네트워크 보안 장비

네트워크 보안, 왜 중요할까요?

- **디지털 세상의 위협:**
  - 개인 정보 유출
  - 기업 데이터 손상
  - 서비스 마비 (해킹)
  - 금전적 손실
  - 사회적 혼란 야기

- **보안 장비의 필요성:**
  - 외부 위협으로부터 내부 네트워크 보호
  - 정보 자산의 안전한 관리
  - 안정적인 서비스 제공
  - 법적/규제적 준수

방화벽 (Firewall)

•내부 네트워크와 외부 네트워크(인터넷) 사이에 위치하여 불법적인 침입을 막는 **보안 시스템의 첫 번째 문지기**
•미리 정해진 **보안 정책(Rule)**에 따라 네트워크 트래픽(데이터 통신)을 허용하거나 차단

기능

- **-패킷 필터링**
- **-상태 기반 검사 (Stateful Inspection)**
- **-네트워크 주소 변환 (NAT)**
- **-VPN** 지원

특징

- **-네트워크 계층 (OSI 3/4계층) 기반 작동:** IP 주소, 포트 번호 등 기반
- **-정의된 규칙에 철저히 따름:** 규칙에 없는 비정상적인 트래픽은 차단
- **-침입 "방지"에 중점:** 알려진 위협에 대한 방어

IDS (Intrusion Detection System): 침입 탐지 시스템

•네트워크 트래픽이나 시스템 로그를 **실시간으로 모니터링**하여 **의심스러운 활동이나 침입 시도를 탐지**하고 관리자에게 **경고(Alert)**를 보내는 시스템
•**탐지**가 주 목적이며, 직접적인 차단 기능은 없음

기능

-시그니처 기반 탐지 (Signature-based Detection
-이상 행위 기반 탐지 (Anomaly-based Detection): 정상적인 시스템/네트워크 행위의 기준을 학습하고, 이 기준에서 벗어나는 비정상적인 행위 탐지
-프로토콜 이상 탐지: 특정 프로토콜의 표준에서 벗어나는 행위 탐지
-로그 분석: 시스템 및 애플리케이션 로그를 분석하여 보안 이벤트 탐지

특징

-침입 "탐지"에 중점: 이미 발생했거나 진행 중인 침입을 알림
-패시브(Passive) 방식: 네트워크에 영향을 주지 않고 모니터링만 수행
-오탐(False Positive) 및 미탐(False Negative) 가능성 존재

IPS (Intrusion Prevention System): 침입 방지 시스템

- IDS의 기능을 포함하여 **탐지된 위협에 대해 능동적으로 "차단" 또는 "방어" 조치를 취하는 시스템**
- 네트워크 중간에 위치하여 트래픽을 검사하고, 의심스러운 트래픽을 즉시 차단
- **하는 기능:**
- **IDS의 모든 탐지 기능 포함** (시그니처, 이상 행위 기반 등)
- **자동화된 방어 조치:**
    - 악성 트래픽 차단
    - 의심스러운 세션 종료
    - 공격 발생지 IP 차단 (블랙리스트 등록)
    - 관리자에게 알림 전송
- **취약점 기반 보호:** 알려진 시스템/애플리케이션 취약점을 이용하는 공격 차단
- **특징:**
- **침입 "방지"에 중점:** 위협을 탐지하는 즉시 자동으로 차단
- **인라인(In-line) 방식:** 네트워크 트래픽 경로에 직접 삽입되어 실시간으로 패킷 검사 및 제어
- 오탐 시 네트워크 성능 저하나 서비스 중단 발생 가능성 (주의 필요)

Proxy Server (프록시 서버)

- 클라이언트(사용자)와 서버(웹사이트 등) 사이에서 **대리인 역할을 수행하는 서버**
- 클라이언트의 요청을 대신 서버에 전달하고, 서버의 응답을 다시 클라이언트에 전달
- **하는 기능:**
- **보안 강화:**
  - 클라이언트의 IP 주소를 숨겨 익명성 제공 (Forward Proxy)
  - 내부 서버의 IP 주소를 숨겨 외부 노출 방지 (Reverse Proxy)
  - 악성 코드 필터링, 웹 필터링 등
- **캐싱(Caching):** 자주 요청되는 콘텐츠를 캐싱하여 응답 속도 향상 및 네트워크 트래픽 감소
- **접근 제어:** 특정 웹사이트 접속 차단 등 내부 정책 적용
- **로그 기록:** 사용자들의 웹 접속 기록을 남겨 보안 감사 및 통계 자료 활용
- **특징:**
- **클라이언트와 서버 사이의 중개자 역할**
- **주로 애플리케이션 계층 (OSI 7계층)에서 작동:** HTTP, FTP 등 프로토콜 이해
- **포워드 프록시 (Forward Proxy):** 내부 사용자가 외부 인터넷 접속 시 사용 (보안, 캐싱, 익명성)
- **리버스 프록시 (Reverse Proxy):** 외부 사용자가 내부 서버에 접속 시 사용 (보안, 로드 밸런싱, 캐싱)

WAF (Web Application Firewall): 웹 애플리케이션 방화벽

- 일반 방화벽이 네트워크 트래픽을 제어하는 것과 달리, **웹 애플리케이션에 특화된 공격을 방어하는 보안 솔루션**
- HTTP/HTTPS 트래픽을 심층적으로 분석하여 웹 기반 공격 차단
- **하는 기능:**
- **OWASP Top 10 공격 방어:**
    - SQL Injection (SQL 삽입 공격)
    - XSS (Cross-Site Scripting, 교차 사이트 스크립팅)
    - CSRF (Cross-Site Request Forgery)
    - 파일 업로드 취약점
    - 디렉토리 탐색
    - 세션 하이재킹 등
- **웹 트래픽 분석:** HTTP/HTTPS 헤더, 바디, URL 등 웹 프로토콜의 모든 요소를 분석
- **정책 기반 차단:** 웹 애플리케이션 취약점을 노리는 공격 패턴 탐지 및 차단
- **봇(Bot) 차단:** 악성 봇이나 스크래핑 봇 활동 제어
- **특징:**
- **애플리케이션 계층 (OSI 7계층)에서 작동:** 웹 서비스에 특화된 보안 제공
- **웹 애플리케이션 취약점 공격 방어에 탁월**
- 기존 방화벽, IDS/IPS로 막기 어려운 웹 기반 공격에 특화
- 웹 서비스의 안정성과 가용성 유지에 기여

네트워크 장비 비교

분류	방화벽 (Firewall)	IDS/IPS	Proxy Server	WAF
주요 역할	네트워크 출입 통제 (문지기)	침입 탐지 및 방어	클라이언트-서버 중개 (대리인)	웹 애플리케이션 공격 방어
작동 계층	OSI 3/4계층 (네트워크/전송)	OSI 2~7계층 (주로 네트워크/전송/애플리케이션)	OSI 7계층 (애플리케이션)	OSI 7계층 (애플리케이션)
주요 보호 대상	네트워크 전체	네트워크 및 시스템 전체	클라이언트/서버 익명성 및 접근 제어	웹 애플리케이션 서비스
주요 기능	패킷 필터링, NAT, VPN	(IDS) 침입 탐지 및 경고, (IPS) 침입 탐지 및 차단	캐싱, 접근 제어, 보안 강화 (IP 숨김)	SQL Injection, XSS 등 웹 공격 방어
공격 방어 방식	IP, Port 기반 규칙	패턴/행위 기반 탐지 및 차단	중개 및 필터링	웹 트래픽 심층 분석 및 차단
장점	기본적인 네트워크 보안 제공, 빠른 처리	다양한 공격 탐지, IPS는 자동 방어	캐싱으로 성능 향상, 익명성, 접근 제어	웹 공격에 특화된 정밀 방어
단점	웹 공격에 취약, 정교한 공격 방어 어려움	오탐/미탐 가능성, IPS는 성능 저하 위험	오버헤드 발생 가능, 단일 장애점 가능	웹 공격 외 다른 유형의 공격 방어 어려움