기업 데이터보호를 위한 실전 보안 마스터 과정

한국생산성본부

Contact liz0904@teiren.io

010-6539-2122

네트워크 보안 취약점

해당 강의자료는 외부 반출을 금합니다.

스니핑(Sniffing)이란?

스니핑이란?

Sniff의 사전적 의미

- 코를 킁킁거리다

개념

- 도청(Eavesdropping)과 엿듣기가스니핑

수동적(Passive) 공격으로 분류

- 공격할때아무것도하지않아도충분하기때문

준비

1. 랜카드 확인
2. 패킷 캡쳐 프로그램 설치
3. TCP Dump

스니핑 준비

랜(LAN) 카드확인하기

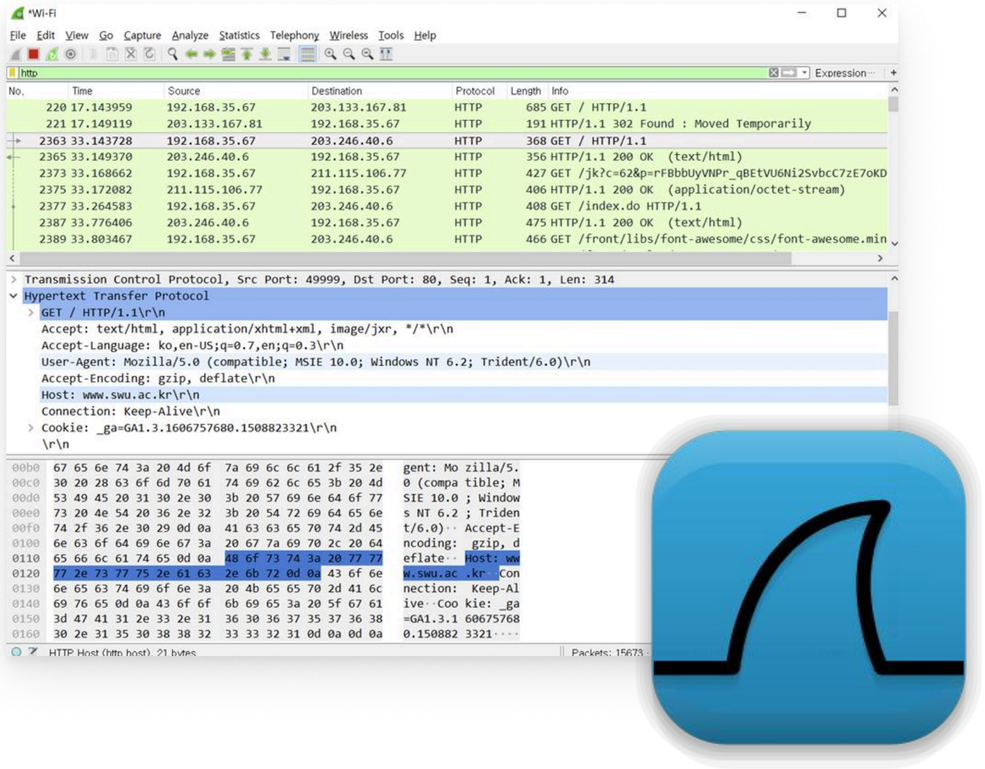
[명령프롬프트] –ifconfig(리눅스), ipconfig(윈도우)

패킷캡쳐프로그램설치

- TCP Dump (리눅스), Wireshark (윈도우)

TCPDump

- 리눅스에서 가장 기본이되는, 하지만 강력한 스니핑 툴
- 처음에는 네트워크 관리를 위해 개발되었기 때문에 관리자 느낌이 강함
- TCP Dump로 획득한 증거 자료는 법적 효력이 있음

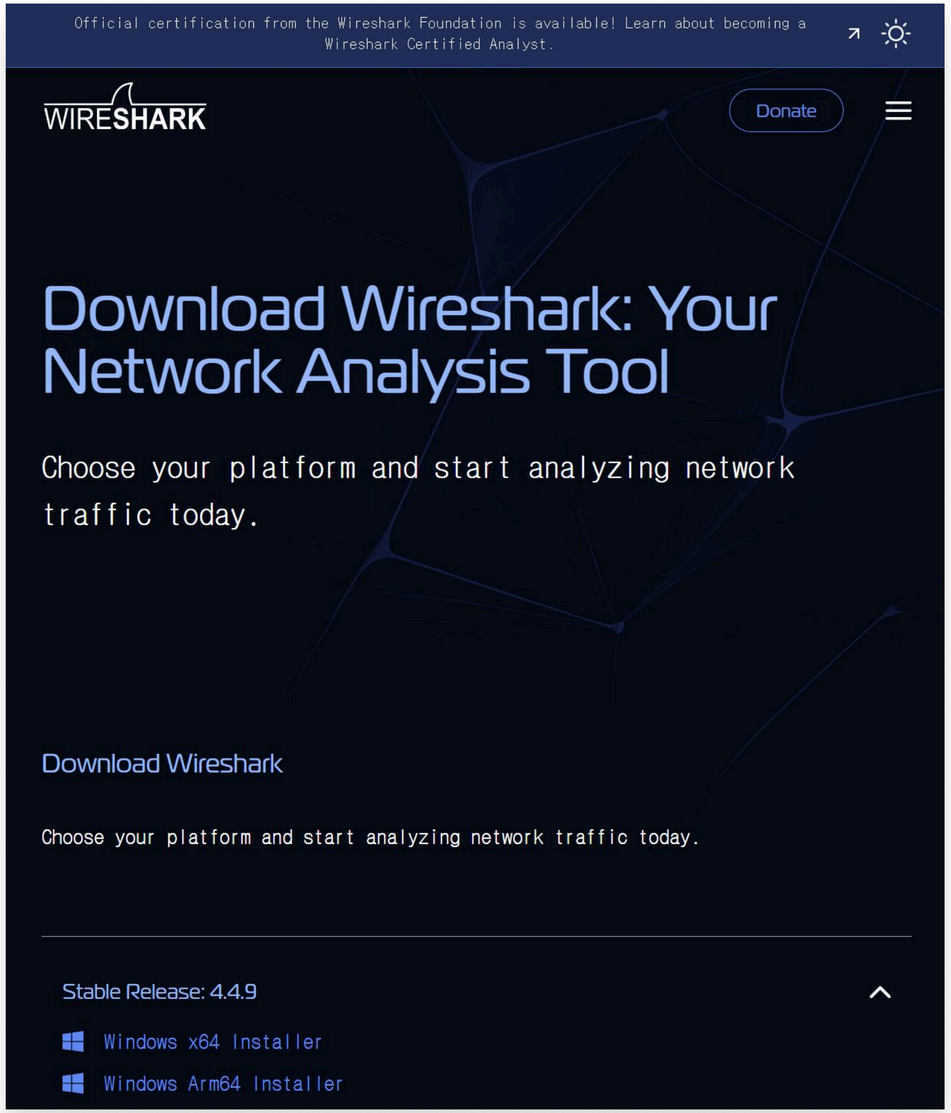


와이어샤크(Wireshark)란?

- 네트워크에서 오가는 패킷(데이터)을 캡처하고 분석하는 가장 널리 쓰이는 GUI 기반 툴

Wireshark로 가능한 일

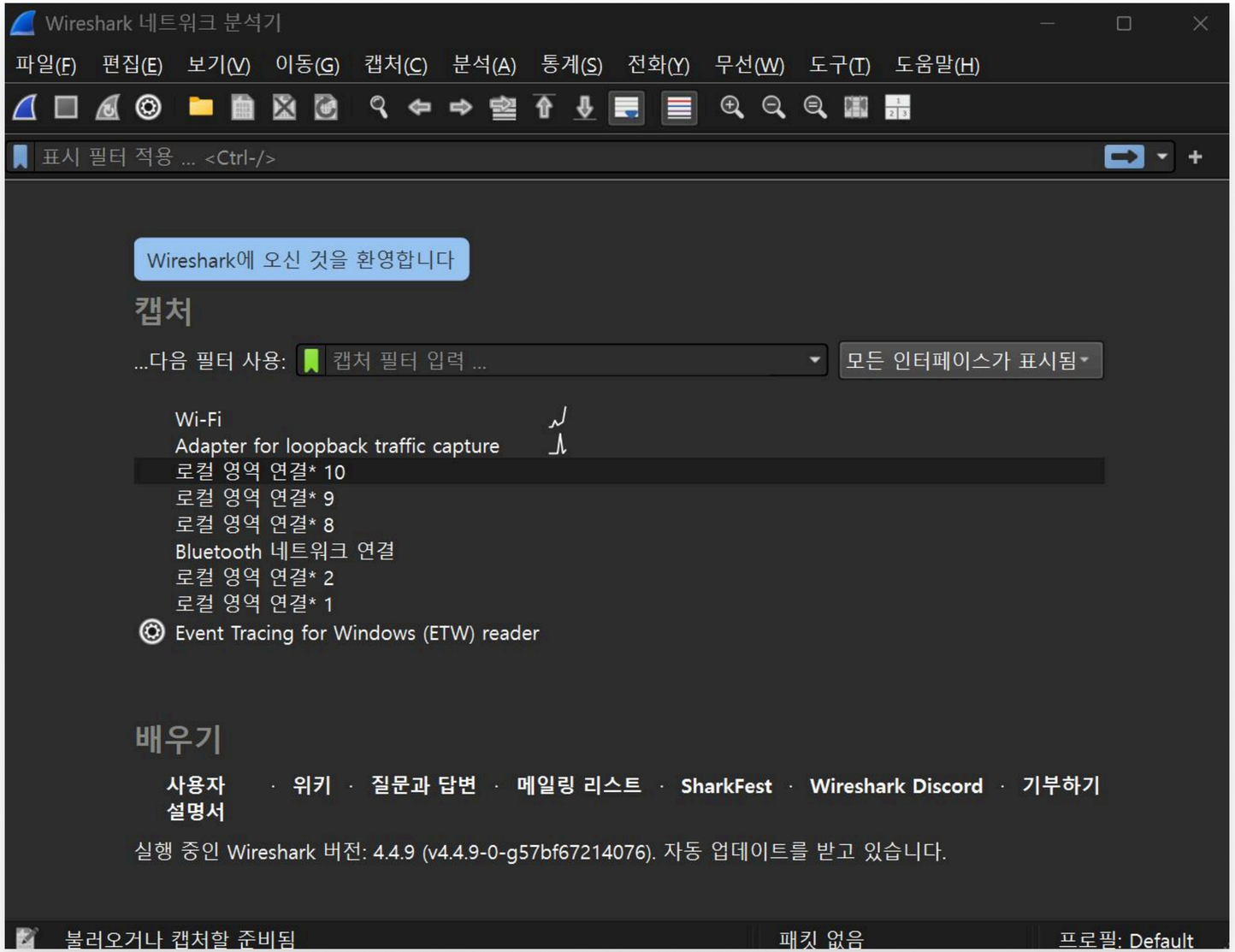
- **네트워크 트래픽 실시간 캡처** 및 pcap 파일 저장
- 패킷별 상세 헤더(이더넷/IP/TCP/UDP/HTTP 등) 해석
- Display filter로 관심 패킷만 보기(예: 특정 IP, 포트, SYN 패킷)
- TCP 스트림 재조합(HTTP 대화, 파일 전송 등 원문 보기)
- 패킷 재조합(IPv4 fragment, TCP 세그먼트) 설정·확인
- 통계 기능: Conversations, Endpoints, IO graph, Protocol Hierarchy 등
- CLI 버전인 tshark로 자동화/스크립트 처리 가능



Wireshark 설치

환경에 맞는 exe 파일 다운로드

- exe 파일 실행 후 기본 세팅 대로 Next



Wireshark 실행

스푸핑이란?

개념

- 사전적 의미: 속이다
- 인터넷이나 로컬에서 존재하는 모든 연결에스푸핑 가능
- 정보를 얻어내기 위한 중간 단계의 기술로 사용 하는 것 외에도 시스템을 마비 시키는데 사용할 수도 있음
- 예: ARP 리다이렉트공격

ARP 스푸핑

- MAC 주소를 속이는 것
- 2계층에서 작동해 공격 대상이 같은 랜에 있어야 함

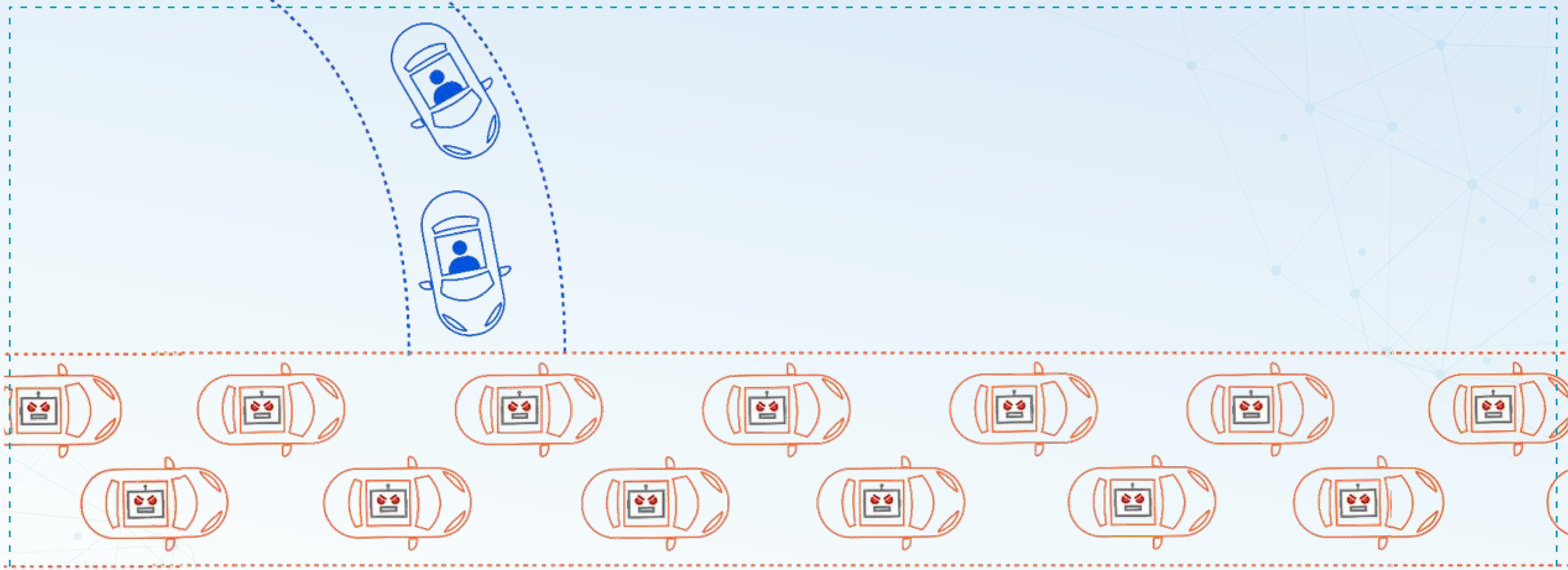
DoS

DoS(Denial of Service,서비스 거부)

- 공격 대상이 수용할 수 있는 능력 이상의 정보를 제공하거나 사용자 또는 네트워크 용량을 초과시켜 정상적으로 작동하지 못하게 하는 공격

DoS공격의특징

- 파괴공격: 디스크, 데이터, 시스템 파괴
- 시스템 자원 고갈 공격
- CPU, 메모리, 디스크의 과다한 사용으로 인한 부하 가중
- 네트워크 자원 고갈 공격
- 쓰레기 데이터로 네트워크 대역폭의 고갈

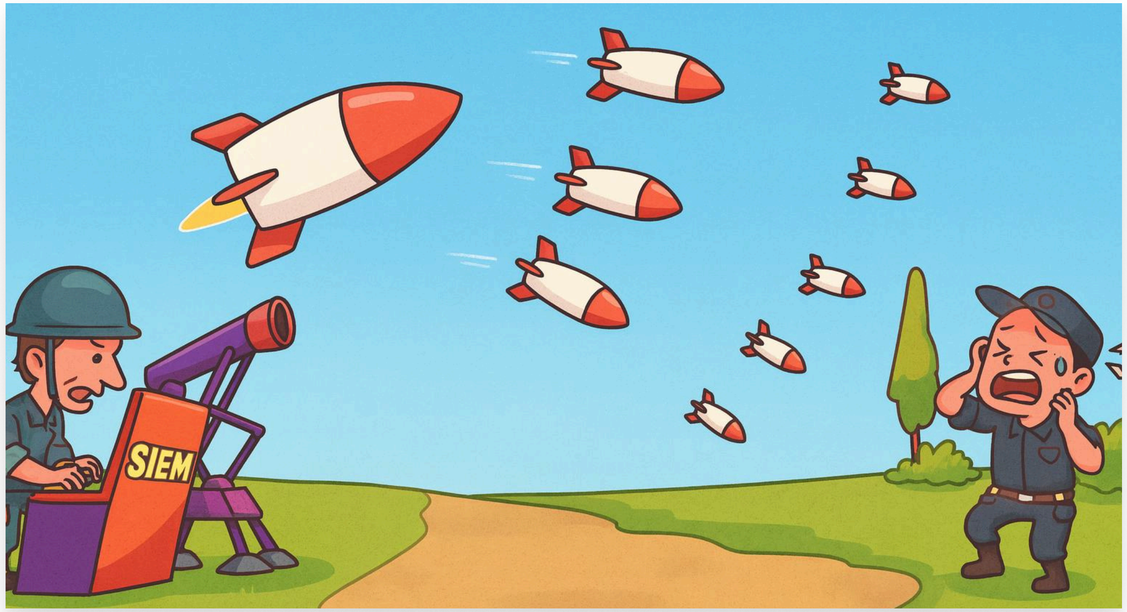


- 네트워크 상에는 허용할 수 있는 데이터의 양이 정해져 있음.
- 허용된 양 이상의 데이터가 서버에 들어오게 되면 통신 속도가 느려지거나, 아예 통신이 되지 않고 서버가 죽어버림
- 해커의 문제 뿐만 아니라, 재해·재난으로 인해 서버가 고장 났을 때에도 가용성이 파손됨.

Ping of Death 공격

Ping of Death 공격 원리

1. ping을 이용하여 ICMP 패킷의 크기를 정상보다 아주 크게 만듦
2. 크게 만들어진 패킷은 네트워크를 통해 라우팅되어 공격 네트워크에 도달하는 동안 아주 작은 조각으로 쪼개짐
3. 공격 대상은 조각화된 패킷을 모두 처리해야 하므로 정상적인 ping보다 부하가 훨씬 많이 걸림



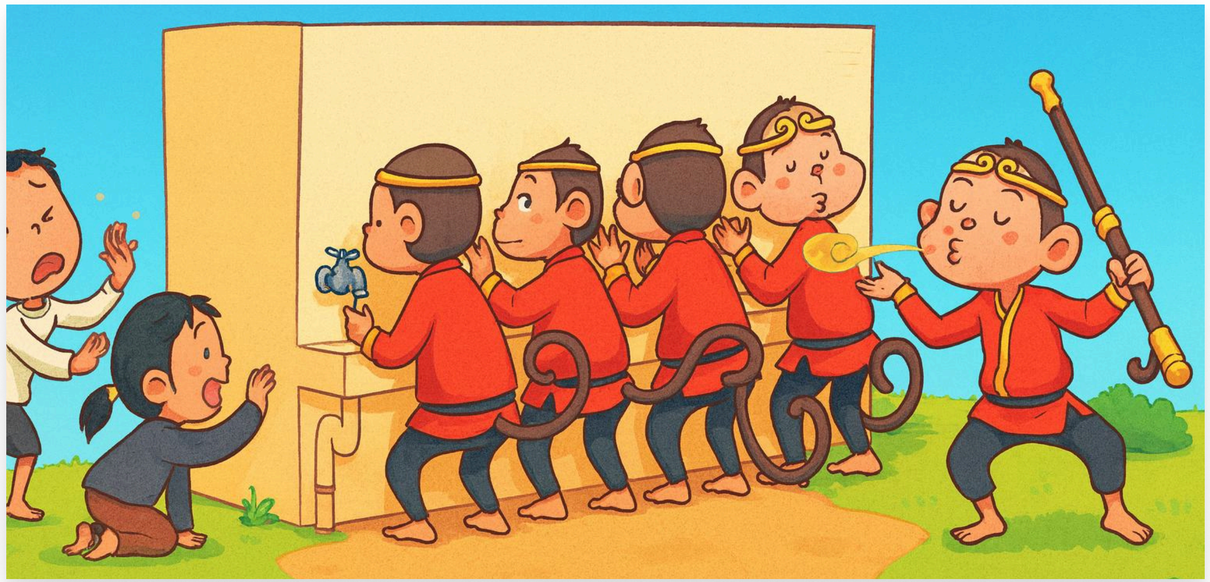
보안대책

- 반복적으로 들어오는 일정 수 이상의 ICMP 패킷을 무시하도록 설정
- 가장 일반적으로 할 수 있는 대책은 패치

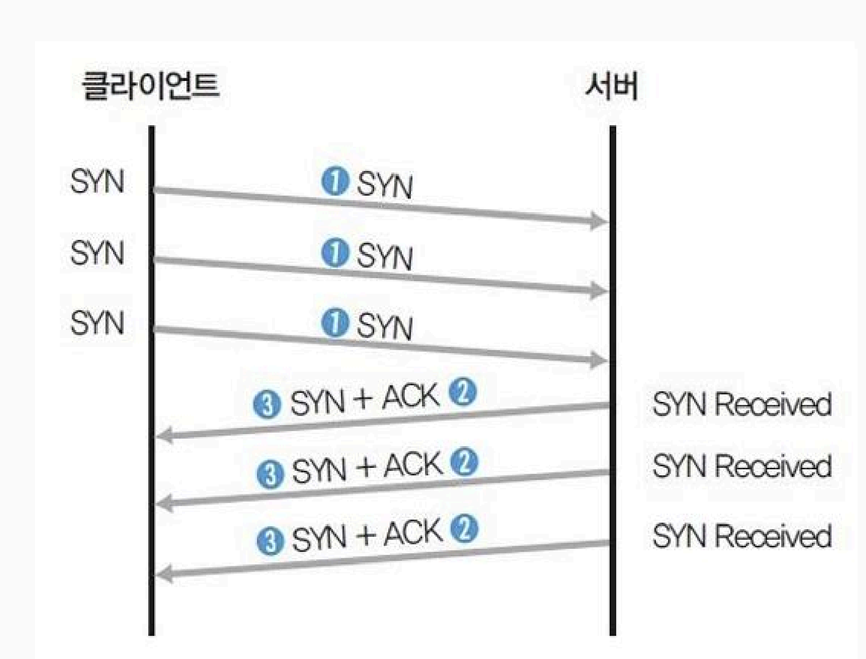
SYN Flooding 공격

SYN Flooding 공격 개념

서버 별로 한정되어 있는 접속 가능 공간에 존재하지 않는 클라이언트가 접속한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게 하는 것



SYN Flooding 공격



SYN Flooding 공격 원리

1. 공격자는 많은 숫자의 SYN 패킷을서버에 보냄
2. 서버는 받은 SYN 패킷에 대한 SYN/ACK 패킷을 각 클라이언트로 보냄
3. 서버는 자신이 보낸 SYN/ACK 패킷에 대한 ACK 패킷을 받지 못함
4. 서버는 세션의 연결을 기다리게 되고 공격은 성공함

DDoS 공격

DDoS (Distributed Denial of Service)

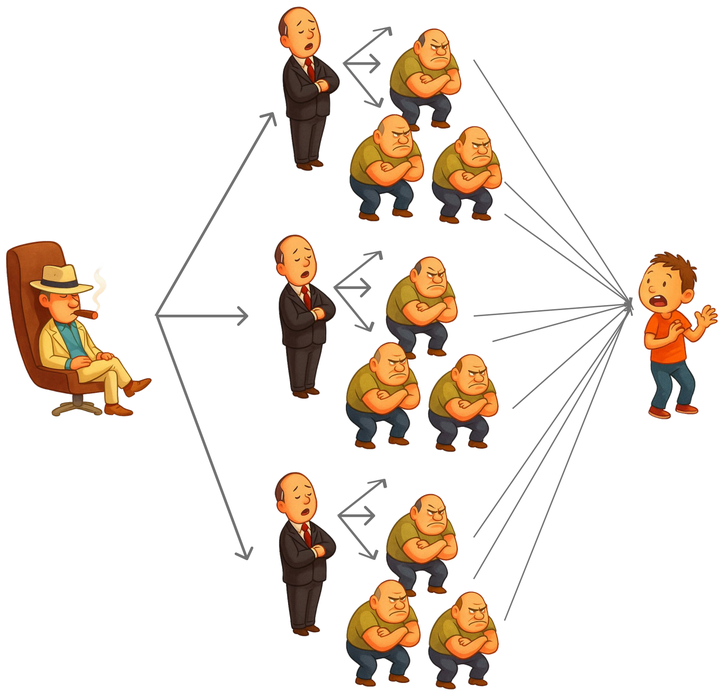
- DoS 공격이 발전된 것
- 피해 양상이 상당히 심각하지만 확실한 대책이 없음
- 공격자의 위치와 구체적인 발원지를 파악하는 일이 무척 어려워 여전히 대응이 어려운 공격 중의 하나
- 특성상 대부분의 DDoS 공격은 자동화 된 툴을 이용

DDoS 공격이 이루어지기 위한 기본 구성

- 공격자(Attacker) : 공격을주도하는해커의컴퓨터
- 마스터(Master) : 공격자에게직접명령을받는시스템, 여러대의에이전트관리
- 핸들러(Handler) 프로그램: 마스터시스템역할을수행하는프로그램
- 에이전트(Agent) : 공격대상에직접공격을가하는시스템
- 데몬(Daemon) 프로그램: 에이전트시스템역할을수행하는프로그램

DDoS 공격 구성도

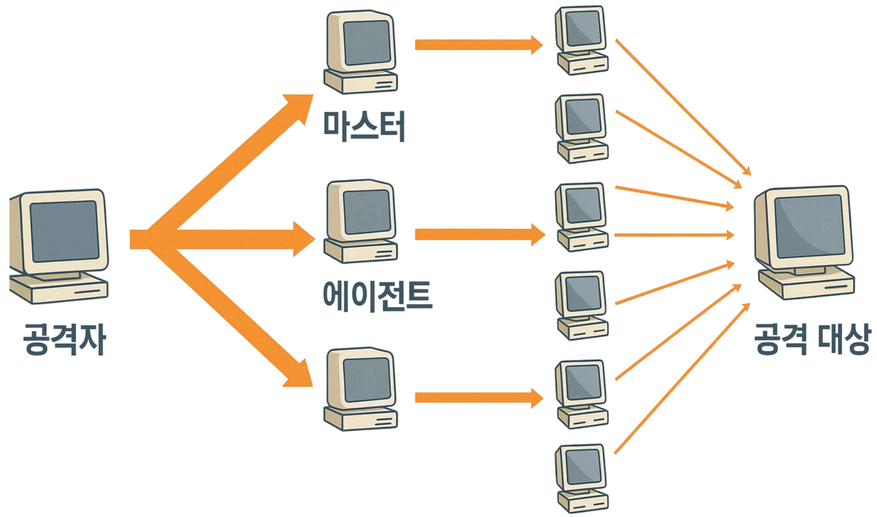
- 공격자는 폭력 조직의 두목
- 마스터는 행동대장
- 에이전트는 졸개에 비유



DDoS 공격이 이루어지기 위한 기본 구성

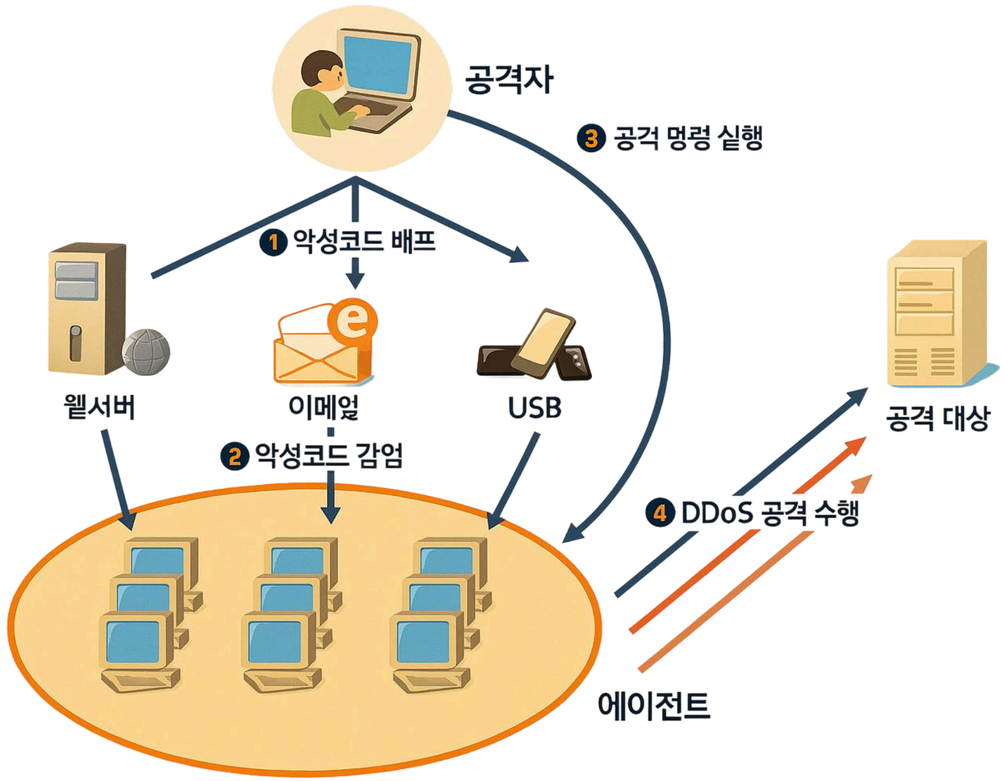
- 공격자(Attacker) : 공격을주도하는해커의컴퓨터
- 마스터(Master)　: 공격자에게직접명령을받는시스템, 여러대의에이전트관리
- 핸들러(Handler) 프로그램: 마스터시스템역할을수행하는프로그램
- 에이전트(Agent) : 공격대상에직접공격을가하는시스템
- 데몬(Daemon) 프로그램: 에이전트시스템역할을수행하는프로그램

- 중간자 역할을 하는 마스터와 에이전트가 피해자이기도 하다는 것이, 폭력 조직과 다름



악성코드를 이용한 DDoS 공격

악성코드에 감염된 좀비PC는 공격자의 공격 에이전트가 되고, 공격자가 공격 명령을 전달하면 공격 대상에게 DDoS 공격을 수행



DoS와 DDoS 탐지 및 예방 방법

방화벽(Firewall)설치와 운영

- 보통 내부 네트워크와 외부 네트워크의 경계선에 우선 설치
- 방화벽이 차단할 수 있는 침입은 실제로 30% 정도

방화벽 룰셋(규칙 집합)

- 최소한의 서비스만 제공하고 사용하지 않는 서비스의 포트는 닫음
- 침입 차단 시스템 내부의 구성 요소 간 트러스트Trust(신뢰)를 금지
- 인증 없이 시스템에 접속할 수 있는 내부/외부 사용자를 허용하지 않음

침입 차단 시스템의 설치와 운영

- 침입 차단 시스템: 네트워크에 침입해서 들어 오는 공격을 탐지하여 능동적으로 대응 하기 위한 시스템
- 실제 공격 시 또는 그 전에 공격 양상을 탐지할 수 있으므로, 이를 설치하여 새로운 패턴을 인식할 수 있도록 지속적으로 업그레이드하고, 관리해야함

DoS와 DDoS 탐지 및 예방 방법

시스템 패치

- 시스템에서 바이러스와 해킹 공격에 취약한 점이 발견되면 각 업체에서 패치를 발표하므로, 이를 설치하는 방법
- 해당 패치가 어떤 작용을 하는지 이해한 뒤, 설치해야 함(백업 필수)

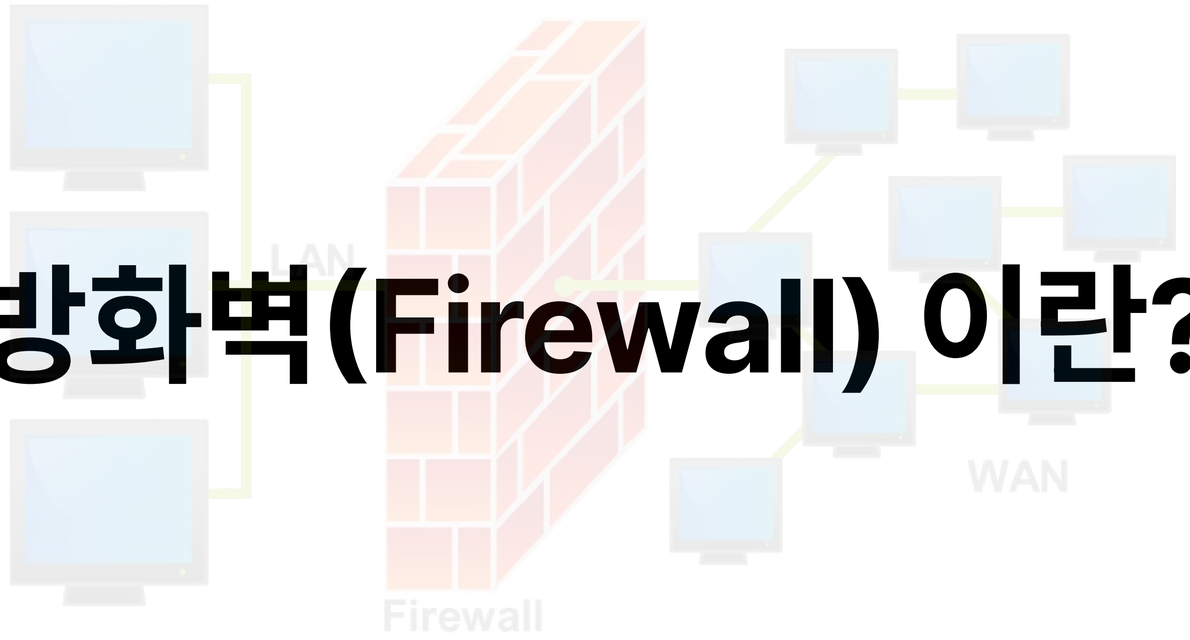
스캐닝

- 포괄적인 의미의 시스템 분석

서비스별 대역폭 제한

- 각 서비스 별로 대역폭을 조절하여 특정 서비스에 대한 공격이 이루어지더라도, 나머지 서비스에 대한 영향을 최소화 할 수 있음
- 공격이 이루어지고 있는 서비스도 공격 성공에 필요한 최소 대역폭을 얻을 수없어 공격에 성공하기 어려움

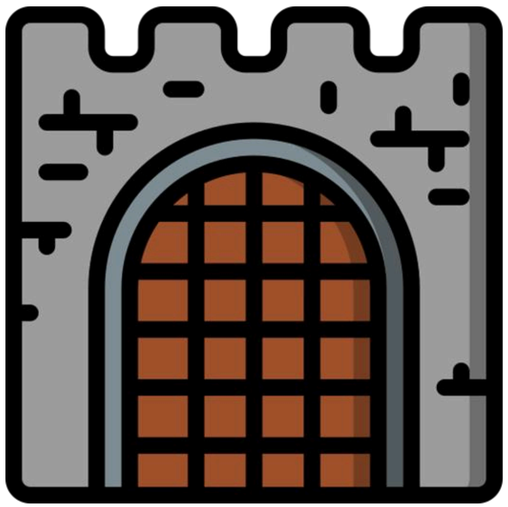
방화벽(Firewall) 이란?

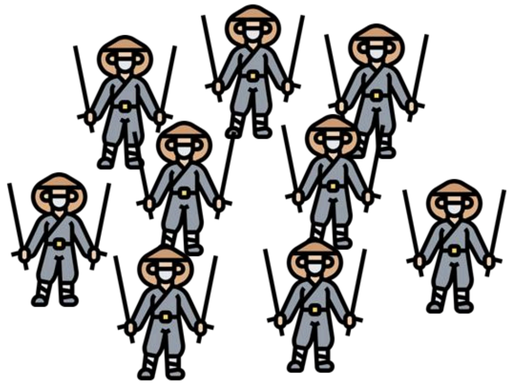


방화벽이란?

개념

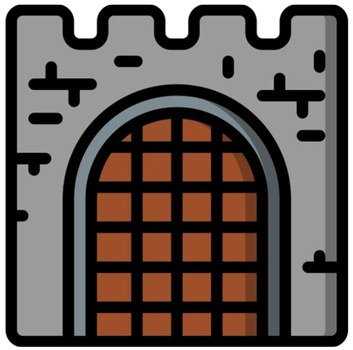
- 원치 않는 데이터가 오는 것을 보호해주는 보안 솔루션
- 성을 외부로부터 지키기 위한 성벽과 같은 비슷

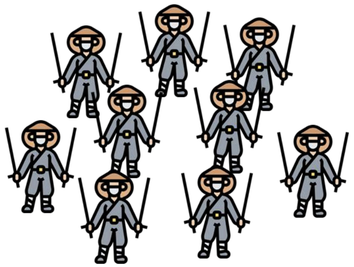




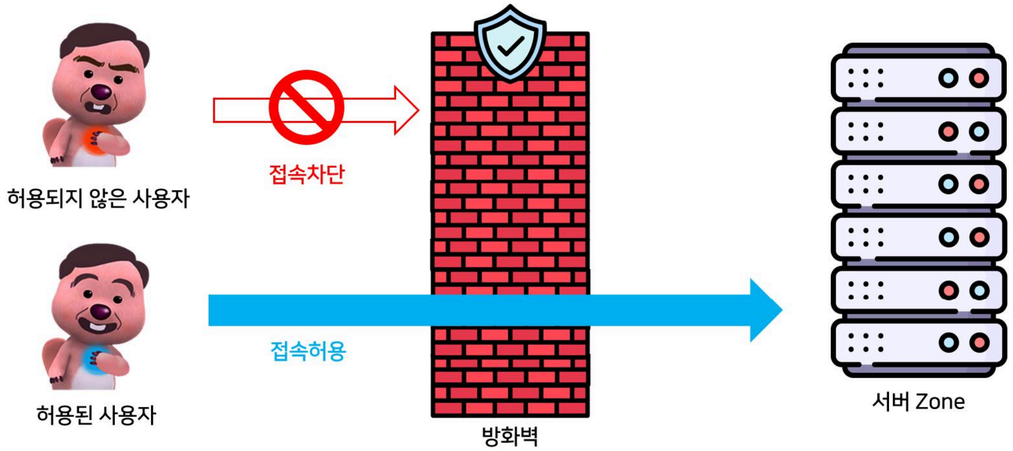
방화벽이란?

- 원치 않는 데이터가 오는 것을 보호해주는 보안 솔루션
- 성을 외부로부터 지키기 위한 성벽과 같은 비슷



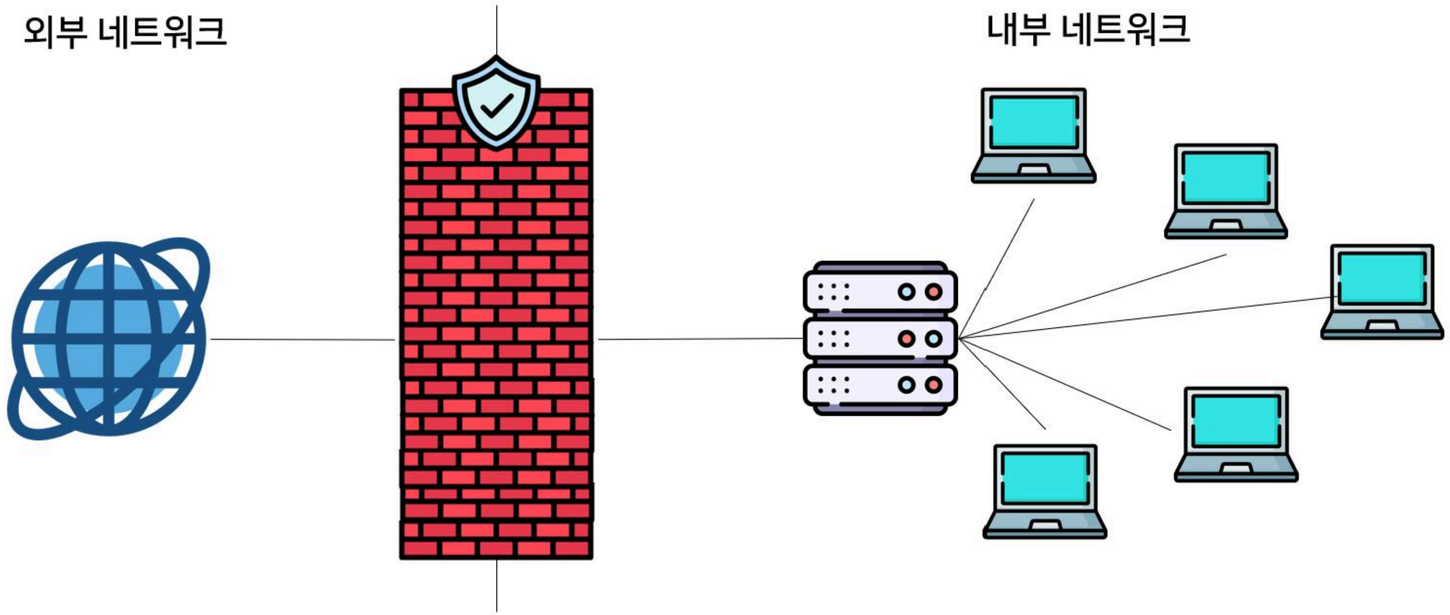


- 허용되지 않은 데이터 또는 사용자가 접근할 경우, 내부 네트워크에 접근하지 못함
- 허용된 사용자만 서버에 접근할 수 있도록 필터 역할을 함



방화벽의 위치

네트워크 보안의 최전방에 위치



방화벽의 역할과 필요

1. 보안 감시

- 인터넷과 내부 네트워크 사이에서 데이터 흐름을 감시해 악성코드나 해킹시도를 탐지

2. 액세스 제어 및 서비스 안정성

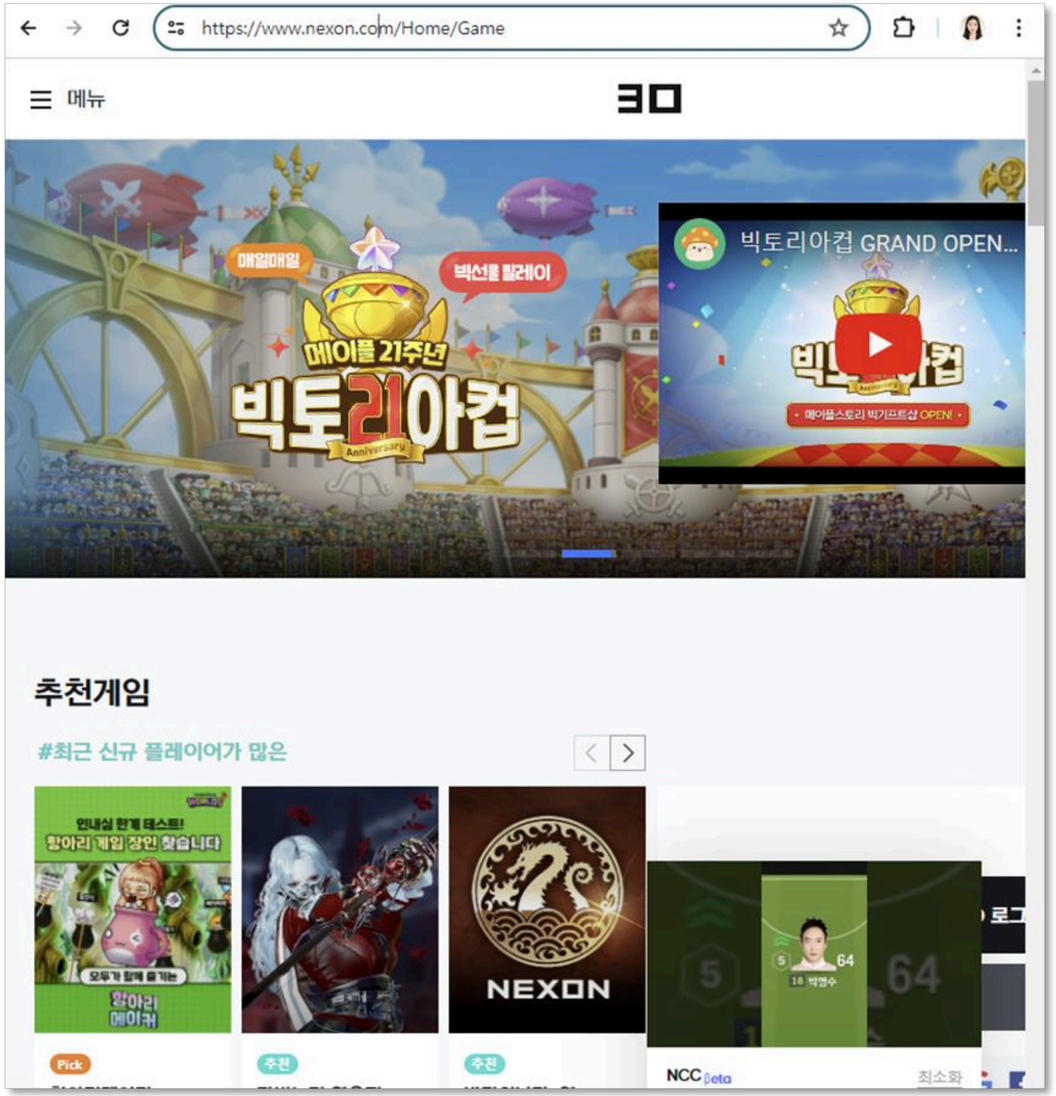
- 어떤 데이터가 내부 네트워크로 들어오는지 제어해, 악의적인 데이터 흐름을 차단
- 데이터의 흐름을 제어함으로써 서버의 원활한 작동을 보장

3. 사용자보호

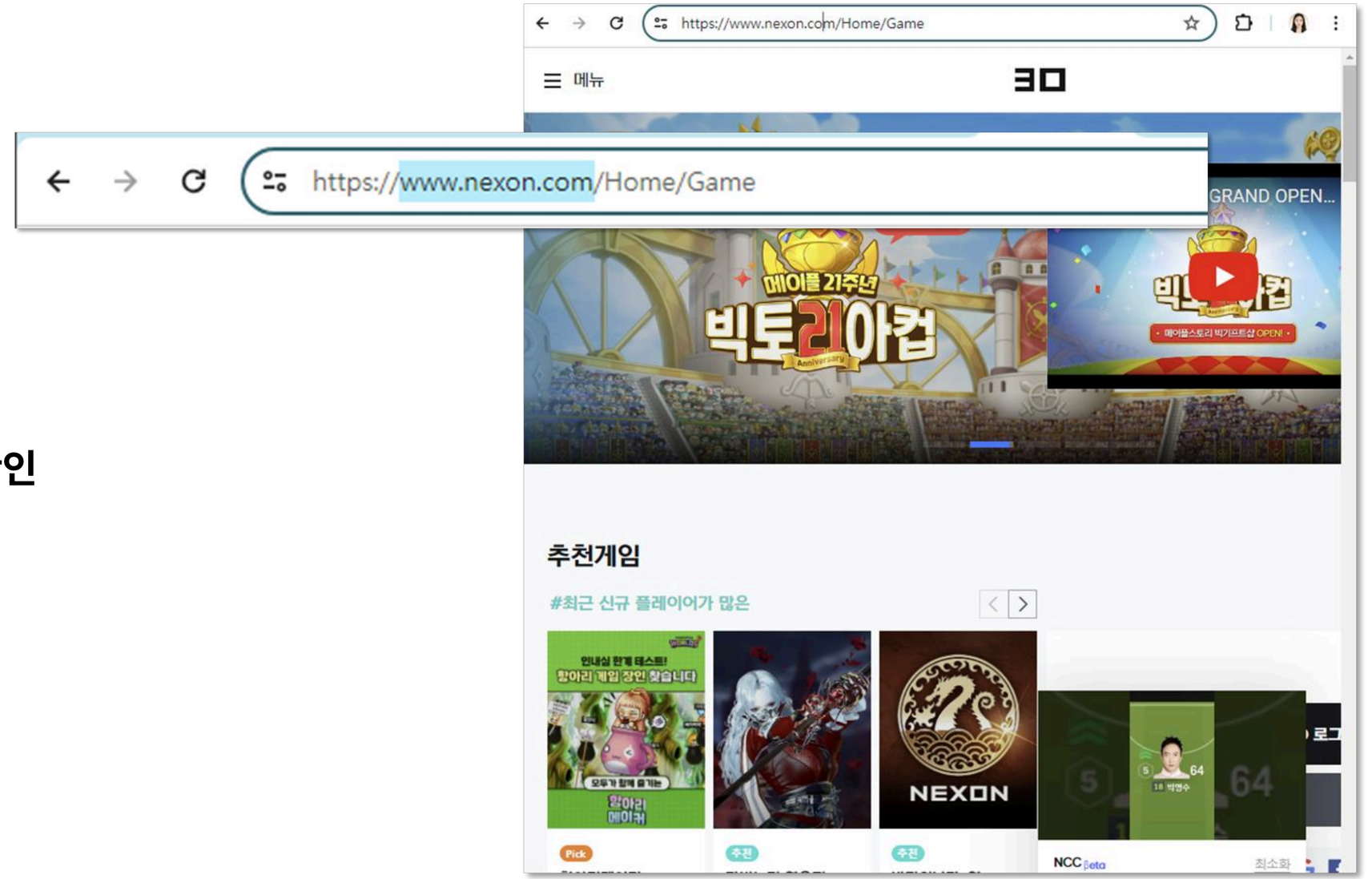
- 그 결과로 개인정보나 기업의 중요한 정보를 보호해 기업과 개인의 안전을 보호

윈도우즈 기본 방화벽 구성 실습

넥슨 사이트 접속


https://www.nexon.com/Home/Game
메뉴
메이플 21주년
빅토리아컵
Anniversary
빅토리아컵 GRAND OPEN...
추천게임
#최근 신규 플레이어가 많은
NEXON
NCC beta

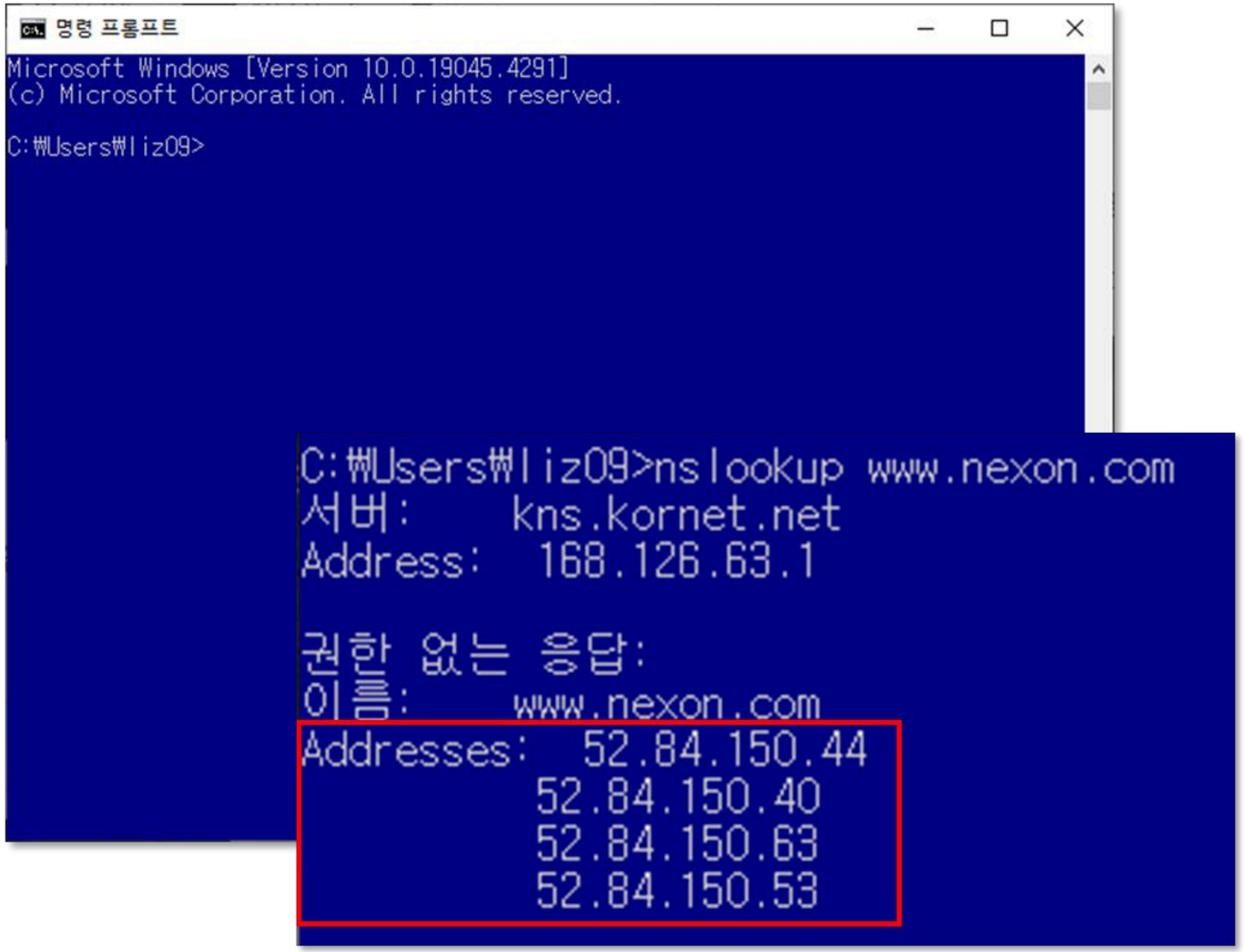
선택한 사이트의 URL 확인



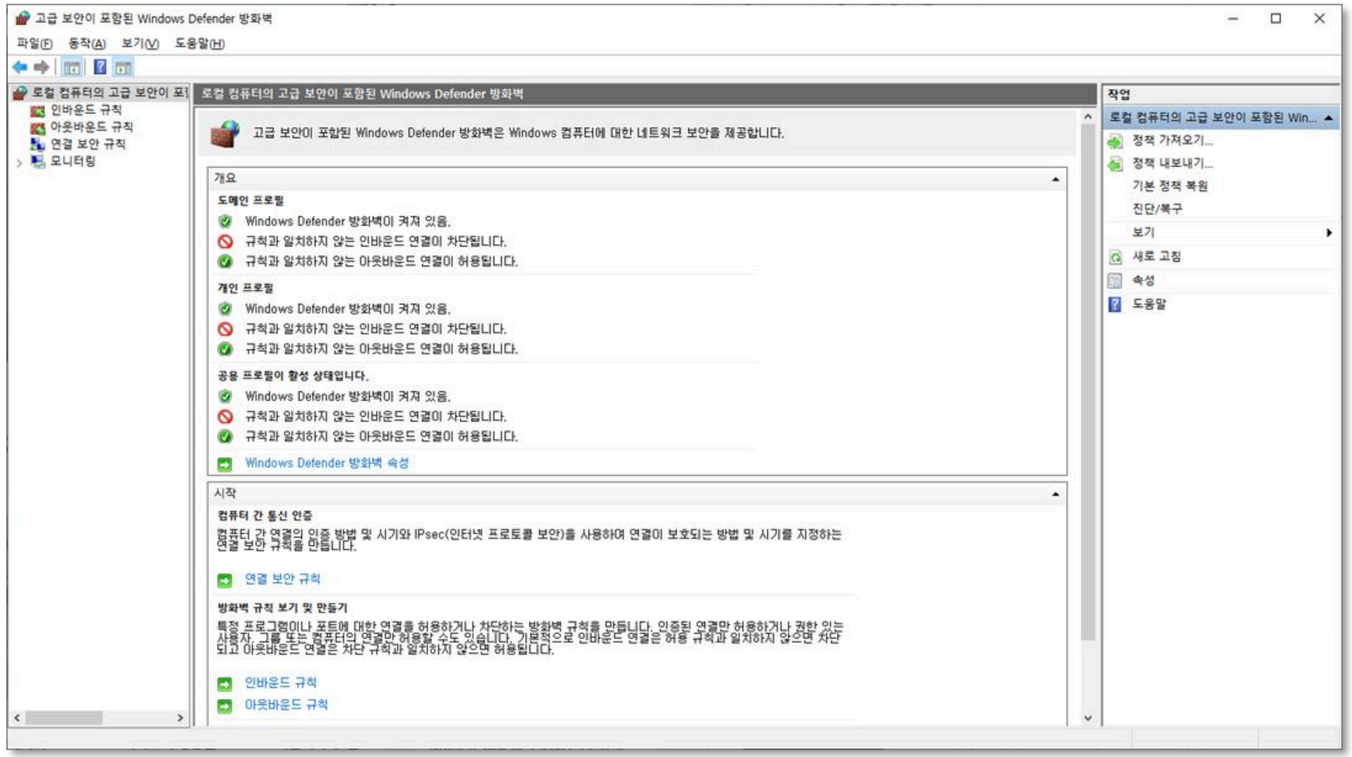
윈도우즈의 명령 프롬프트(cmd) 창에서 넥슨 사이트의 IP 알아내기

nslookup

- 입력한 웹사이트의 정보를 조회하는 명령어
- 서버 이름과 IP 주소를 알려줌
- 명령어 사용 방법: nslookup [웹사이트 url]
- 예) nslookup www.naver.com



[고급 보안이 포함된 Windows Defender 방화벽]
프로그램 실행



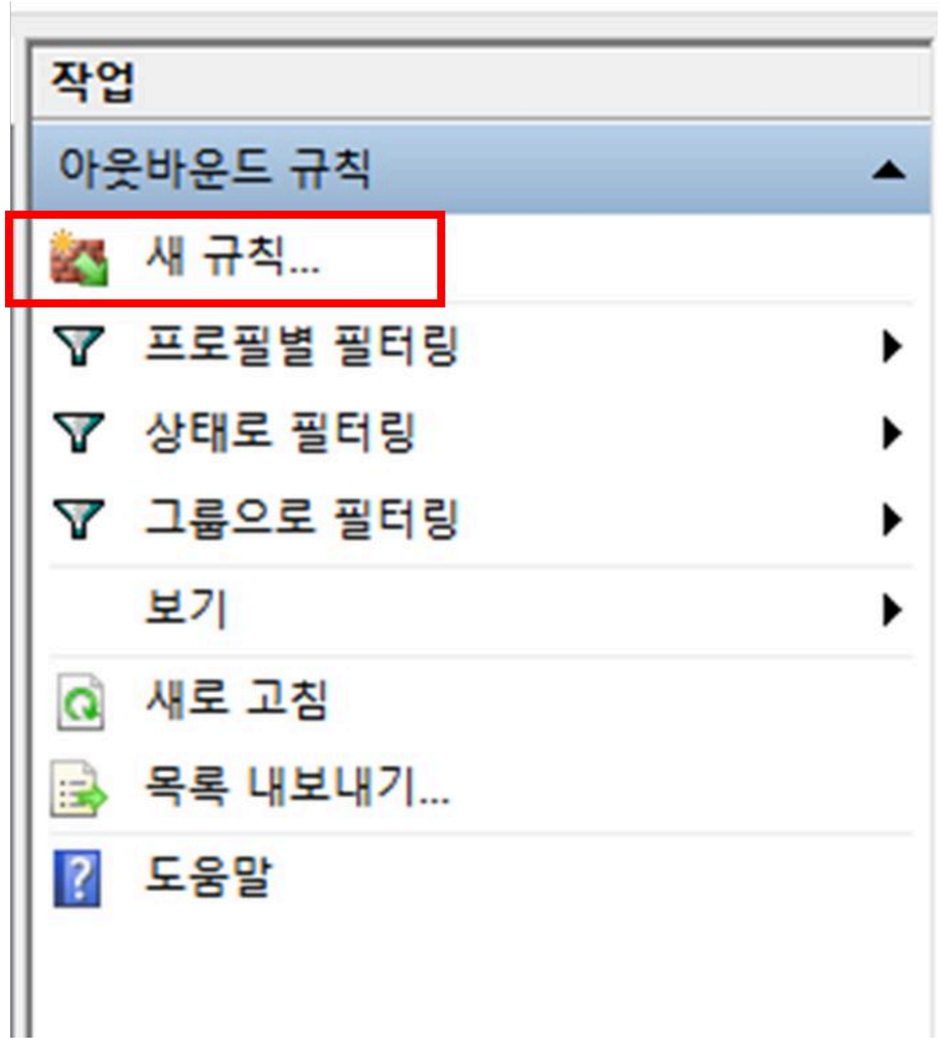
아웃바운드 규칙 설정

인바운드

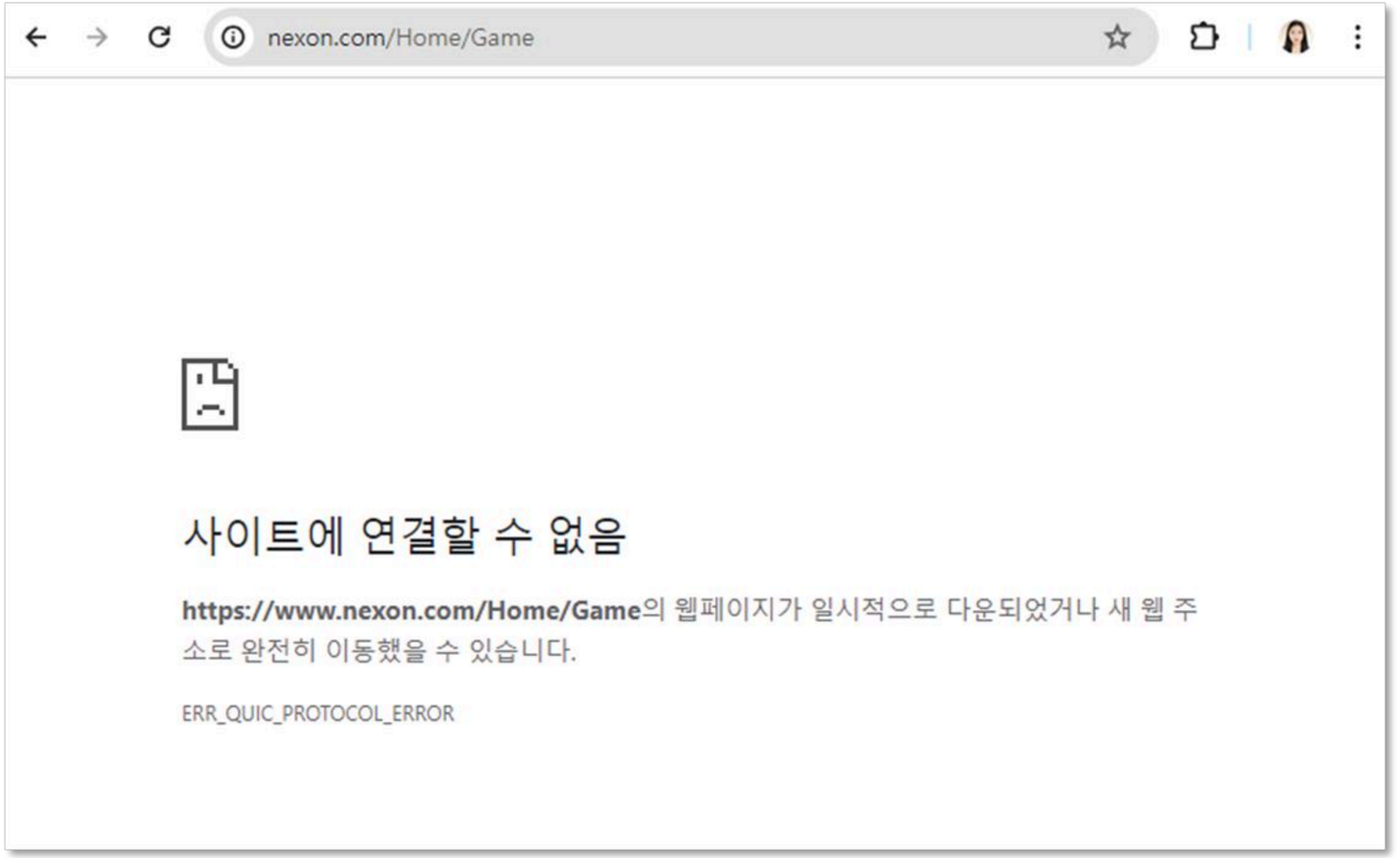
- 외부에서 내부로 들어오는 데이터
- ex) 파일 다운로드

아웃바운드

- 내부에서 외부로 나가는 데이터
- ex) 파일 업로드



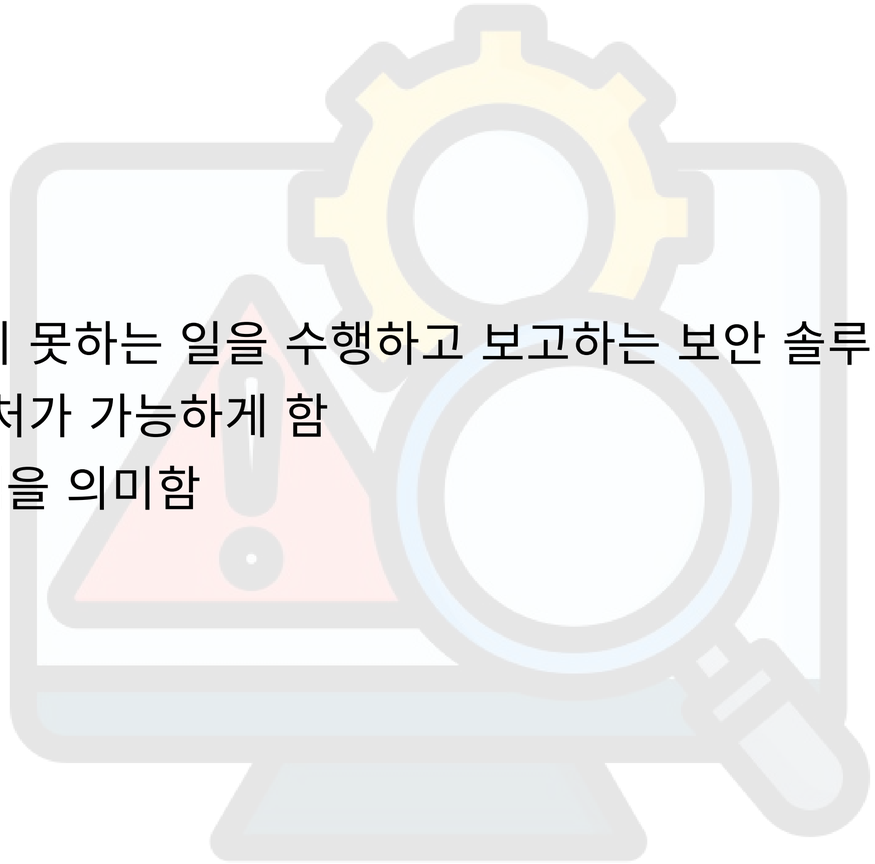
방화벽 설정 확인


nexon.com/Home/Game
사이트에 연결할 수 없음
https://www.nexon.com/Home/Game의 웹페이지가 일시적으로 다운되었거나 새 웹 주소로 완전히 이동했을 수 있습니다.
ERR_QUIC_PROTOCOL_ERROR

침입 탐지 시스템이란?

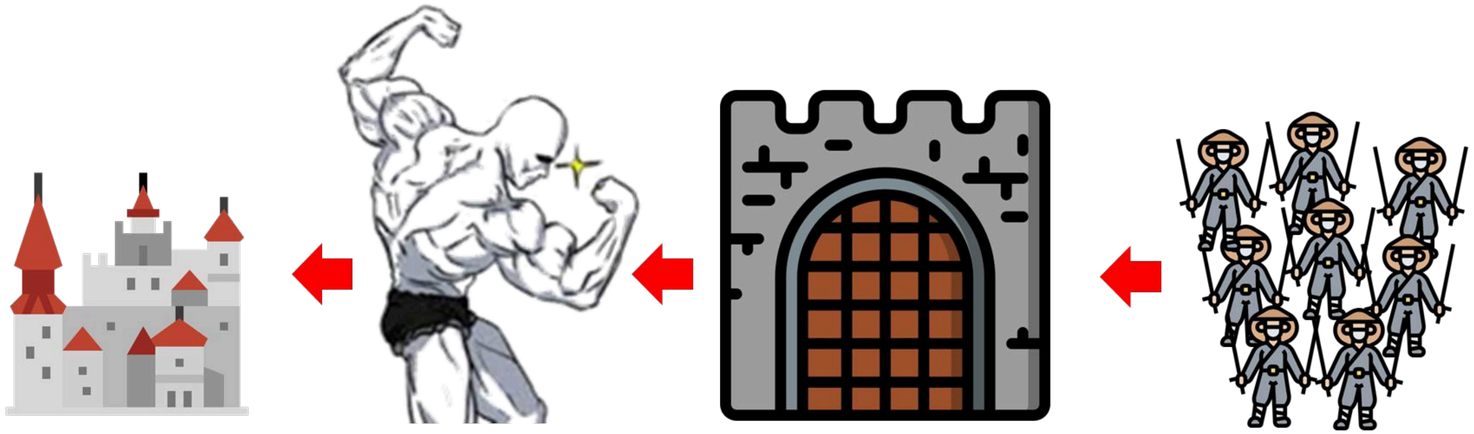
침입 탐지 시스템(Intrusion Detection System)

- 네트워크에서 백신과 유사한 역할을 하는 것
- 네트워크를 통한 해킹 공격을 탐지하기 위한 장비
- 내부의 해킹이나 악성 코드 활동 탐지와 같이 방화벽이 하지 못하는 일을 수행하고 보고하는 보안 솔루션
- 보안 공격이 발생했을 때 이를 관리자에게 알려, 적절한 대처가 가능하게 함
- IDS와 늘 함께 나오는 개념이 IPS, IPS는 침입 방지 시스템을 의미함



방화벽 VS 침입탐지시스템

- 방화벽(firewall)은 단순히 IP주소와 포트 번호 등의 속성으로 차단을 결정
- IDS는 전달되는 메시지(데이터)의 내용을 분석해 차단을 결정
- 방화벽(firewall)은 단순히 IP주소와 포트 번호 등의 속성으로 차단을 결정
- IDS는 전달되는 메시지(데이터)의 내용을 분석해 차단을 결정
- 즉, 방화벽은 성벽, 침입탐지 시스템은 성 안의 병사!



허니팟이란?

허니팟(Honey Pot)

- 사냥할 때 곰을 유인하기 위해 꿀단지를 설치해두는 것에서 유래
- 해커를 유인해서 정보를 얻거나 잡기 위해 유인하는 것
- 허니넷(HoneyNet): 허니팟을 포함한 네트워크

허니팟의 요건

1. 해커에게 쉽게 노출되어야 한다.
2. 쉽게 해킹이 가능한 것처럼 취약해 보여야 한다.
3. 시스템의 모든 구성 요소를 갖추고 있어야 한다.
4. 시스템을 통과하는 모든 패킷(통신)을 감시하고 있어야 한다.
5. 시스템에 접속하는 모든 사람에 대해 관리자에게 알려준다.