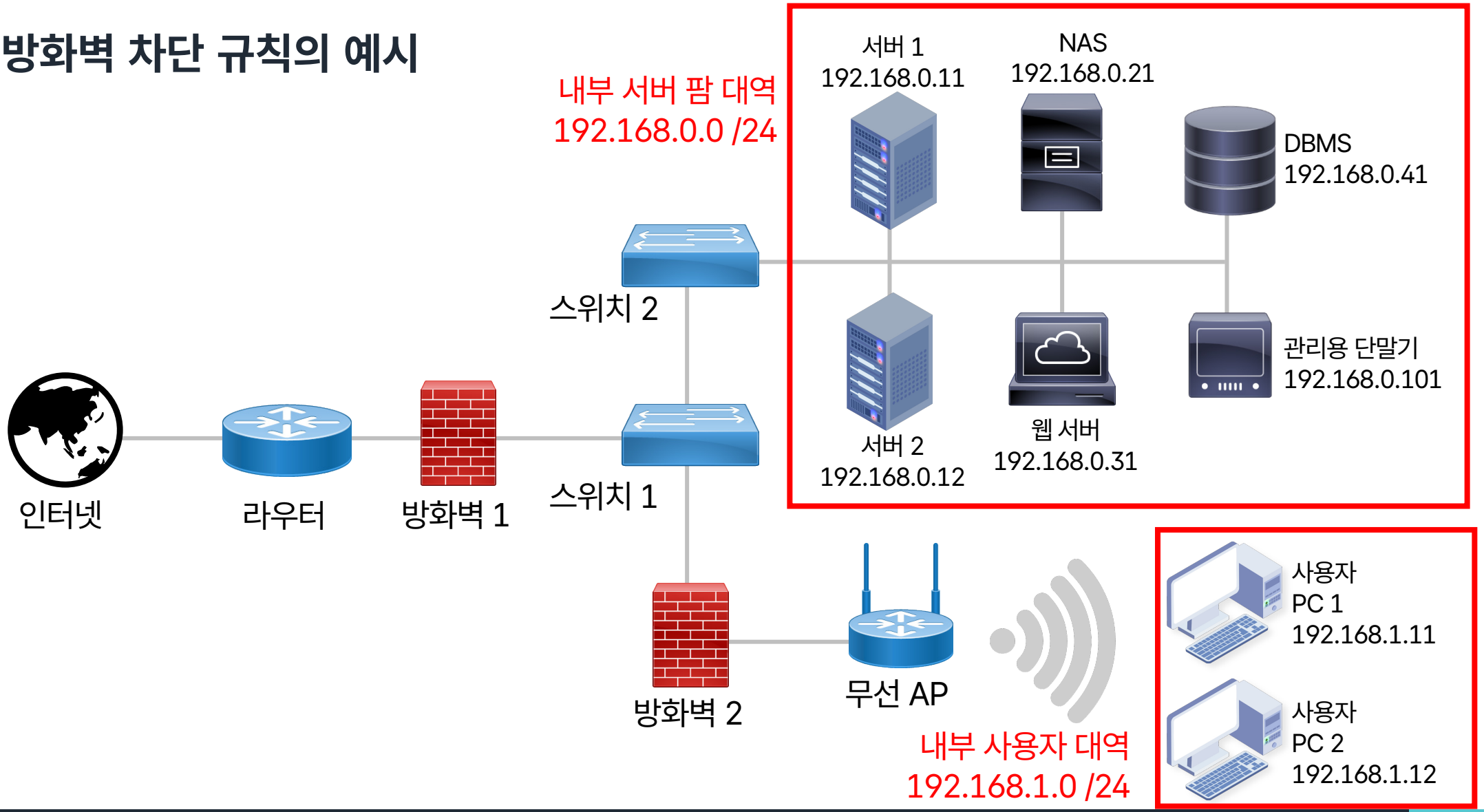
- **탐지 규칙의 우선 순위에 따라 검사**하여 적용(차단) 여부를 결정
- 조직에서 정한 정책에 따라 블랙리스트 방식으로도 운용 가능

2 방화벽 정책 · 규칙의 이해

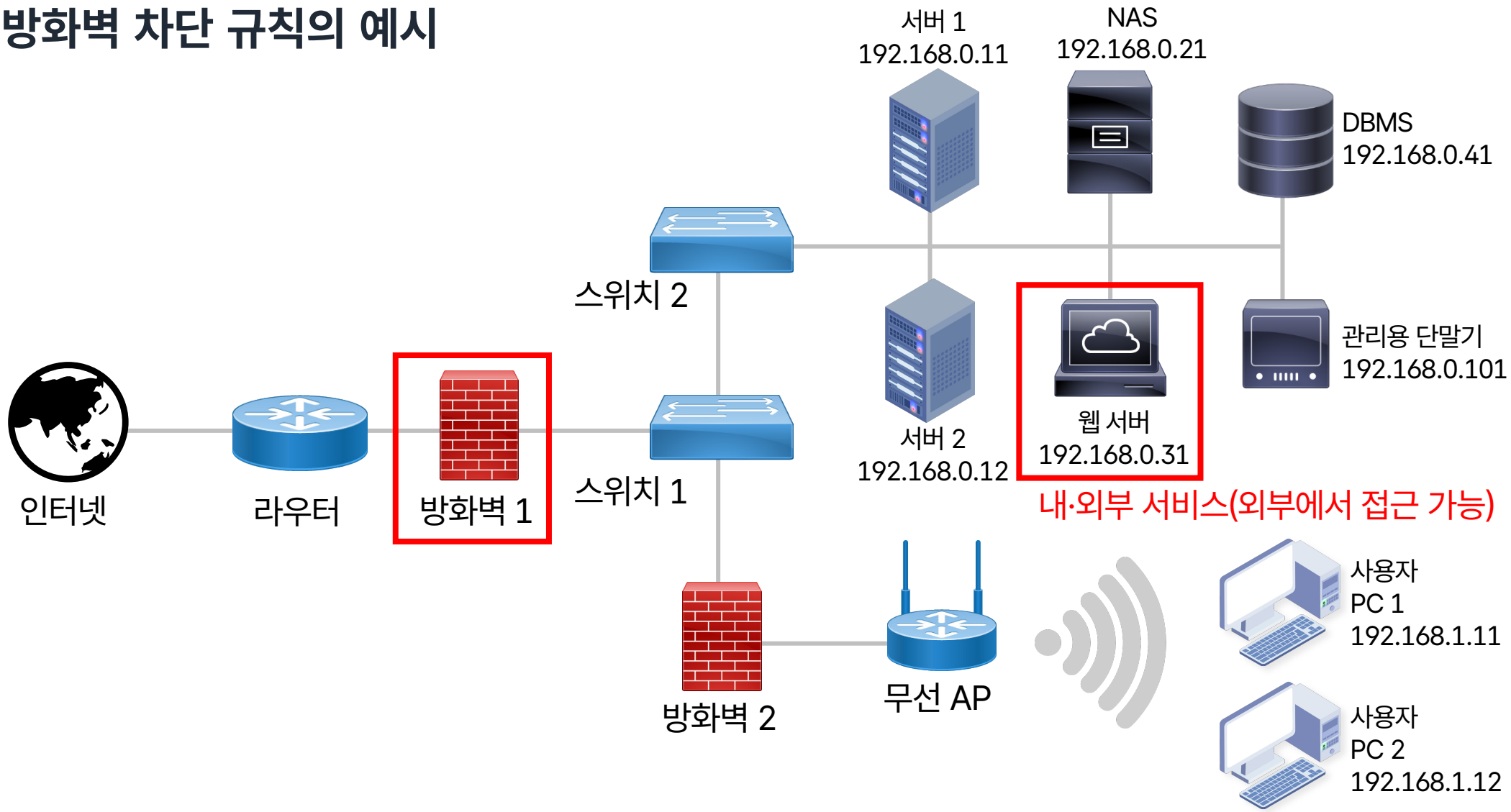
- 방화벽의 **차단 규칙을 잘못 구성**하는 경우
  - 모든 트래픽이 허용되어 악성 트래픽이 유입될 가능성
  - 모든 트래픽이 차단되어 어떠한 통신도 불가할 가능성

- 방화벽을 비롯한 모든 정보보호체계의 규칙은 **조직 내 보안운영 정책 관리 프로세스에 따라 등록 · 변경 · 삭제**
  - 기술적인 측면으로만 접근하면 규칙이 중구난방이 될 가능성

3 방화벽 차단 규칙의 예시



3 방화벽 차단 규칙의 예시



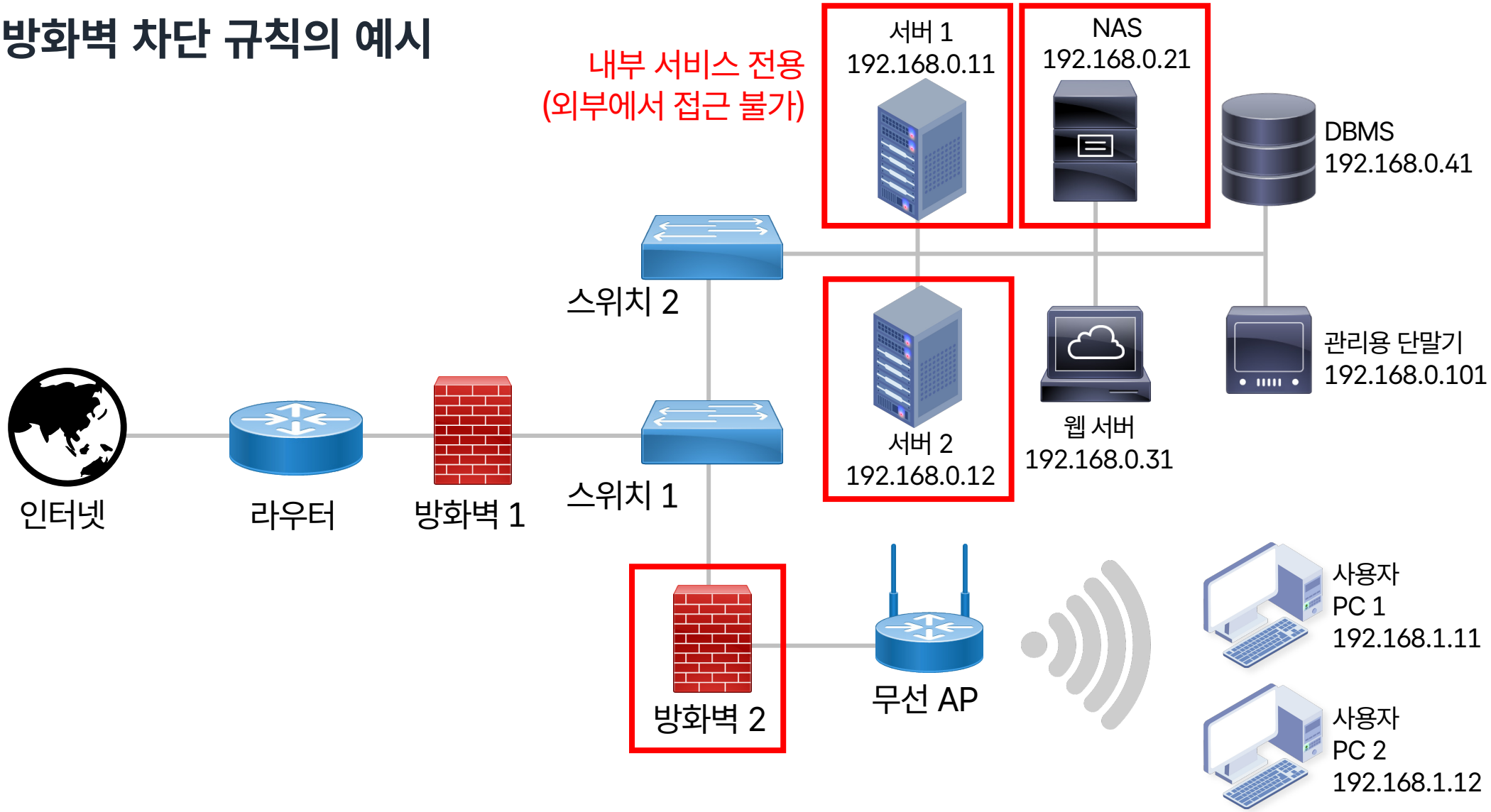
3 방화벽 차단 규칙의 예시

- **방화벽 1**

	출발지 IP	출발지 포트	목적지 IP (자산명)	목적지 포트	동작
1	ANY	ANY	192.168.0.31(웹 서버)	80, 443	허용(allow)
All Deny (화이트리스트)					

방화벽 (침입차단시스템)

3 방화벽 차단 규칙의 예시

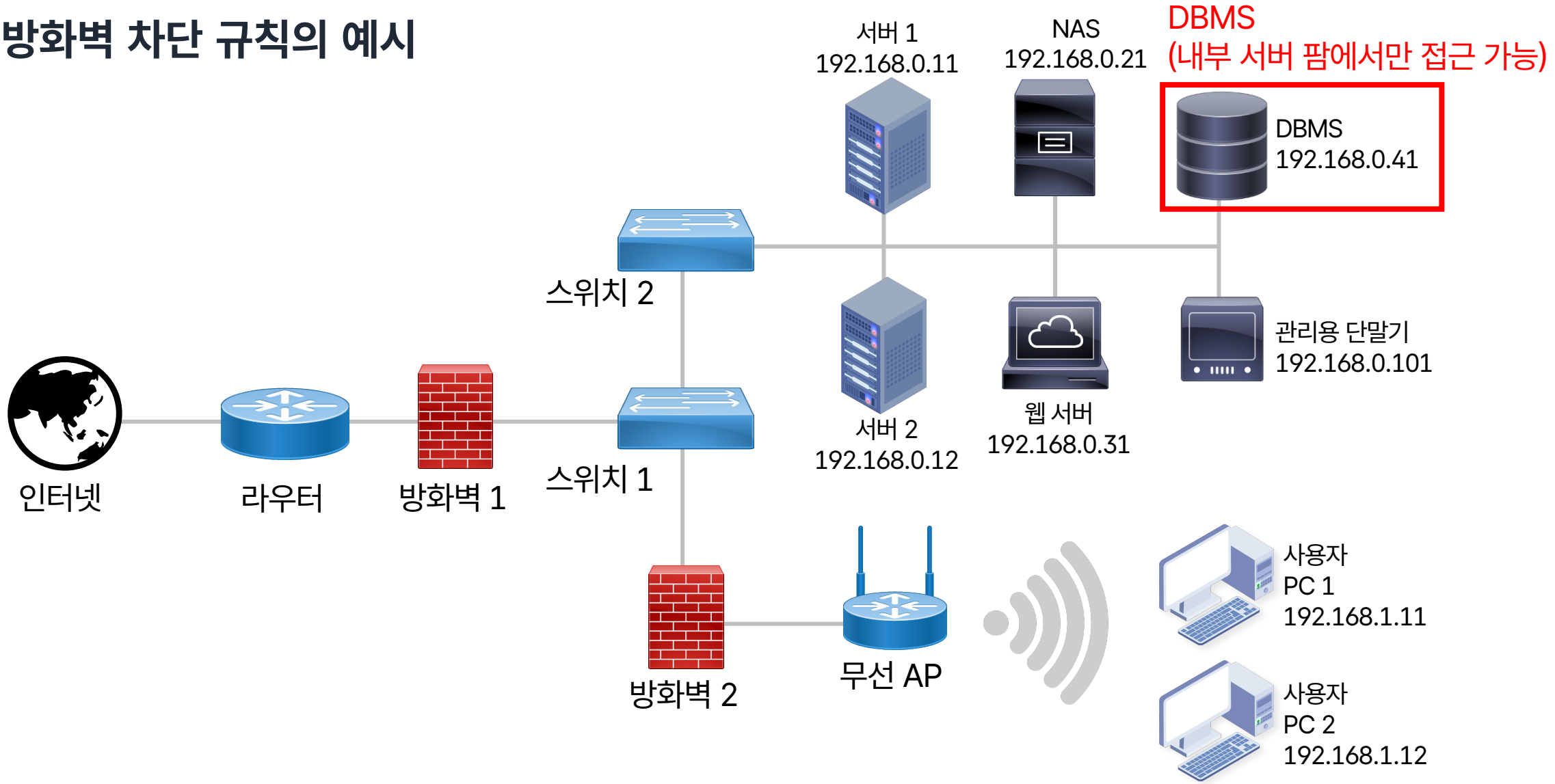


3 방화벽 차단 규칙의 예시

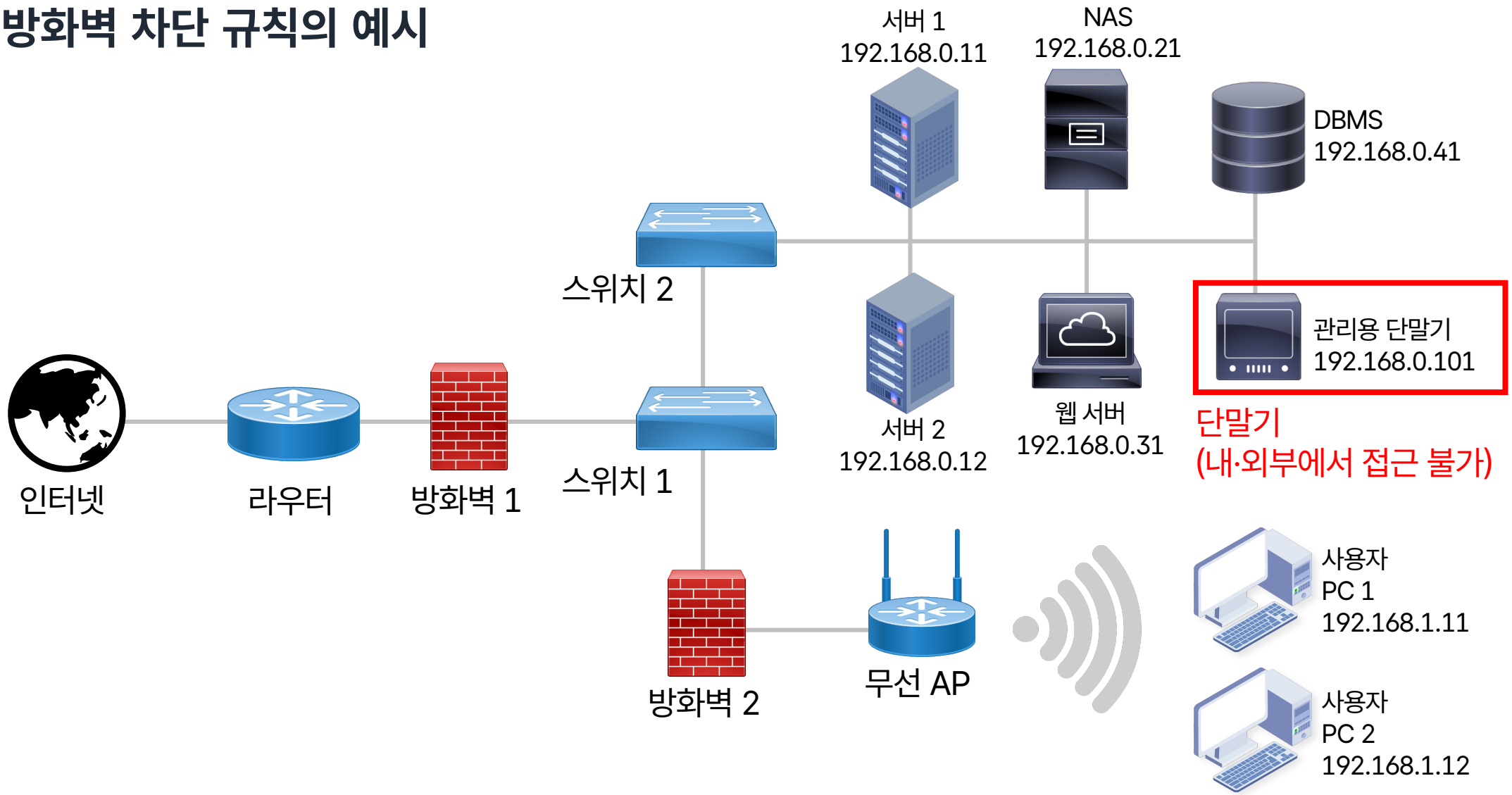
- **방화벽 2**

	출발지 IP	출발지 포트	목적지 IP (자산명)	목적지 포트	동작
1	192.168.1.0 /24	ANY	192.168.0.11(서버 1)	23	허용(allow)
2	192.168.1.0 /24	ANY	192.168.0.12(서버 2)	25, 110, 143	허용(allow)
3	192.168.1.0 /24	ANY	192.168.0.21(서버 3)	137, 138, 139, 445, 548	허용(allow)
All Deny (화이트리스트)					

3 방화벽 차단 규칙의 예시



3 방화벽 차단 규칙의 예시



4 방화벽 차단 규칙 구성 시 주의사항

모두 허용
(All Any)
규칙 금지

방화벽이 없는 것과
다름없는 효과

과도한 허용
(Any)
규칙 지양

특정 IP 또는 대역으로
허용 범위 한정

테스트용
임시 등록 규칙
테스트 종료 시
삭제

테스트 목적과 유효기간
명시

실효성 없는
장기 미사용
규칙 삭제

불필요한
중복 규칙
삭제

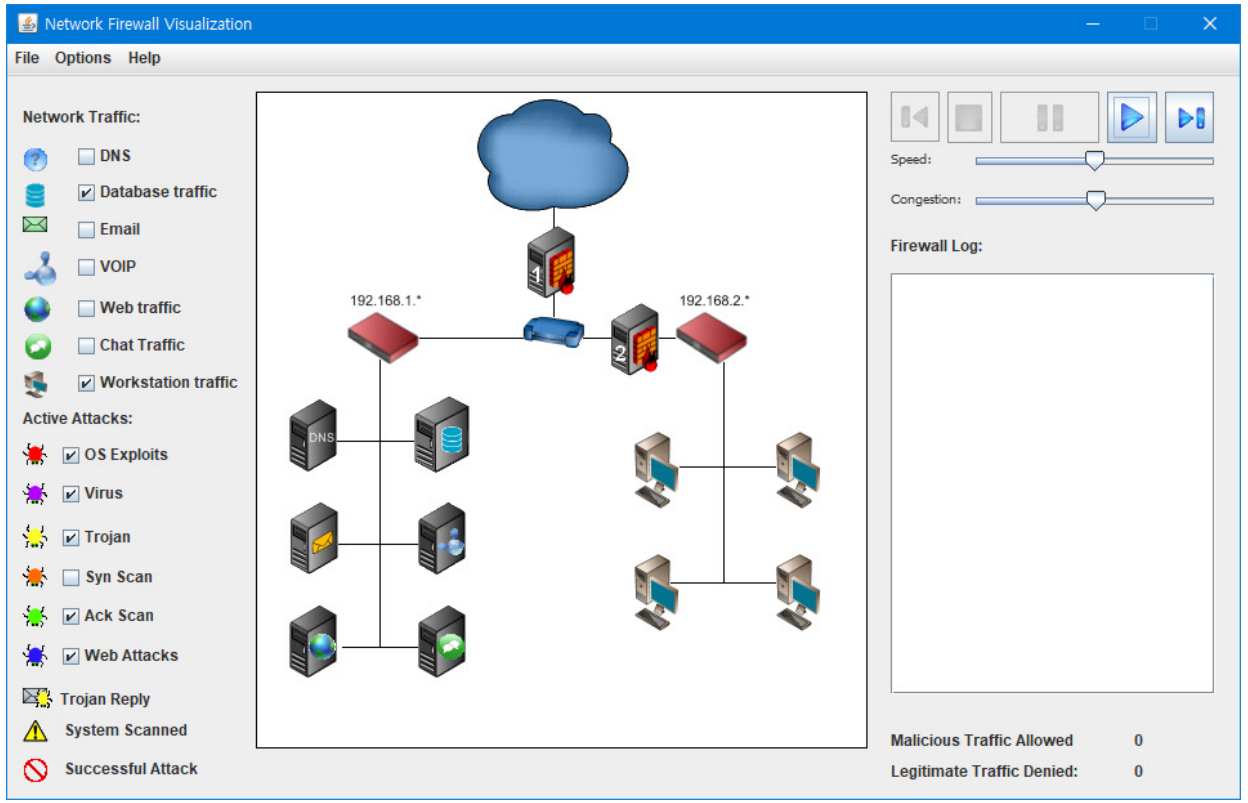
IV

방화벽 정책 · 규칙 작성

IV 방화벽 정책 · 규칙 작성

1 실습 도구 안내

- **Network Firewall Visualization**
  - 미 공군사관학교 소속 중위들이 2010년 개발하여 공개한 교육용 실습 도구
  - 네트워크 구성도와 애니메이션 효과를 통해 직관적인 사용자 환경 제공
  - 방화벽에 차단 규칙을 직접 등록하고 시뮬레이션 해봄으로써 규칙의 효과성을 확인할 수 있도록 구성



출처 Justin Warner, David Musielewicz, G. Parks Masters, Taylor Verett, Robert Winchester, and Steven Fulton. 2010. Network firewall visualization in the classroom. J. Comput. Sci. Coll. 26, 2 (December 2010), pp. 88–96.

2 실습

- **Network Firewall Visualization**

요약 정리

- 지금까지 학습한 내용을 정리해보겠습니다.

요약정리

정보보호시스템의 이해

정보보호시스템

- 정보보호제품이라고도 하며, 정보의 접근제어 · 통제 등을 위한 보안 기능을 주 기능으로 하는 어플라이언스 또는 소프트웨어
  - 사이버 공격 및 침해 시도를 탐지하거나 차단하고 관련된 내용을 보안 정보 및 이벤트 기록으로 보관

정보보호시스템의 필요성

- **네트워크 정보보호시스템 :** 사이버 공격이 들어오는 경계 또는 통로에서 침해시도를 탐지 · 차단
  - 방화벽(침입차단시스템), IDPS(침입탐지/방지시스템), NAC(네트워크접근통제), 웹 방화벽(WAF), 통합위협관리(UTM), 무선침입방지(WIPS), NDR 등
- **호스트 정보보호시스템 :** 네트워크 보호에 실패한 경우 호스트 자체에서 침해시도를 탐지하여 차단하거나, 침해사고 발생 시 호스트를 신속히 격리하고 원인 규명을 지원
  - 안티 바이러스(A/V), 호스트 방화벽, 자료유출방지(DLP), 디지털저작권관리(DRM), EDR 등

정보보호시스템 인증 · 평가 제도

- **필요성**
  - 정보보호체계는 보안 기능을 주 기능으로 하는 만큼 국가안보에 영향을 미칠 수 있기 때문에 일정 수준 이상의 보안 기능 품질이 담보되어야 하는 만큼 신뢰할 수 있는 평가기관을 통해 정보보호체계의 보안 기능 수준을 객관적으로 측정하고 보증해야 할 필요
  - 우리나라를 비롯한 각 국에서는 정보보호체계의 성능과 보안 기능의 안전성 및 신뢰성 등을 인증 · 평가하기 위한 제도를 마련하여 운영 중
- **과학기술정보통신부 소관 인증 · 평가**
  - CC 평가 · 인증 (과학기술정보통신부), 정보보호제품 성능평가 (과학기술정보통신부)
- **국가정보원 소관 인증 · 평가**
  - 보안기능 시험 (국가정보원), 보안적합성 검증 (국가정보원), 암호모듈 검증 (국가정보원)
    * 단, 국방 분야의 경우 위임에 따라 軍 보안적합성 검증과 상용암호모듈 보안적합성 검증 별도 시행 중

요약정리

- **방화벽(침입차단시스템)**
  - **네트워크 경계를 보호하거나 내부 통신을 통제하기 위한 목적으로 사용되는 가장 기본적인 정보보호 시스템**
    - 패킷 필터링 기능 : IP 주소와 포트 번호를 토대로 패킷을 허용/차단하는 기능
    - 상태기반 패킷 검사 기능 : 프로토콜 및 TCP 연결 상태 정보 등을 이용하여 패킷을 허용/차단하는 기능
  - **특성**
    - 방화벽은 1980년대부터 존재했던 전통적인 정보보호체계로, 빠른 탐지/차단 처리를 위해 헤더만 확인
  - **정책 · 규칙의 이해**
    - 방화벽은 기본적으로 화이트리스트 방식으로 동작하며 규칙의 우선 순위에 따라 검사 · 적용(차단) 여부 결정
      - 블랙리스트 방식 : 기본적으로 모두 허용(allow)하고 차단(deny)할 것들만 규칙에 등록
      - 화이트리스트 방식 : 기본적으로 모두 차단(deny)하고 허용(allow)할 것들만 규칙에 등록
    - 모든 정보보호시스템의 정책 · 규칙은 조직 내 보안운영 정책 관리 프로세스에 따라 등록/변경/삭제

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
- 지역 기업 사이버 보안 '취약'…투자계획도 없어, KBS(2023.09.07), https://www.youtube.com/watch?v=_teCTriqgjM
- Justin Warner, David Musielewicz, G. Parks Masters, Taylor Verett, Robert Winchester, and Steven Fulton. 2010. Network firewall visualization in the classroom. J. Comput. Sci. Coll. 26, 2 (December 2010), p. 88–96

수고하셨습니다