네트워크 보안

2023.07.17 하계 워크샵 3주차 – (1)

한림대학교 정보과학대학 씨애랑

(HALLYM SECURITY TEAM SHIELD)

목차

- 보안 관점에서의 OSI 7계층
- 각 계층별 보안 솔루션
- 방화벽 디자인
- NAT에서 발생 가능한 보안 취약점

목차

- 방화벽 운용 및 룰 관리
- IPS (Intrusion Prevention System)
- IDS (Intrusion Detection System)

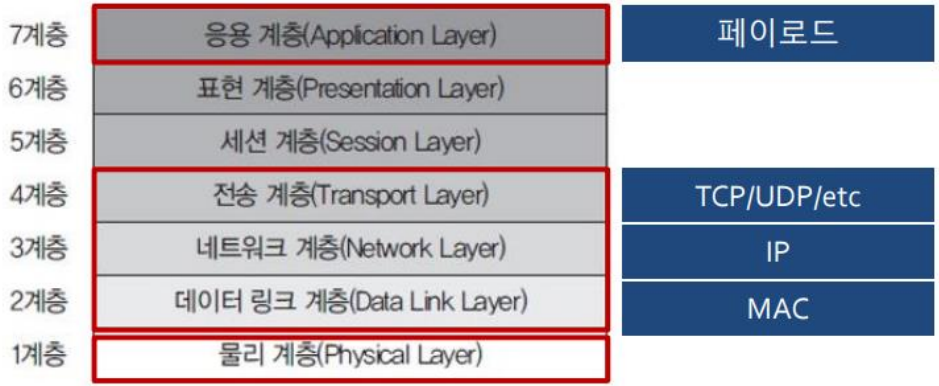
보안 관점에서의 OSI 7계층

보안 관점에서의 OSI 7계층

■ OSI 계층 (중요 계층별 역할)

□ L1 물리 계층의 경우, 신호 처리, Finger Printing, Jamming Solution 등 특정 분야에 대한 기반 지식이 필요함.

- 식별(Identification)을 위해 수집된 원격의 컴퓨팅 기기의 하드웨어 및 소프트웨어 정보



- NAT 모드 : 정책에 따라 IP를 변환하는 모드임. 기본적으로 사용하는 모드로,
  - 대부분 사설 IP를 공인 IP로 변환하는 목적으로 많이 사용함.
- Transparent 모드 : IP의 변환 없이 사용하는 모드임. 해당 모드는 NAT 장비와 백본 장비 사이에서 사용하거나,
  - 내부 기기들이 공인 IP를 사용할 때 사용함.

보안 관점에서의 OSI 7계층 - L2

■ L2는 데이터 링크 계층

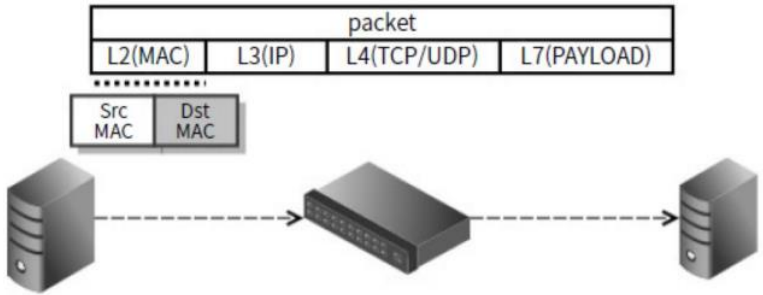
□ 패킷 발생 시, 패킷의 이더넷 부분만 확인하여 전송 라인을 결정함.

- 이더넷의 프레임 헤더에는 Source MAC 주소와 Destination MAC 주소가 포함됨.

■ L2와 가장 관계가 깊은 보안 시스템 : 방화벽

□ 일반적으로 L2 방화벽이라고 부르며, "Bridge Mode" or "Transparent Mode" 라고도 부름.

- 방화벽에 NAT 기능을 사용하지 않고 Transparent Mode 로 사용하게 되면,
  - 두 장비 사이에 위치하는 방화벽은 해당 장비 사이로 오가는 모든 트래픽을 제어할 수 있음.
  - 방화벽의 경우, 최소 두개 이상의 NIC (Network Interface Card) 카드가 필요.
  - L3 이상의 방화벽에서는 패킷이 들어오는 인터페이스(e.g., 공인 IP)와 나가는 인터페이스의 IP (e.g., 사설 IP) 대역이 다른 것이 보통이지만, L2 방화벽에서는 두 인터페이스 모두 같은 IP 대역 주소 대역을 사용할 수 있음.



보안 관점에서의 OSI 7계층 - L2

■ L2 방화벽의 장점

□ L2 방화벽을 설치 할 때, 네트워크 디자인을 바꾸지 않아도 됨.

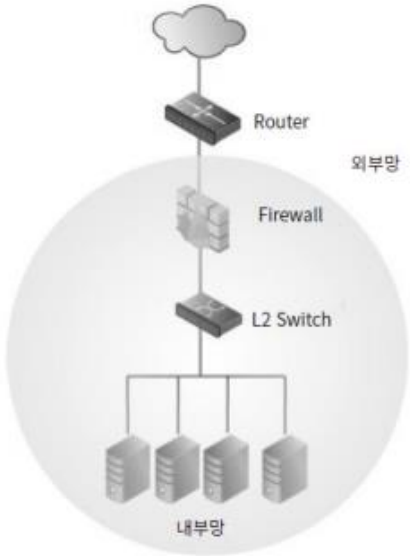
- 내부/외부망에서 방화벽이 보이지 않음.
- 방화벽을 공격할 수 있는 해킹 및 취약점으로부터 안전할 수 있음.

■ L2 방화벽의 단점

□ L2 방화벽은 동일한 네트워크 안에서만 가능하기 때문에,

- 다양한 네트워크 환경에 적용할 수 없음.
  - (e.g., 본사와 지사간의 통신을 위한 방화벽)

- 다양한 네트워크 환경에 방화벽을 구성하기 위해서는
  - 상위 레이어에서 작동하는 방화벽이 필요함.

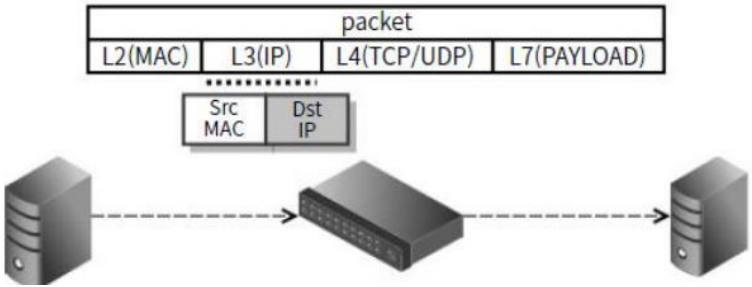


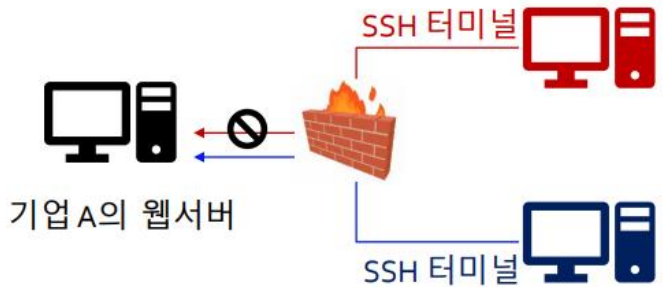
보안 관점에서의 OSI 7계층 - L3

■ L3 계층은 네트워크 계층

□ L3 계층에서는 하나의 네트워크 장비 (e.g., 방화벽)을 통해 여러 개의 네트워크 망을 구성할 수 있음.

- 하나의 장비로 여러 개의 네트워크 망을 구성하기 위해서는 NAT과 VLAN 기술이 필요함.



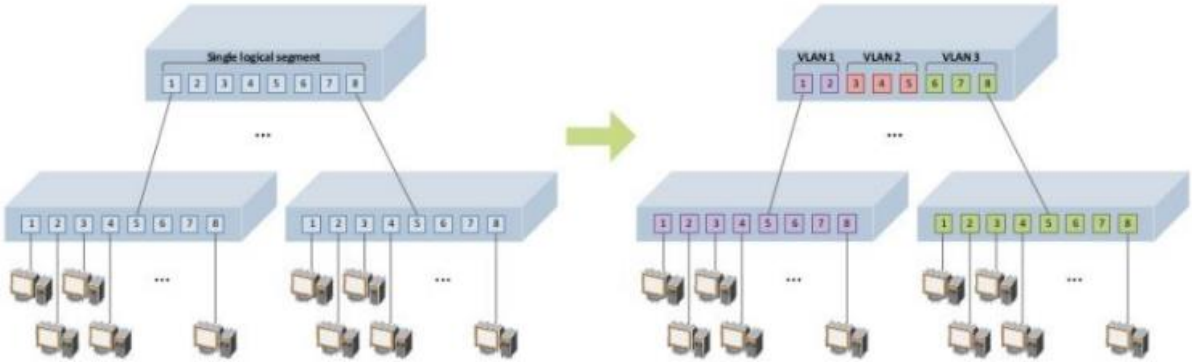


보안 관점에서의 OSI 7계층 - L3

■ L3 계층은 네트워크 계층

□ VLAN (Virtual Local Area Network)

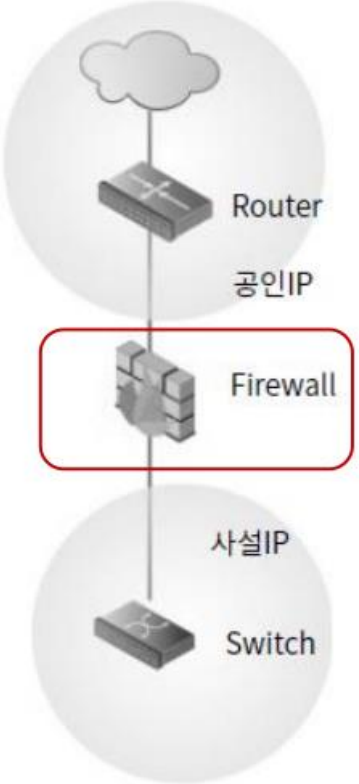
- 물리적 배치와 상관없이 논리적으로 LAN을 구성할 수 있는 기술
- 네트워크가 분리되기 때문에, 정책을 통해 허용된 대상만 접근 가능
- 기존 구성에서 큰 물리적인 변화가 없어도 VLAN을 통해 네트워크의 구조를 변경할 수 있음.



하나의 LAN segment에 연결된 단말의 개수가 많아질수록 망 성능의 저하 현상 발생 (Broadcast traffic의 증가)

Broadcast traffic은 각 VLAN 내에서만 전파되므로, 망 전체의 대역폭이 그만큼 절약되어 더 효율적으로 사용될 수 있다.

보안 관점에서의 OSI 7계층 - L3



■ L3 방화벽의 장점

□ L2 방화벽에서는 접근 제어의 한계가 존재함
- 인사팀, 개발팀 모두 웹서버에 터미널 접근 허용 or 불허용

□ L3 방화벽에서는 NAT과 VLAN을 통해 다양한 설정의 접근제어가 가능함

■ L3 방화벽의 단점

□ L3 방화벽을 설치할 때, 일반적으로 네트워크 디자인을 바꾸어야 할 수 도 있음.
- Transparent 하지 않으므로 내부망 혹은 외부망에서 방화벽의 존재를 유추 가능함.
  - 공격자가 방화벽을 공격할 수 있는 취약점을 활용 할 수 있음.

[NAT 모드의 방화벽]

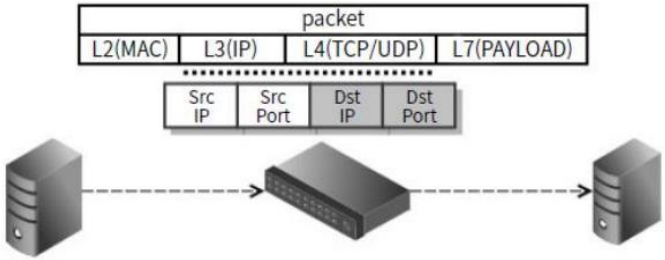
* 방화벽에서도 L3를 제어할 수 있지만, 라우터나 L3 스위치에서도 제어할 수 있음.

보안 관점에서의 OSI 7계층 - L4

■ L4는 전송 계층임.

□ TCP/IP 관점에서 TCP는 L4 계층이고, IP는 L3 계층임.

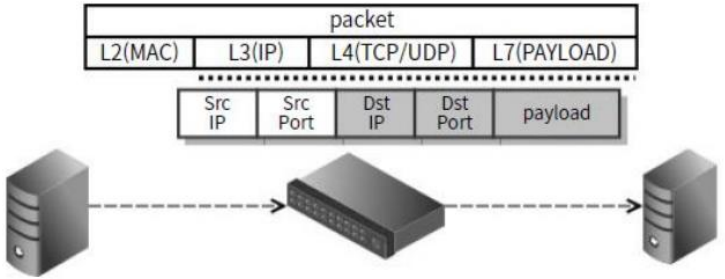
- L4에서는 패킷을 포트 수준까지 확인하고 처리가 가능함.



□ L5는 세션 계층, L6는 표현 계층, 그리고 L7는 응용 계층에 해당함.

- 요즘에는 L5, 6, 7 을 통틀어 L7로 부르기도 함

주의 위의 용어는 일하는 업무환경에 따라 달라질 수 있음



각 계층별 보안 솔루션

각 계층별 보안 솔루션

■ 계층 별 역할

계층	하는 일	참조하는 곳
L2	MAC정보를 보고 스위칭을 수행함	MAC 테이블
L3	IP 주소 정보를 보고 스위칭을 수행함	라우팅 테이블
L4	IP 주소 + 포트를 보고 스위칭을 수행함	세션 또는 연결
L7	Application data를 보고 스위칭을 수행함	Contents

각 계층별 보안 솔루션

■ Anti-DDoS

- □ DDoS 방어 장비를 인라인 모드로 디자인 하는 경우, 네트워크 맨 상단에 설치함.
- □ 전통적인 DDoS 장비는 L4 계층까지 커버했지만, 최근 장비들은 L7 계층까지 커버할 수 있음.

■ 방화벽

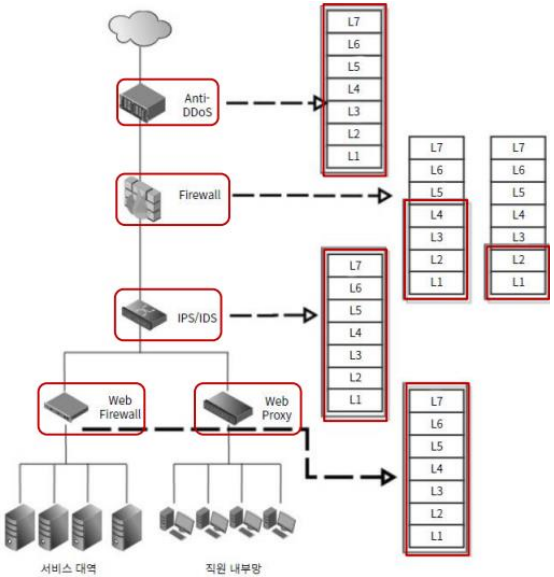
- □ NAT 모드로 설치할 경우, L4계층까지 커버할 수 있음.
- □ TP 모드로 설치할 경우, L2계층까지 커버할 수 있음.
  - 최근 장비들은 L7계층까지 커버하기도 함.

■ IPS/IDS (Intrusion Prevention System/Intrusion Detection System)

- □ 페이로드를 읽어서 패킷을 완전히 보는 것이므로 L7 계층까지 커버함.

■ 웹 방화벽 / 웹 프록시

- □ 웹 방화벽은 IPS의 역할과 비슷하며 L7까지 커버
- □ 웹 프록시
  - 인터넷에 접속할 때, 악성 사이트에 접근할 수 없도록 위험한 사이트를 차단하는 역할
    → 패킷의 페이로드를 보기 위해서 L7 계층을 커버 해야함.



방화벽 디자인

방화벽 디자인 - 1세대 방화벽

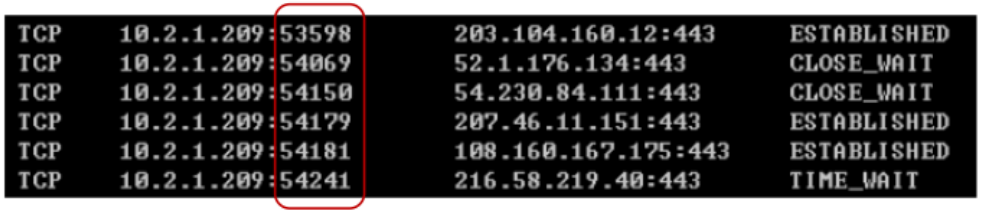
- **네트워크 방화벽 : 여러 대의 PC와 서버를 커버함.**
- **소프트웨어 기반의 방화벽 : 설치된 host PC만을 보호함.**

- **패킷 필터링 기반의 1세대 방화벽**

src IP	dst IP	scr Port	dst Port	Control
any	1.1.1.1	any	80	permit

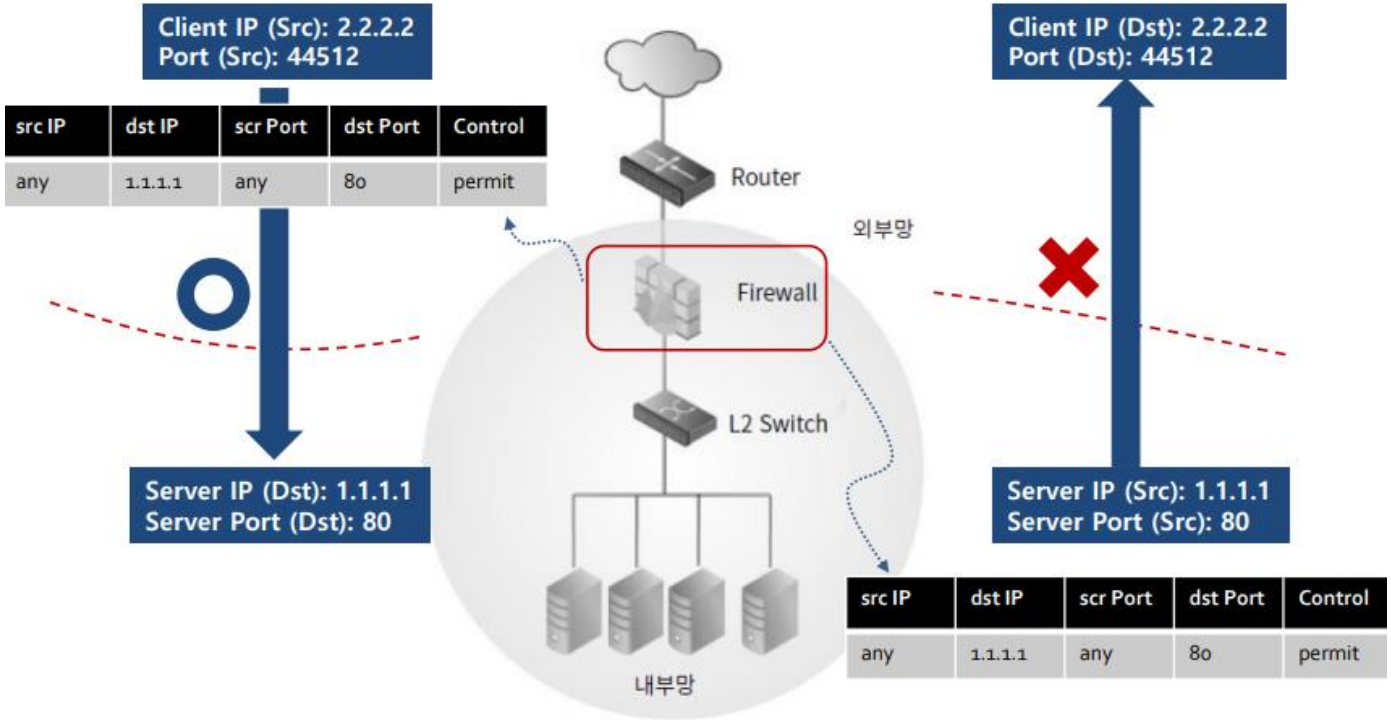
- 80번 포트를 열어 두고 있음.
- 80번 포트에 대한 접근을 허용함 (80은 HTTP 포트임, 웹 서비스)

- 제대로 작동할까 ? 제대로 동작하지 않음 !
  - 패킷 필터링 기반의 방화벽에서는 모든 패킷에 대해 현재 가진 룰을 참고해서 통신을 허가 할지 차단할지를 결정함.
    - 따라서, 해당 커넥션에 대해 되돌아 나가는 통신도 허용해야 함. (e.g., TCP handshake)



방화벽 디자인 - 1세대 방화벽

■ 패킷 필터링 기반의 1세대 방화벽



방화벽 디자인

■ 패킷 필터링 기반의 1세대 방화벽

□ 돌아오는 패킷도 처리하기 위해서 새로운 룰을 설정함.

□ 즉, 웹서비스를 위해 80번 포트를 방화벽에서 열 때, 되돌아 나가는 포트에 대해 많은 포트들을 열어줘야 함.

- 룰 관리 이슈 (룰이 추가됨), 포트 개방에 관련 이슈 (많은 포트를 여는 문제점)

src IP	dst IP	scr Port	dst Port	Control
any	1.1.1.1	any	80	Permit
1.1.1.1	any	80	any	permit

■ 2세대 방화벽에서는 Stateful Inspection을 수행함.

□ Stateful Inspection이란?

- TCP 접속 시, 방화벽에서 패킷의 payload를 보면서 3way handshake의 state를 추적하여 rule 자동적으로 추가함.
  - (패킷 간의 Connection검증)

방화벽 디자인

■ **Stateful Inspection 예제**

src IP	dst IP	scr Port	dst Port	Control
any	1.1.1.1	any	80	permit

만약 dst port가 44512, src IP가 2.2.2.2 라면, 자동적으로 룰이 추가됨

src IP	dst IP	scr Port	dst Port	Control
any	1.1.1.1	any	80	permit
1.1.1.1	2.2.2.2	80	44512	permit

Connection 종료 시, 룰이 제거됨

src IP	dst IP	scr Port	dst Port	Control
any	1.1.1.1	any	80	permit

방화벽 디자인

■ Stateful Inspection 의 장점

□ Response 패킷에 대한 룰을 불필요하게 작성할 필요가 없음
- 보안성이 향상 되는 것 뿐만 아니라, 룰 관리도 쉬워짐.

□ Stateful inspection 이 동작하는 동안 패킷의 checksum(e.g., MAC)도 계산하므로,
- checksum이 잘못된 패킷을 폐기할 수 있음.
  - 불량 패킷 또는 DDoS 공격이라고 판단하고 접속을 종료

■ 3세대 방화벽은 L7 방화벽 또는 애플리케이션 방화벽이라고 함.

□ 2세대 방화벽은 차단 룰을 만들고, 커넥션을 검증

■ L7 방화벽은 실제 패킷의 내용을 검사해서 단순한 IP Address / Port Number 조사 뿐만 아니라 어떤 애플리케이션과 통신하고 있는지 파악할 수 있음.

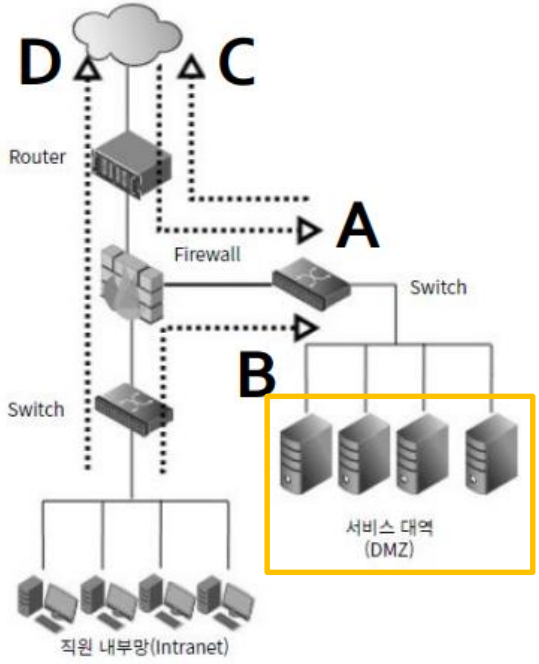
□ 예를 들면, 기존 방화벽은 웹 검색을 위해 사용되는 80/443을 전부 허용 또는 차단과 같이, 양자 택일을 수행
- 하지만, L7 방화벽은 페이스북은 차단, 인스타그램은 허용 등의 룰을 만들 수 있음.

방화벽 디자인 - 방화벽 배치

■ 일반적인 방화벽 구성도

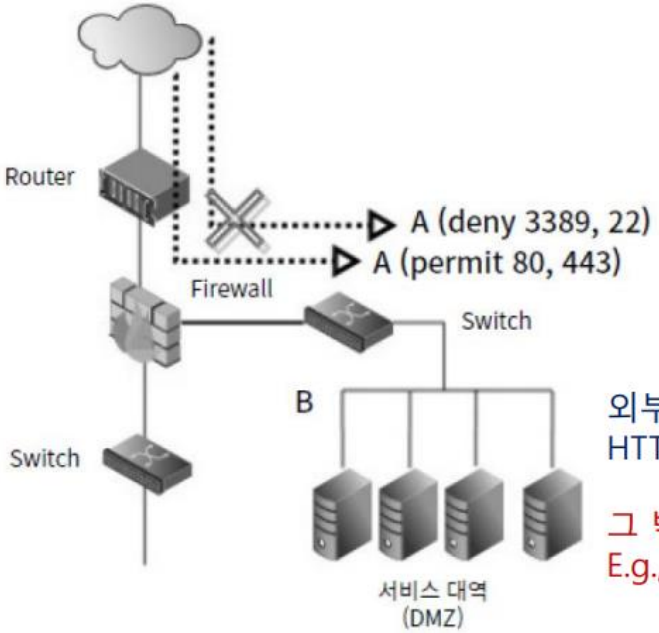
□ 네트워크에서 중립 지역을 뜻하는 DMZ (demilitarized zone)는

- 외부에 서비스를 제공해야 하는 상황에서 내부 자원을 보호하기 위해 내부 네트워크와 분리시킨 공간.



방화벽 디자인 - 방화벽 배치

■ A 구간 : 외부에서 서버로 접속

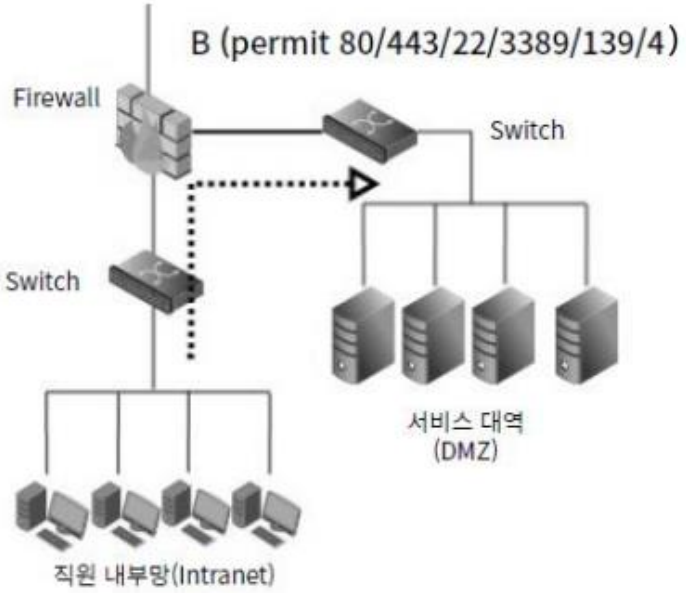


외부로 공개된 웹서버가 존재한다면,
HTTP (80), HTTPS (443) 포트 허용

그 밖의 모든 포트는 차단!
E.g., RDP (3389), SSH (22)

방화벽 디자인 - 방화벽 배치

■ B 구간 : 내부망에서 서버로 접속

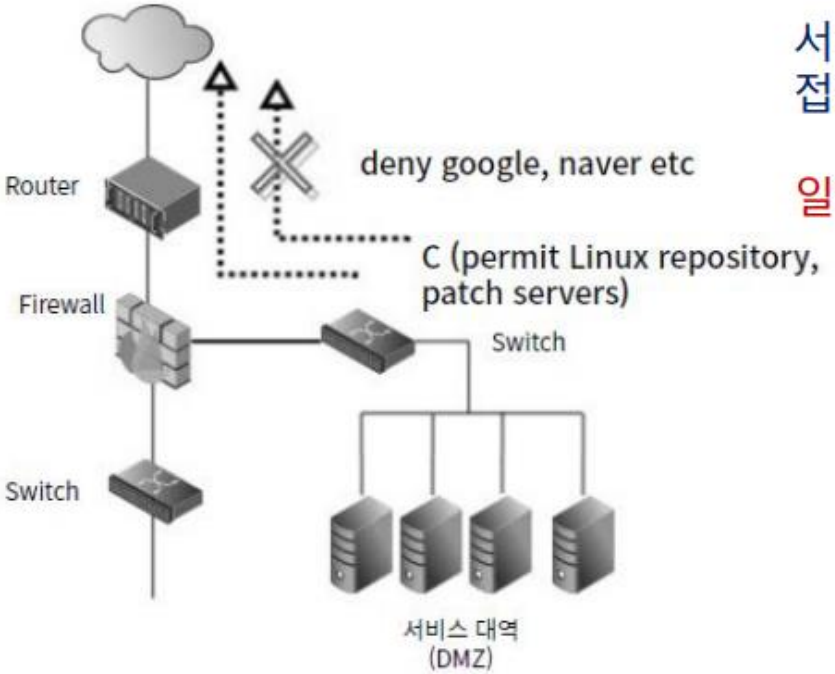


내부망에 존재하는 엔지니어들을 위해 다양한 제어 포트를 열어 둠

E.g., HTTP (80), HTTPS (443), SSH (22), RDP (3389) 등

방화벽 디자인 - 방화벽 배치

■ C 구간 : 서버에서 외부망 접속

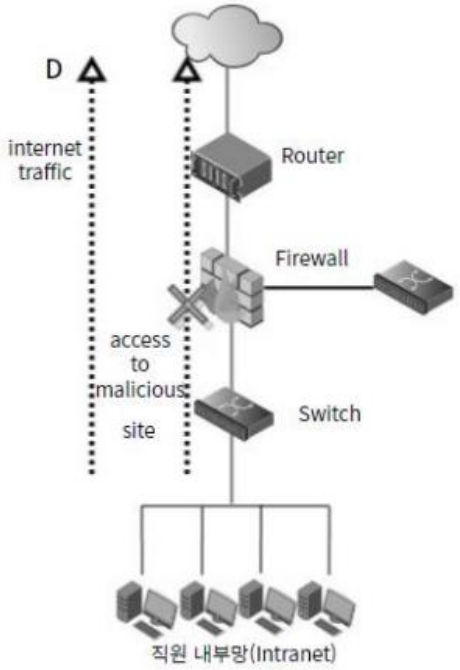


서버 패치를 위해 Linux Repository 접근 허용!

일반 사이트 접속 불허용!

방화벽 디자인 - 방화벽 배치

■ D 구간 : 내부망에서 외부망으로 접속



파일 유출 방지를 위해 구글 드라이브, 네이버 드라이브 불허용!

악성코드 감염 방지를 위해 악성 사이트 접근 불허용

NAT에서 발생 가능한 보안 취약점

NAT에서 발생 가능한 보안 취약점

■ NAT (Network AddressTranslation)

■ IP 주소

□ 공인 IP 주소 (public IP address)

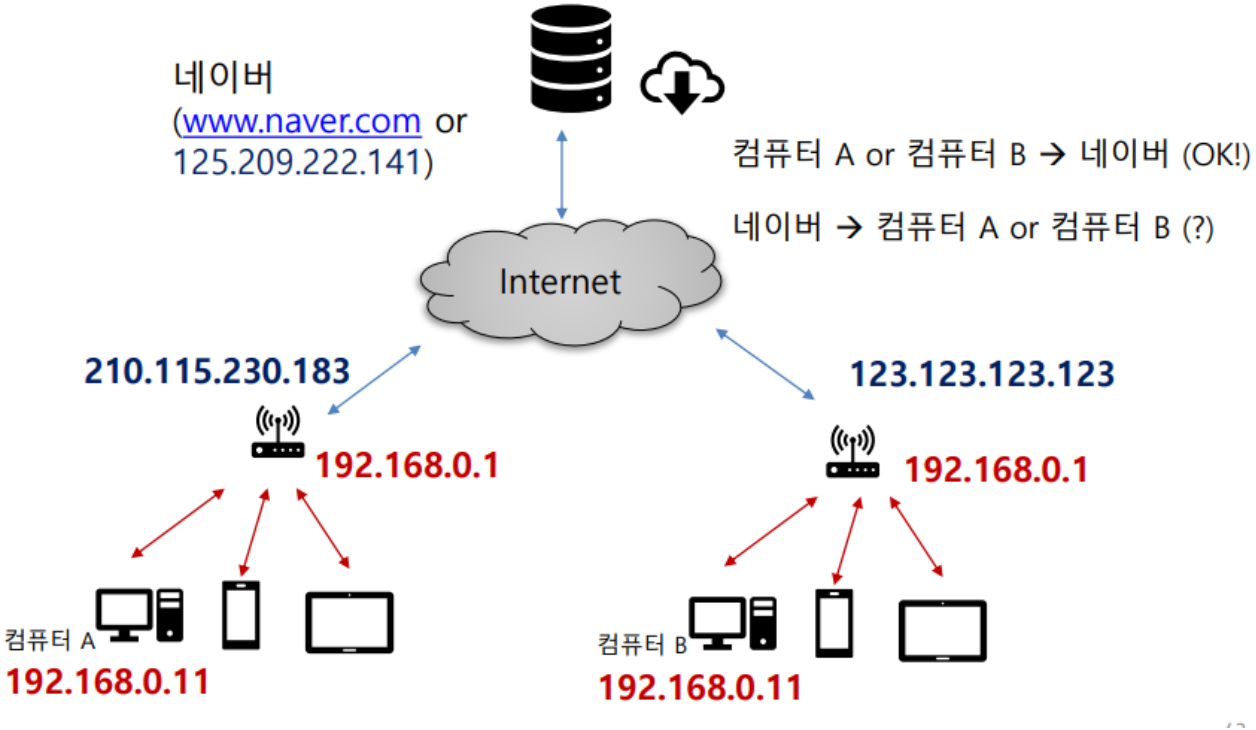
- 전 세계적으로 고유한 주소 (예: 강원도 춘천시 한림대학교 공학관 1305호)

□ 사설 IP 주소 (private IP address)

- 주소가 고유하지 않음 (예: 1305 호)
- 사용 예 : 공유기에 공인 IP 할당 후, 공유기에 연결된 다수의 컴퓨터에 사설 IP를 할당
- RFC 1918에 의해 정의된 사설 IP 주소 범위
  - 10.0.0.0 ~ 10.255.255.255: 주소 개수 16,777,216 개
  - 172.16.0.0 ~ 172.31.255.255: 주소 개수 1,048,576개

NAT에서 발생 가능한 보안 취약점

■ 공인 IP 주소 vs. 사설 IP 주소

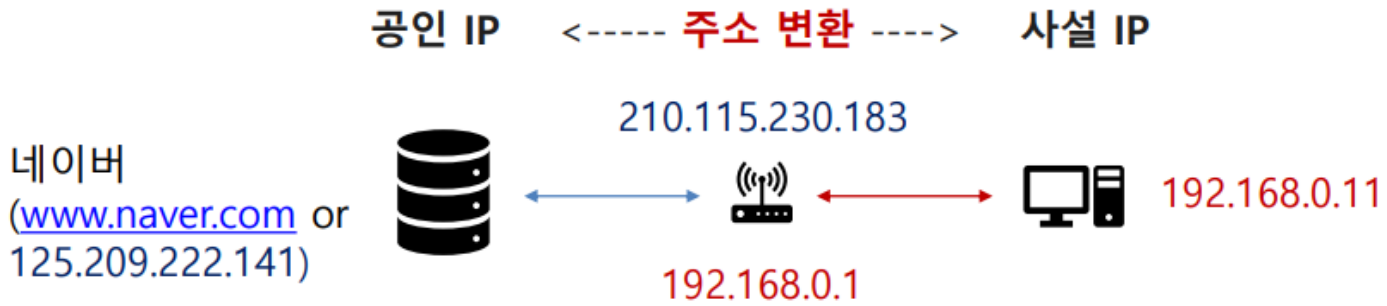


NAT에서 발생 가능한 보안 취약점

■ NAT

□ IP 패킷의 TCP/UDP 포트 번호와 소스 및 목적지의 IP 주소 등을 재기록 하면서

- 라우터를 통해 네트워크 트래픽을 주고 받는 기술.
  - 즉, 공인 IP 주소를 기반으로 내부 네트워크에 1개 이상의 IP 주소를 할당하여 IP 주소 및 포트 번호를 매핑, 변환해주는 기술



NAT에서 발생 가능한 보안 취약점

■ NAT은 DNAT와 SNAT 2가지로 구성되어 있음.

□ DNAT (Destination Network AddressTranslation)

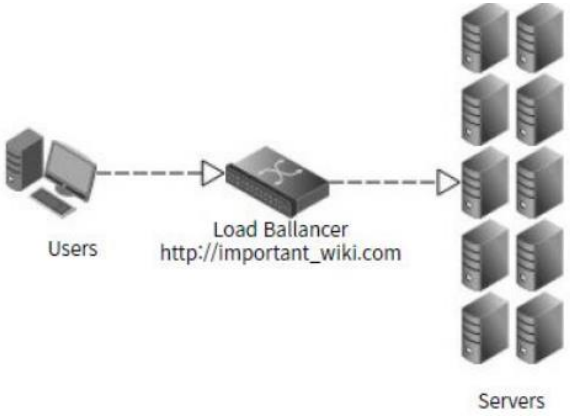
- 외부에서 방화벽 안쪽으로 들어올 때, 네트워크 주소가 변환되는 것
- 예) 회사의 웹서버가 192.168.1.3에 있을 경우, 외부의 일반 사용자는 해당 IP로 접근이 어려움.
- DNAT 이용 시, 공인 IP주소 A.A.A.A를 통해 외부의 일반 사용자가 접근하면, NAT 테이블을 참조해서 해당 내부 IP주소 192.168.1.3 으로 매핑을 확인하고 커넥션을 연결

□ SNAT (Source Network Address Translation)

- 외부와의 연결을 위해, 내부에서 외부로 접속을 수행하게 될 경우 네트워크 주소가 변환되는 것

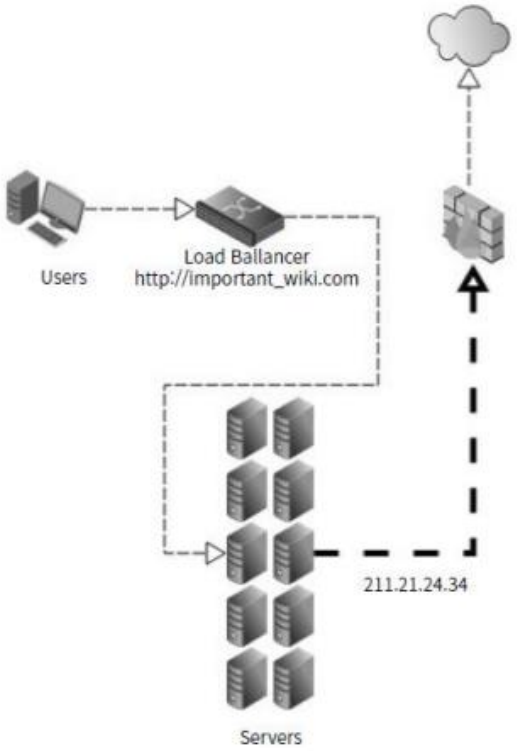
□ 보안 취약점 예시

- 어떤 회사는 효율적인 서비스 제공을 위해 10개의 서버를 운용하고 있음.
- 10개의 서버는 L4 스위치에 의해 서버 리소스에 따라 로드 밸런스 되고 있음



NAT에서 발생 가능한 보안 취약점

■ 보안 취약점 예시



■ 관리자의 실수 혹은 내부 IP 주소 부족으로 10개의 서버에 SNAT을 통해 211.21.24.34 라는 같은 외부 주소를 할당함.

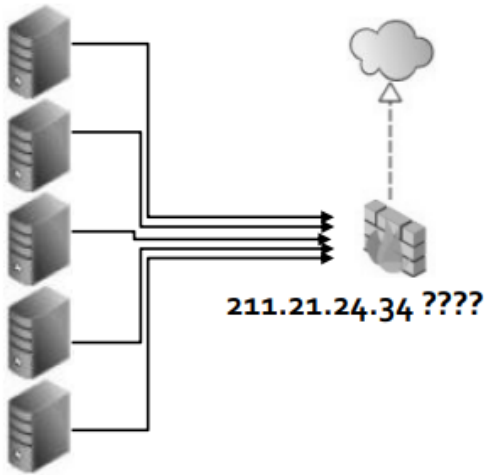
■ 10개의 서버 중 1대가 감염됨.

■ 211.21.24.34 주소로 악의적이 파일이 배포되기 시작함.

■ 관리자는 10개의 서버의 로그를 모두 조사해야 함.

NAT에서 발생 가능한 보안 취약점

■ 보안 취약점 예시



■ 악의적인 공격 트래픽 및 해킹을 당했다는 의심을 가지는 IP 주소에 대해 확실한 조사가 필요한 상황

■ 만약 해당 211.21.24.34 IP 주소를 나만 할당한 것이 아닌, 다른 부서의 네트워크 담당자도 할당한 경우

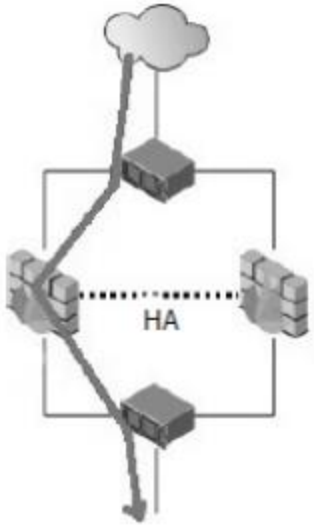
- 조사할 서버의 수가 10개 이상

■ 또한, 아웃 바운드가 열린 상태에서 계속 다른 서버로 침투할 가능성이 있기 때문에, 침해의 원인이 되는 서버를 찾기가 더 어려워 짐

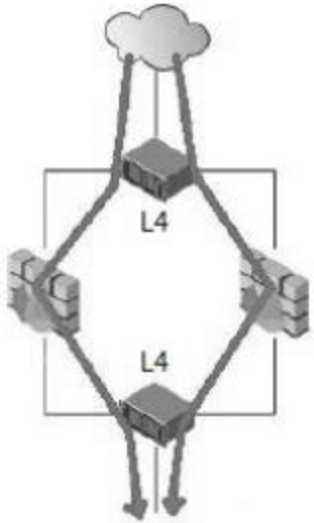
방화벽 운용 및 룰 관리

방화벽 운용 및 룰 관리

- **High Availability 는 2대의 방화벽을 통해,1개 의 방화벽에 장애가 생겼을 경우를 대비하는 것임.**
  - 한대는 온라인 상태, 한대는 대기/레디 상태 (ActiveStandby)
  - 두개는 항상 온라인 상태 (Active-Active)



Active-Standby



Active-Active

방화벽 운용 및 룰 관리

■ Active-Standby (AS)

□ 1번 방화벽으로 트래픽이 흐르다가, 1번 방화벽에 문제가 생길 경우,

- 2번 방화벽으로 전환하여 네트워크 흐름에 문제가 없도록 구성
  - 다만, 1번 방화벽과 2번 방화벽은 실질적으로 방화벽의 상태가 동일해야 하기 때문에 설정 동기화 과정이 필수적임.

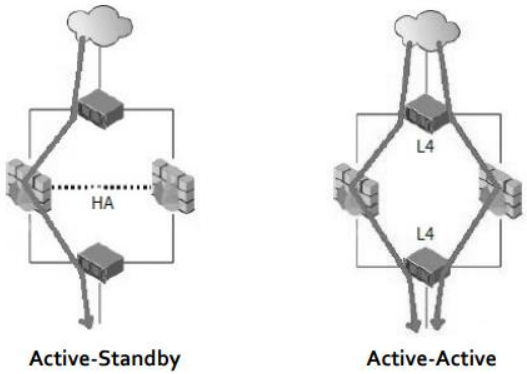
■ Active-Active (AA)

□ L4 스위치가 두개의 방화벽에 연결되어 있어서,

- L4 스위치가 트래픽을 적절히 분배해서 좀 더 여유 있는 방화벽 쪽으로 트래픽을 전달함.

□ AS와는 다른 두개를 통해 High Availability 과 안정성을 최우선 목표로 설정.

- 다만, HA를 정교하게 디자인 할수록 2개 이사의 장비가 필요하기 때문에, 예산이 많이 요구됨



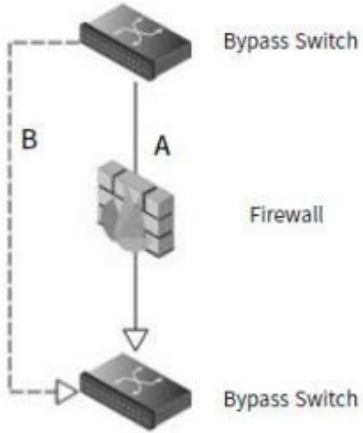
방화벽 운용 및 룰 관리

■ 바이패스 스위치

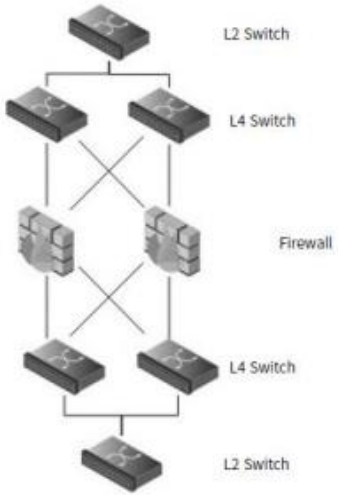
□ 방화벽 장비에 장애가 생겼을 경우, 우회경로를 만들어 주는 방법 (네트워크 전체가 멈추는 것을 방지)

■ Full Mesh

□ 네트워크 장비를 2대 이상 준비한 후, 모두 연결



바이패스 스위치 방식

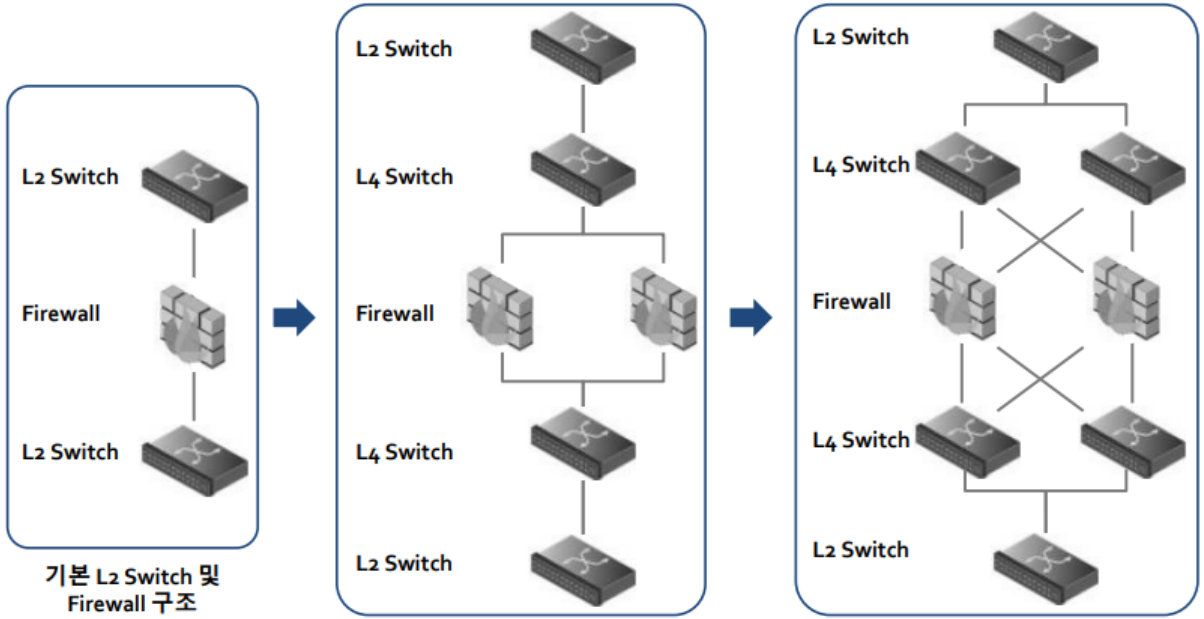


Full Mesh 방식

방화벽 운용 및 룰 관리

■ Full Mesh

□ 네트워크 장비를 2대 이상 준비한 후, 모두 연결



방화벽 운용 및 룰 관리

■ 방화벽 룰 관리

- □ 오래된 룰은 정기적으로 확인 후, 필요 없는 경우 해당 룰을 지워 주어야 함.
- □ 룰이 겹치지않도록 튜닝하는 것도 필요함

Access	Protocol	scr.port	dst.port	Direction
Permit	tcp	any	80	any
Permit	tcp	any	443	any
Permit	tcp	any	3389	any
...				
Permit	any	any	any	any

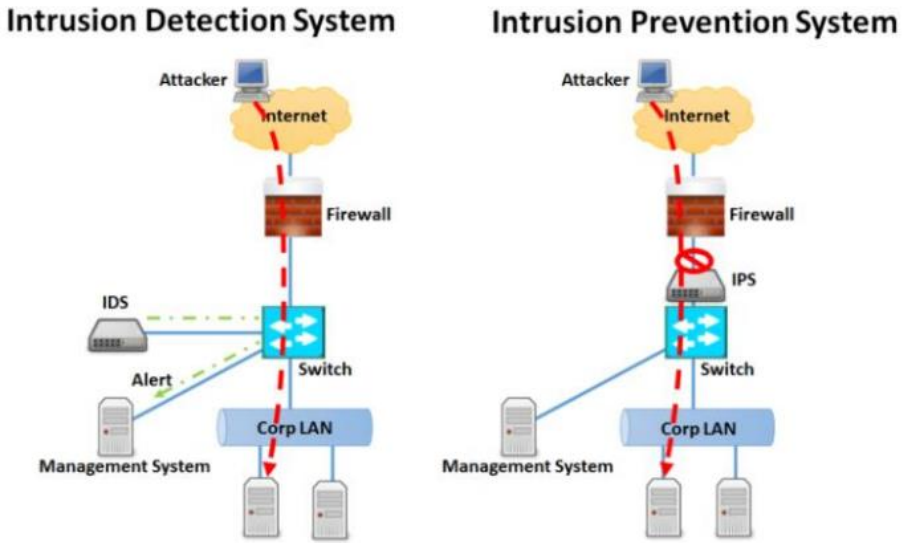
IPS (INTRUSION PREVENTION SYSTEM)

IPS (Intrusion Prevention System)

■ **IDS vs. IPS**

- □ Intrusion Detection System
- □ Intrusion Prevention System

■ **IDS는 공격 패킷에 대한 블록 기능은 존재하지 않고, 공격 탐지를 위한 로깅만 수행하는 경우가 많음.**



IPS (Intrusion Prevention System)

- IDS vs. IPS

	IPS	IDS
System Type	Active (monitor & automatically defend) and/ or passive	Passive (monitor and Notify)
Detection mechanism	Statistical anomaly based detection Signature detection	Statistical anomaly based detection Signature detection
Placement	Inline to data communication	Out of band from data communication
Anomaly response	Drop, alert or clean malicious traffic	Sends alarm/alert of detecting malicious traffic
Network performance impact	Slows down network performance due to delay caused by inline IPS processing	Does not impact network performance due to non-line deployment of IDS.

IPS (Intrusion Prevention System)

■ 방화벽에 L7 기능이 없던 시절...

□ 악성코드나 Exploit 공격코드의 페이로드를 확인하기 위해 IDS를 방화벽과 함께 구축하는 경우가 많았음.

- 즉, IDS로 패킷을 모니터링 하다가, 의심되는 내용이 발견될 경우 추가적인 분석 과정을 거쳐서 방화벽 Rule을 세팅함.
- 보안 관리자들에 업무량 증가 및 불편함을 야기함!

- 취약점 공격 또는 익스플로잇 (exploit)이란 컴퓨터의 소프트웨어나 하드웨어 및 컴퓨터 관련 전자 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 만들어진 절차나 일련의 명령, 스크립트, 프로그램 또는 특정한 데이터 조각을 말하며, 이러한 것들을 사용한 공격 행위를 이르기도 함.

■ IPS 에서 제공되어야 하는 기능

□ L7 계층을 커버할 수 있어야 함.

□ DDoS를 막을 수 있어야 함.

□ Traffic을 학습할 수 있어야 함.

IPS 장비

IPS (Intrusion Prevention System)

■ IPS의 필요성

□ L4 방화벽으로 공격을 차단하는 것에는 한계가 존 재함

- 따라서, 방화벽에도 IDS에서 패킷을 모니터링 하는 것과 같이 침입탐지 패턴이 있어야 함.
  - 즉, 인라인으로 연결된 네트워크 보안 장비로도 L7 계층 을 커버해야 함.
  - 방화벽에 IDS 기능을 넣으려는 시도에서 IPS가 발전하게 됨.

□ IPS가 L7 계층의 데이터를 이용하여 공격 탐지 및 차단이 가능함.

■ Signature 기반 공격 탐지의 한계

□ Signature 기반 탐지

- 악성 행위에는 일정한 패턴(Signature)이 존재하고 이러한 패턴 을 탐지 룰에 추가함으로써 공격을 탐지
- 하지만, Signature 기반 탐지는 Unknown 공격을 탐지 못함.
  - Signature 기반 탐지의 한계를 극복하기 위해 Anomaly 기반 공격 탐지가 설계됨.

□ Anomaly 기반 공격 탐지

- Anomaly 기반 공격 탐지란? 일반적인 상황의 트래픽을 학습해 두었다가, 비정상적인 트래픽이 발생하면 공격으로 간주함.
  - E.g., 평소에 IP 주소당 최대 10Mbps가 발생하는데, 어느 날 20Mbps를 발생시키는 IP주소가 생긴다면, 이상 행위로 간주함.
    - 하지만, Anomaly 기반 공격 탐지는 오탐이 존재함.

IPS (Intrusion Prevention System)

■ IPS 디자인의 예

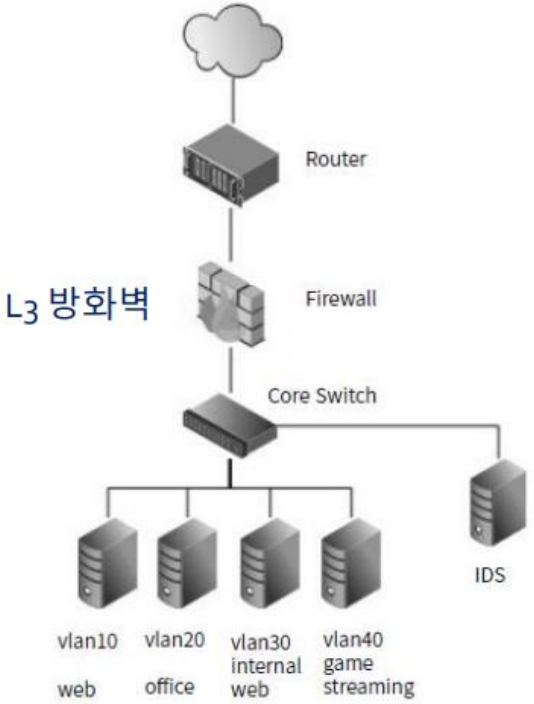
□ vlan10 : 외부에서 회사에 접근하는 서버 (e.g., 웹서비스)

□ vlan20 : 사내직원들이 사용하는 통신 구역

□ vlan30 : 본사/지사/협력관계를 위한 통신 구역
- (일반인에게는 오픈되지 않음)

□ Vlan40 : 회사가 제공하는 다른 서비스
- 외부에서 접근이 가능함.

- 공격으로 부터 안전할까?
  - 먼저 위협을 정의해야 함.

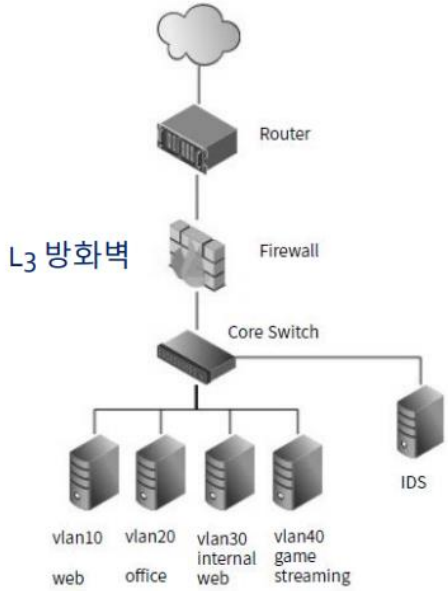


IPS (Intrusion Prevention System)

■ IPS의 위치

□ 1. 서버를 통해 발생하는 위협 (e.g., vlan10)
- 웹서버는 모든 사용자가 접근 가능하므로 공격에 노출 되어 있음.
- L3 방화벽으로는 일반 사용자의 공격을 막을 수 없음.
  - 알려지지 않은 IP로 공격을 할 수 있음.
- 따라서, L7 계층의 IPS 혹은 L7 방화벽이 필요함.

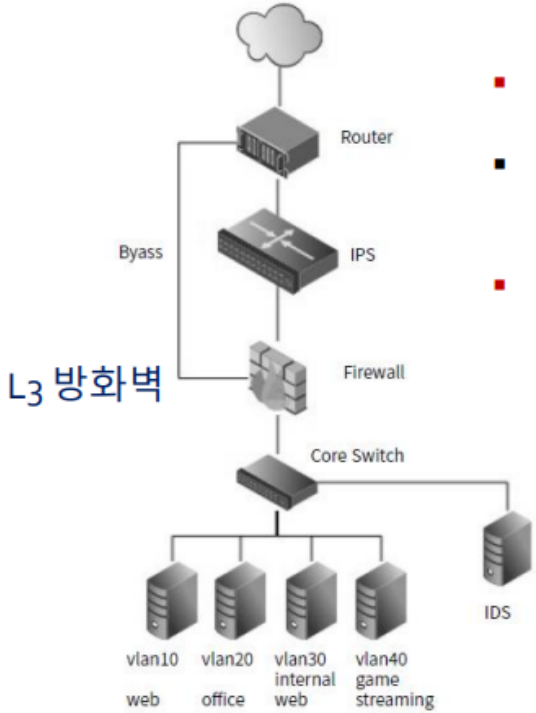
□ 2. 직원들의 사내망을 통해 발생하는 위협 (e.g., vlan20)
- vlan10 서버의 SSH/RDP 접근이 vlan20에서 가능할 경우,
  - 공격자는 vlan20의 PC를 감염시키는 시도를 할 수 있음.
- 스팸 메일, 악성 USB등을 통해 vlan20구역을 감염시킬 수 있음.
- L3 방화벽으로는 한계가 있음.
  - 허용된 접근으로 이루어진 공격일 가능성이 존재함.
    - 따라서, L7 계층의 IPS 혹은 L7 방화벽이 필요함.



□ 3. DDoS 공격으로부터 발생하는 위협
- 웹서비스를 vlan10구역에서 제공하고 있으므로, 해당 서비스를 보호하기 위한 DDoS대응이 필요함.

IPS (Intrusion Prevention System)

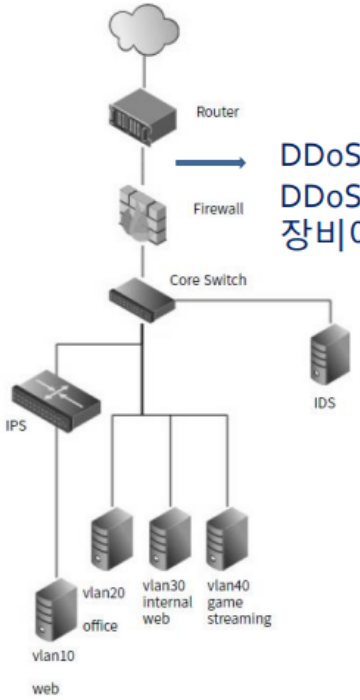
■ DDoS를 방어하기 위한 IPS 위치



- IPS를 방화벽위에 위치시키는 것이 좋음
- 많은 트래픽이 발생하여, L3방화벽이 다운될 수 있음
- 또한, IPS 장애를 대비하여 Bypass 라인을 만들면 좋음

IPS (Intrusion Prevention System)

■ 웹 서버를 지키는 IPS 위치

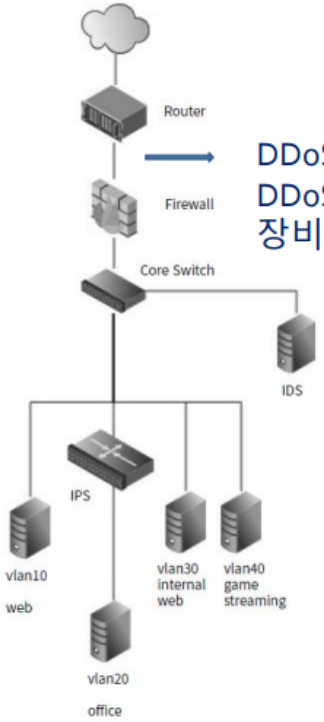


DDoS공격은 전문
DDoS 공격 대응
장비에게 위임

- 웹서버가 위치한 vlan10구역에 IPS를 위치시킴

IPS (Intrusion Prevention System)

■ 직원들의 PC를 지키는 IPS 위치



DDoS공격은 전문
DDoS 공격 대응
장비에게 위임

- 직원 PC가 위치한 vlan20구역에 IPS를 위치시킴

IPS (Intrusion Prevention System)

■ IPS의 현실

□ IPS의 많은 기능들이 L7 방화벽에서 수행됨.

□ DDoS 공격 탐지도 전문 DDoS 탐지 장비들이 대체 하고 있음.

□ URL 차단 등은 웹 필터 기반 애플리케이션으로 대체 가능함.

□ 그러나, 아직도 기업의 상황에 따라 IPS를 사용하는 곳이 있음.

- 필요없는 장비는 없으며, 현실 상황에 맞게 사용하면 됨.

IDS (INTRUSION DETECTION SYSTEM)

IDS (Intrusion Detection System)

■ IDS의 종류

□ NIDS (Network-based IDS)
- 네트워크 인프라를 관리할 수 있는 위치에서 작동하는 IDS

□ HIDS (Host-based IDS)
- Host에서 작동하며 Host의 상황을 관리하는 IDS

	장점	단점
NIDS	모든 호스트에 개별적으로 설치하지 않아도 되고, 네트워크 전체를 한군데서 분석 가능	IDS를 경유한 공격만 확인 가능하며, 암호화된 트래픽을 통해 서버 로컬에서 침해당한 건은 알 수 없음
HIDS	Host별 상세 분석이 가능하며, 사용자 단위 분석 가능	개별로 설치 및 관리해야 하며, Host 감염 시 제대로 동작하지 않을 수 있음

IDS (Intrusion Detection System)

■ IDS의 패킷 모니터링

□ NIDS는 탐지 위주의 정책을 이용하므로 네트워크 사이에 인라인으로 끼어들어가지 않음.

- 따라서 장애를 예방하기 위한 이중화 구성은 필수사항이 아님.
  - NIDS의 장애가 발생할 경우, 네트워크 로그의 연속적인 저장이 필요하다면 NIDS도 Backup 장비를 통한 이중화 구성 필요

□ NIDS에 필요한 것은 분석에 필요한 데이터

- NIDS의 경우 전체 네트워크 패킷이 필요
  - 보안 모니터링이 필요한 네트워크 패킷들을 IDS로 전송
    - Cisco 에서는 트래픽 전송을 SPAN (Switched Port Analyzer)라고 부르며, 대부분의 스위치가 SPAN (혹은 포트 미러링)을 제공
  - HIDS의 경우 호스트 네트워크 패킷, 시스템 로그 등

■ 포트 미러링

□ 스위치 환경에서 포트 미러링을 통해 스니핑 (패킷을 엿듣는 행위)를 제공함.

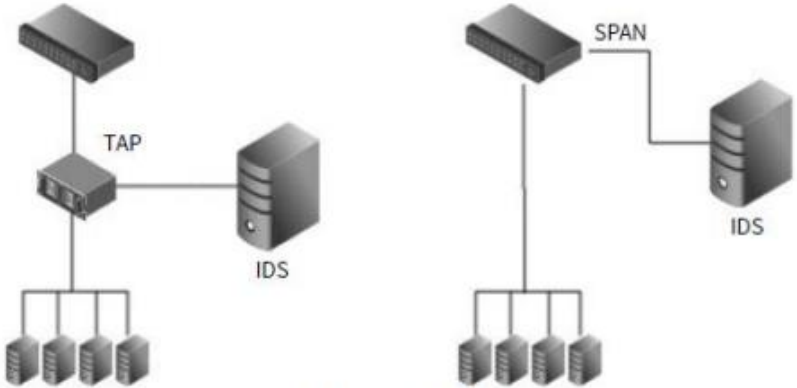
- 스위치 환경에서 패킷을 분석하기 위해 스위치 포트에 스니퍼를 연결함.
- 스위치가 포트 미러링을 지원해야 하고, 스니퍼를 연결하기 위한 포트가 남아있어야 함.

IDS (Intrusion Detection System)

■ 네트워크 TAP을 통한 모니터링

- □ 스위치의 SPAN (or 포트 미러링)에 과부하가 걸릴 경우
  - 모니터링해야 할 패킷이 유실될 수 있음.
  - 스위치 전체가 다운될 수도 있음.
- □ 따라서, 네트워크 TAP 장비를 사용할 수 도 있음.
  - 원활한 네트워크 트래픽 복사를 위해서 네트워크 TAP장비의 스펙을 확인할 필요가 있음.

네트워크 TAP장비



TAP vs SPAN

IDS (Intrusion Detection System)

■ 패킷 유실 관점에서는 SPAN 보다는 TAP이 IDS를 구축에 용이할 수 있음.

□ 하지만, 네트워크 상황에 따라 TAP구성을 잘못하면,

- NAT 때문에 트래픽이 제대로 보이지 않는 현상이 나타날 수 있음.

■ IDS의 위치

□ IDS의 위치를 디자인하기 위해서는 모니터링이 필요한 자산 (중요한 자산)을 정의해야 함.

□ 일반적으로 센서는 아래와 같은 상황에 설치가 고려됨.

- 사무실 네트워크가 분리되는 지점
- 연구팀/개발팀 네트워크가 분리되는 지점
- 외부 직원들의 접근 영역이 분리되는 지점
- 무선 인터넷이 분리되는 지점

THANK YOU