Chapter 12
보안 솔루션

목차

01 Firewall
개념

사전적 의미

다른 곳으로 불이 번지지 않게 차단하는 벽

정보보안에서의 방화벽

외부 네트워크에서 내부 네트워크로 유입되는 침입을 사전 정책에 따라 차단하는 하드웨어/소프트웨어 주체

01 Firewall

접근제어

● 외부에서 내부 방향으로 접근하는 것을 규칙 집합(Rule Set)에 따라 허용/차단

번호	출발지		목적지		정책
	IP Addr.	Port Addr.	IP Addr.	Port Addr.	
0(default)	Any	Any	Any	Any	Deny
1	Any	Any	192.168.0.0~ 192.168.255. 255	80	Allow

01 Firewall

로그와 감사증적

감사로그

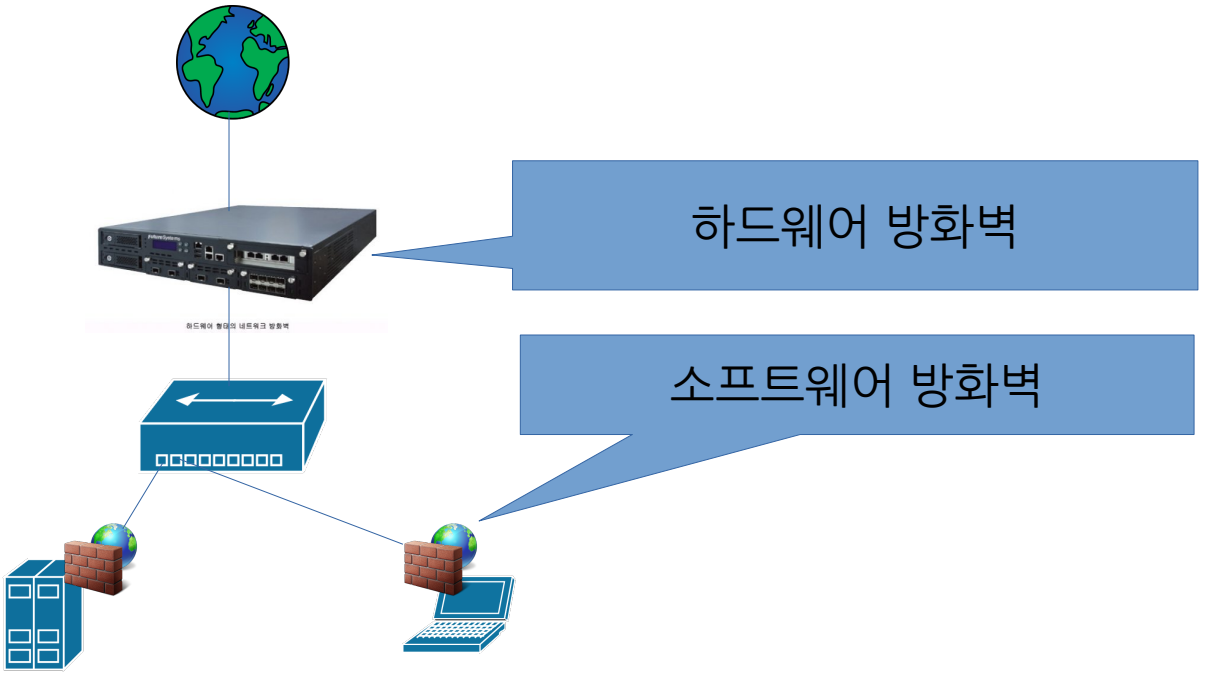
방화벽 정책 변경, 조작에 관한 로그
-감사 증적(Audit Trail), 감사 추적이라고도 불림
-책임 추적에 사용됨

운영로그

정책에 따라 허용/차단된 패킷의 정보
-공격 시도를 발견하는데 사용됨

01 Firewall

H/W방화벽, S/W방화벽



01 Firewall

H/W방화벽, S/W방화벽

구분	특징
하드웨어 방화벽	성능이 우수함 보안 정책 변경 사항을 중앙에서 한번에 제어할 수 있음 장비의 비용이 비교적 고가임 네트워크 단위의 보호
소프트웨어 방화벽	외부에 출장가는 경우에 대해서도 적용할 수 있음 사내 네트워크 내부에서 시도하는 침입에 대해서도 차단 가능 호스트 단위의 보호

01 Firewall

운영체제 내장 방화벽

Microsoft Windows

→Windows 방화벽

GNU/Linux

→

Iptables,
Firewalld,
nftables,
UFW,
etc..

MAC OS

→방화벽

02 IDS, IPS
개념

IDS

Intrusion Detection System, 침입 탐지 시스템
- -NIDS(Network-based Intrusion Detection System)
- -HIDS(Host-based Intrusion Detection System)

IPS

Intrusion Prevention System, 침입 방지 시스템
- -NIPS(Network-based Intrusion Prevention System)
- -HIPS(Host-based Intrusion Prevention System)

02 IDS, IPS

Intrusion Detection System

IDS

보다 상세한 분석(오용 탐지, 이상 탐지)을 통해 침입을 탐지, 기록 하거나 알리는 시스템

IDS가 탐지 가능한 공격의 예

구분	내용
스캐닝	시스템 상태와 취약점을 찾고자 여러 가지 종류의 패킷을 보내고 그에 대한 응답을 수집하는 수동적 공격 · 능동적 공격의 전초 단계 · 내부 네트워크의 구조, 각 서버의 운영체제 및 설치 소프트웨어 등의 정보 취득이 목적
DoS 공격	가용성을 해치고자 보내는 일련의 공격 (DoS, DdoS, Worm)
침투 공격	허가받지 않은 방법을 동원하여 시스템 자원과 권한 획득으로 데이터 변조 시도(Buffer overflow)

02 IDS, IPS

IDS 동작원리

02 IDS, IPS

IDS 동작원리(데이터 수집)

정의

분석 및 탐지에 사용될 원본 데이터들을 수집하는 단계

설명

교재에서는 Mirroring기법을 설명
네트워크(스위치)를 타고 돌아다니는 패킷을 수집
-Sniffing도 일종의 미러링 기법
-(교재에서는 스위치의 Monitor 포트를 예시로 들음)

IDS, IPS

02

IDS 동작원리(데이터 정제)

정의

분석의 효율을 위해 분석에 필요 없는 것으로 판단되는 데이터를 Filtering하고 Re-duction하는 과정

설명

데이터 축약에 통계적/수학적 기법을 적용할 수 있음

Clipping Level

-데이터를 저장할 수준(Threshold)

-단순 오류인지 공격인지 판단할 임계 수준

클리핑 레벨	장점	단점
높음	로그의 양이 줄어듬	중요 정보가 유실될 가능성이 높음
낮음	중요 정보가 유실될 가능성이 낮음	로그의 양이 많아짐

02 IDS, IPS

IDS 동작원리(분석과 탐지)

오용탐지

Misuse Detection
미리 정의된 침입 패턴, 시그니처가 발견되는지 확인

이상탐지

Anomaly Detection
정상, 평균을 범주를 크게(임계치 기준) 벗어났는지 확인

02 IDS, IPS

IDS 동작원리(분석과 탐지)

		Actual (실제)	
		Positive(양성)	Negative(음성)
Predicted (예측)	Positive(양성)	True Positive (Positive로 예측했는데 맞음)	False Positive (Positive로 예측했는데 틀림) (1종 오류)
	Negative(음성)	False Negative (Negative로 예측했는데 틀림) (2종 오류)	True Negative (Negative로 예측했는데 맞음)

IDS, IPS

02 IDS 동작원리(분석과 탐지)

	오용 탐지	이상 탐지
탐지 방법	패턴 매칭(Pattern Matching) 시그니처 기반 지식 기반	임계치 초과 통계 기반 행위 기반
	전문가 시스템	인공지능
장점	오탐률 낮음	새로운 공격 탐지 가능
단점	새로운 공격 탐지 불가능(시그니처가 있는 공격만 탐지 가능) 시그니처 업데이트 필요	오탐률 높음 임계치 설정이 어려움

이상 탐지는 오탐률이 높아 현장에서는 잘 사용되지 않지만, 아직 패턴을 알 수 없는 0-day 공격은 이상 탐지가 효과를 발휘하기에 보완적 탐지 기법으로 여전히 사용.

빅데이터 기반의 머신러닝이 비약적으로 발전함에 따라 이상 탐지의 중요성이 증가되고 있음

02 IDS, IPS

IDS 동작원리(결과 리포트)

정의

분석과 탐지 과정에서 발견한 정보들을 관리자에게 전달하는 단계
- -팝업, 메일, 문자
- -SNMP Trap(Simple Network Management Protocol, Trap)

설명

관리자는 이 리포트를 확인하고 적절한 대응 조치 가능
- -공격자에 대한 접근통제
- -공격받은 서비스 중지
- -책임 추적성 기능을 제공
  - -Transaction History를 보고 행위자 추적

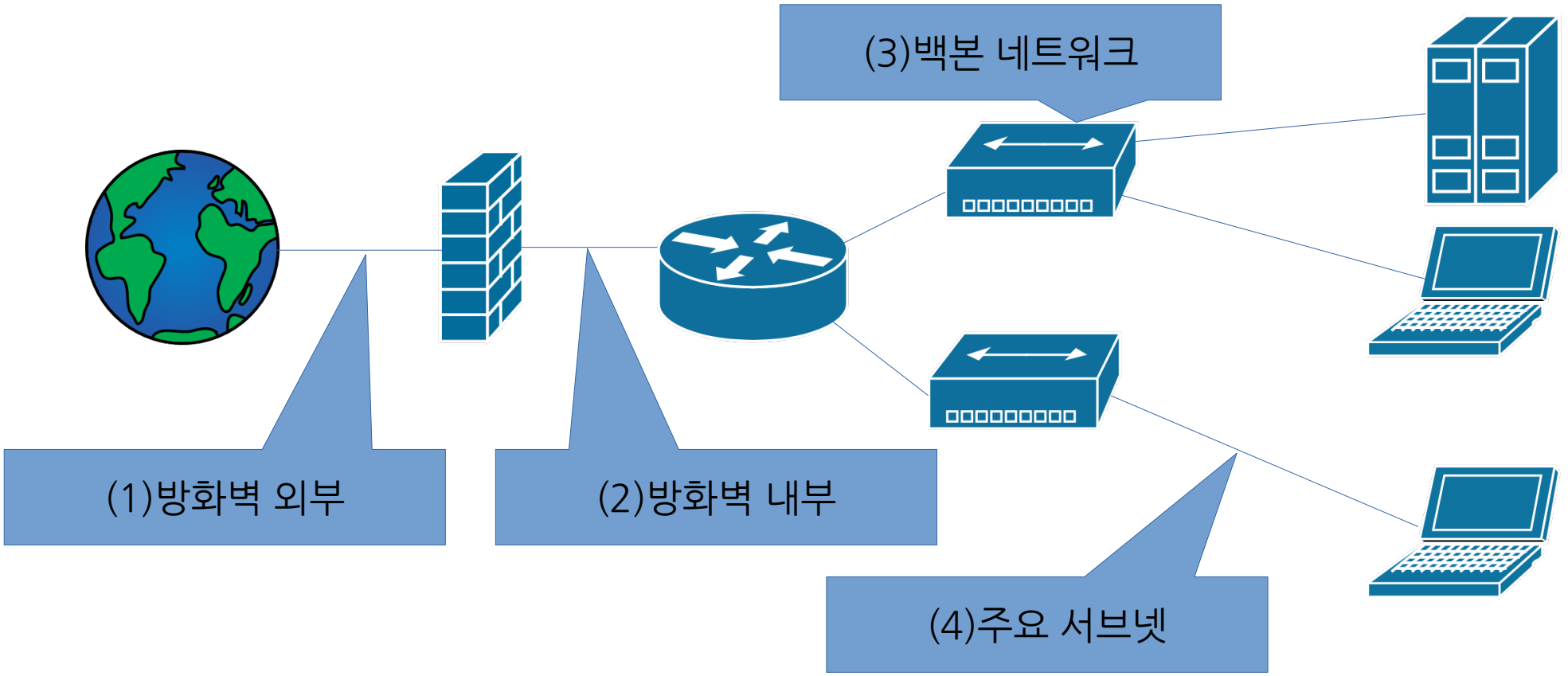
02 IDS, IPS

SNORT:오픈 소스 NIDS

- https://github.com/snort3/snort3/releases
  - https://github.com/snort3/snort3

02 IDS, IPS

NIDS 설치 위치



02 IDS, IPS

NIDS 설치 위치

(1)방화벽 외부

외부에서 내부로 유입되는 모든 침입 탐지가 가능하고 방화벽 자체에 대한 침입을 탐지함

(2)방화벽 내부

방화벽을 통과한 침입을 탐지함, 방화벽이 접근 통제 규칙에 따라 명확하게 작동하는지 확인할 수 있음

(3)백본 네트워크

내부 사용자의 악의적 사용이나 오남용을 탐지, 대규모 네트워크 트래픽 감시

(4)주요 서브넷

망내부 사용자의 악의적 사용이나 오남용을 탐지, 소규모 네트워크 트래픽 감시

02 IDS, IPS

HIDS

- **파일의 위변조 여부를 탐지**
  - 파일의 해시 값 대조를 통해 확인
  - 주기적으로 해시 값을 재계산하여 처음과 다른지 확인
- **정확도 높음**
  - 1비트만 변화해도 완전히 다른 해시 값이 발생됨
- **리소스 소모**
  - 해시를 계산하고 대조하는 과정에서 호스트의 자원이 사용됨
  - 각 호스트의 HIDS를 모두 관리해야 하는 것에는 어려움이 따름
- **HIDS 자체의 변조 위험성**
  - 호스트 내 파일 변조가 가능하다는 것은 곧 호스트의 HIDS를 구성하는 파일이나 로그 역시 변조가 가능하다는 것을 시사함

02 IDS, IPS

TripWire:오픈 소스 HIDS

- https://github.com/Tripwire/tripwire-open-source

02 IDS, IPS

IPS

정의

Intrusion Prevention System, 침입 방지 시스템
시스템이나 네트워크에 대한 다양한 불법 침입 행위를 실시간 탐지, 분석하여 위협을 자동적으로 차단하는 시스템

설명

①관리자에게 보고만 하는 IDS와 달리 능동적이고 즉각적인 차단이 이루어짐
②주로 Inline방식의 Gateway로 동작하는 경우가 많은 것으로 추측
③많은 패킷이 IPS를 통해서 전달되기 때문에 처리 용량이 중요
④IPS에 고장이 발생하면 해당 IPS 하위의 네트워크와 통신 불가

02 IDS, IPS

Firewall, IDS, IPS 비교

	방화벽	침입 탐지 시스템	침입 방지 시스템
패킷 차단	O	X	O
패킷 내용 분석	X	O	O
오용 탐지	X	O	O
오용 차단	X	X	O
이상 탐지	X	O	O
이상 차단	X	X	O