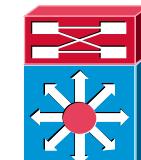
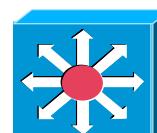
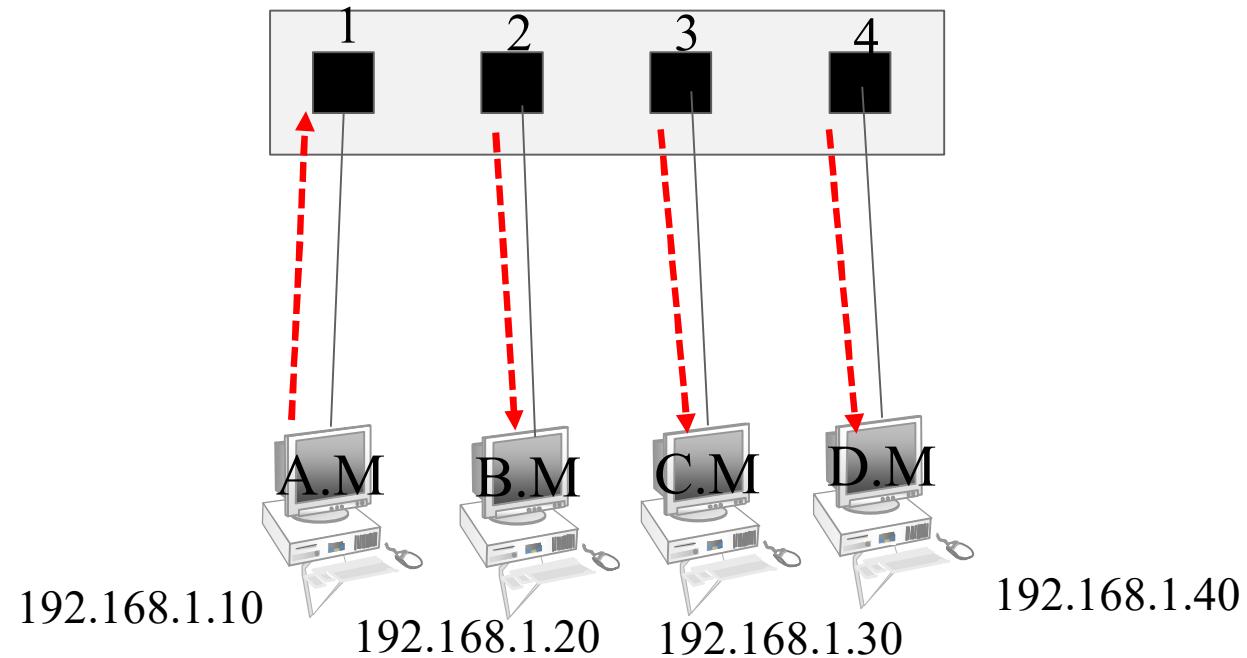


Multilayer Switch(다계층스위치)

구분	L2 Switch	L3 Switch	L4 Switch	L7 Switch
OSI 7계층	2계층 (MAC Address)	3계층 (Network 관리)	4계층 (Session 관리)	7계층 (Content 관리)
기능	Switching - Learning - Forwarding - Filtering	Switching Routing	L3 Switch Load Balance	L4 Switch Security Content 인식
주요 용도	Frame 전송	Packet 전송	FLB SLB	FLB SLB Security





Data	1606	80	192.168.1.10	192.168.1.40	A.M	D.M
	송Port	수Port	송신자IP	수신자IP	송MAC	수MAC

L4 Switch

http://200.1.1.10



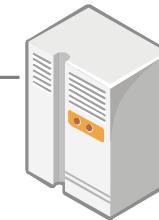
https://200.1.1.10



200.1.1.10

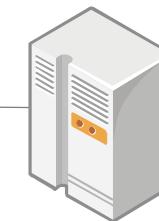
200.1.1.10:80	192.168.10.10
	192.168.10.20
200.1.1.10:443	192.168.10.30
	192.168.10.40

192.168.10.10



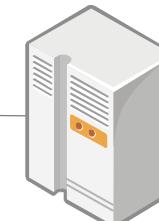
Web#1

192.168.10.20



Web#2

192.168.10.30



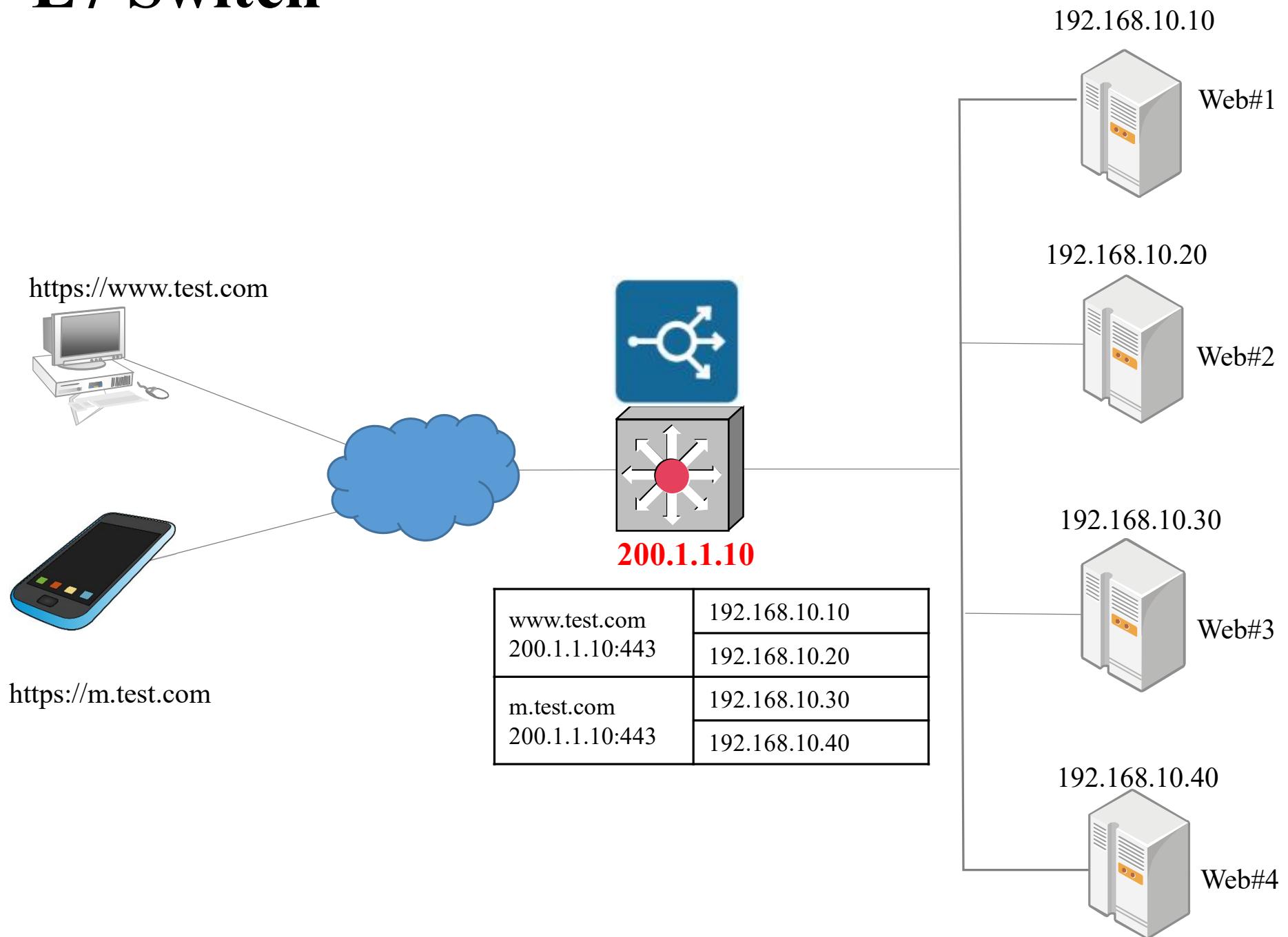
Web#3

192.168.10.40

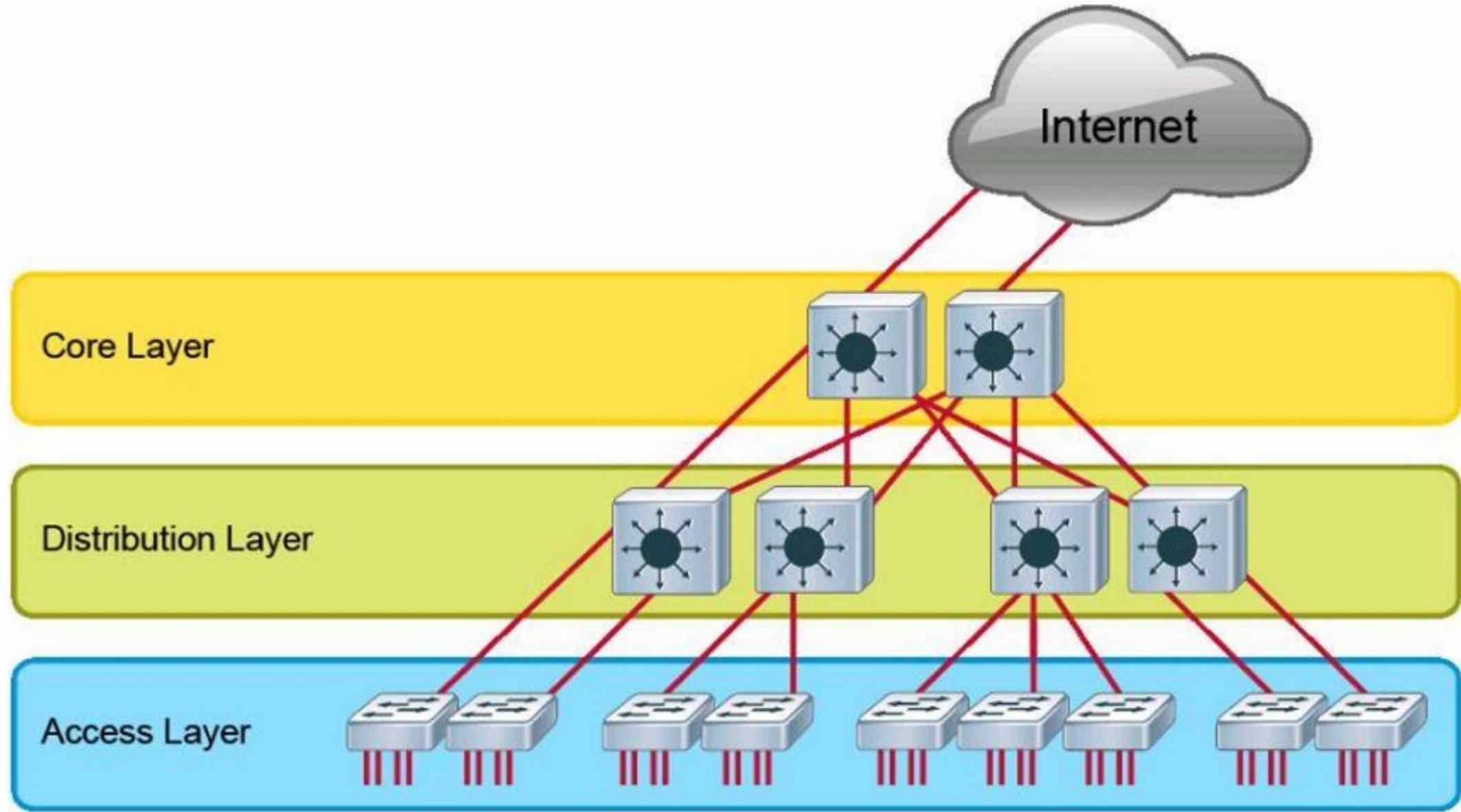


Web#4

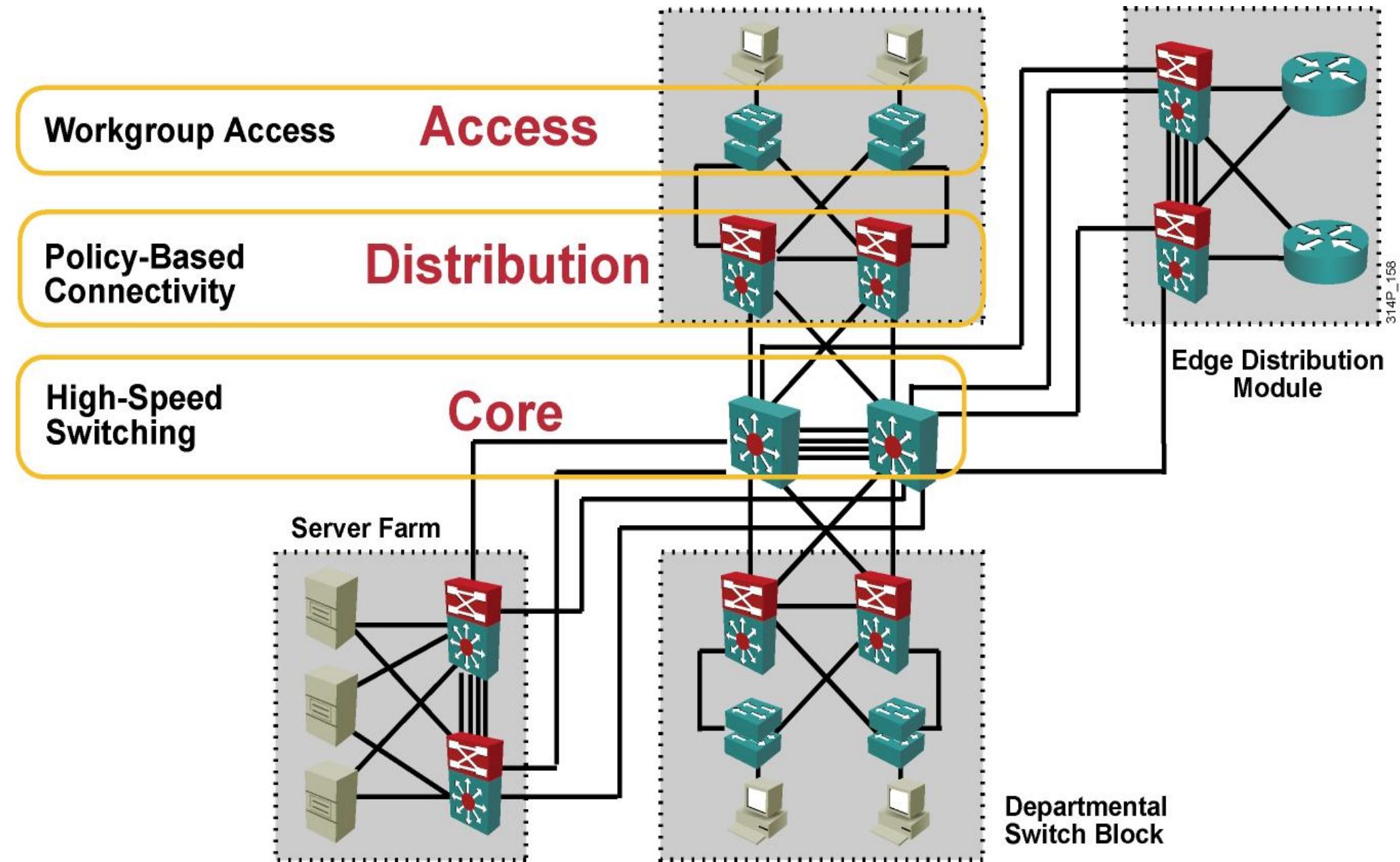
L7 Switch



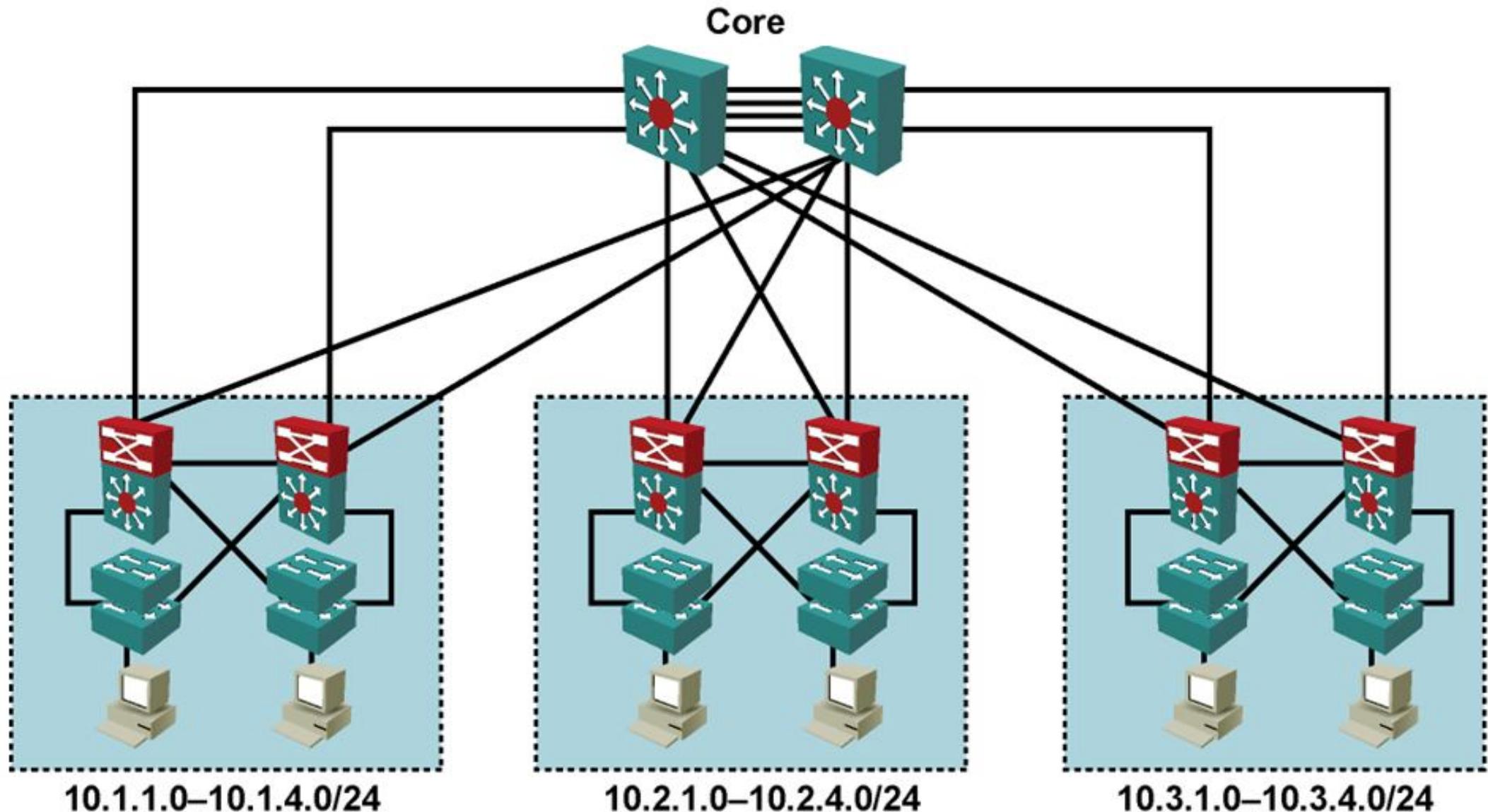
사내망 구성도



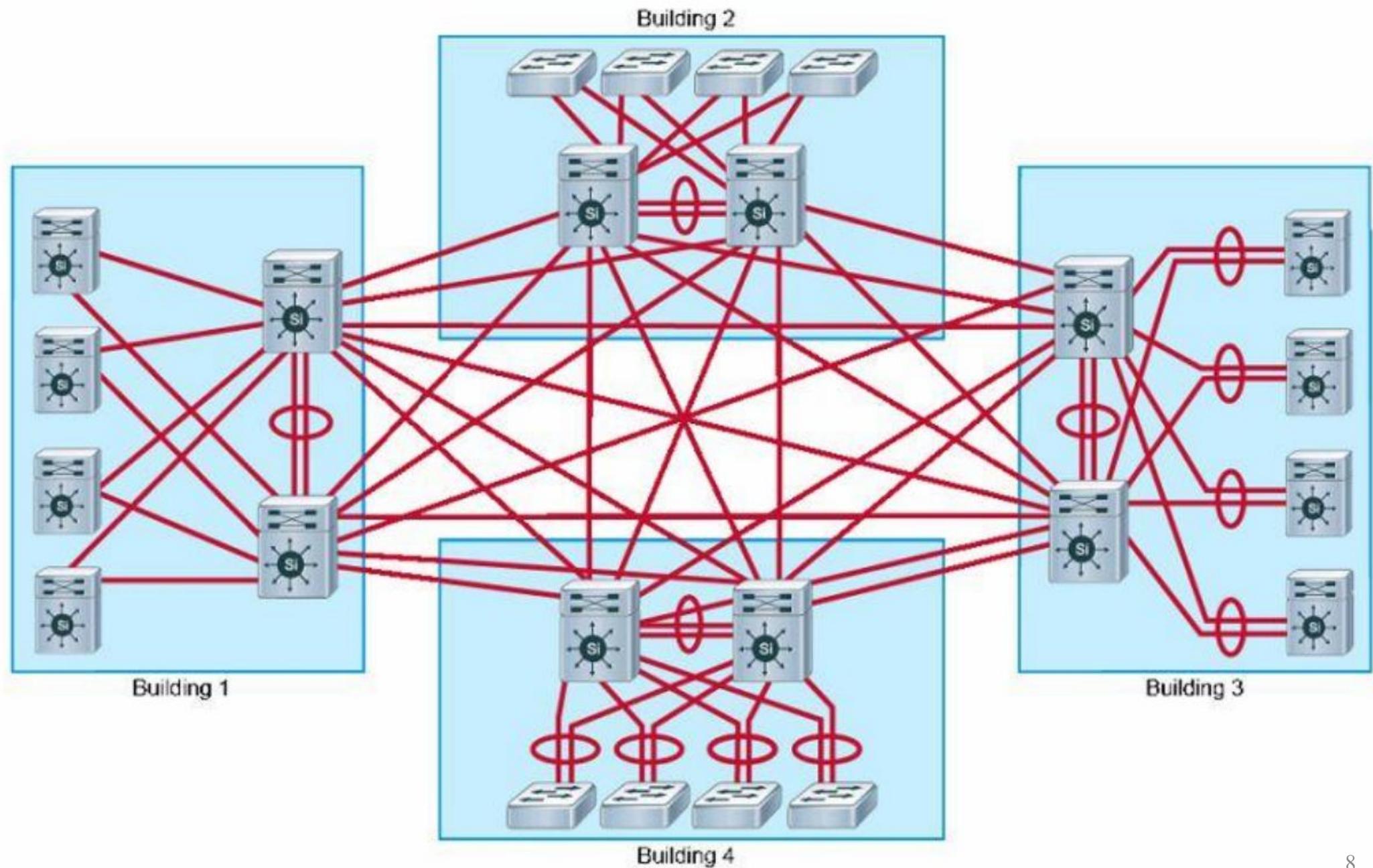
1 구성도



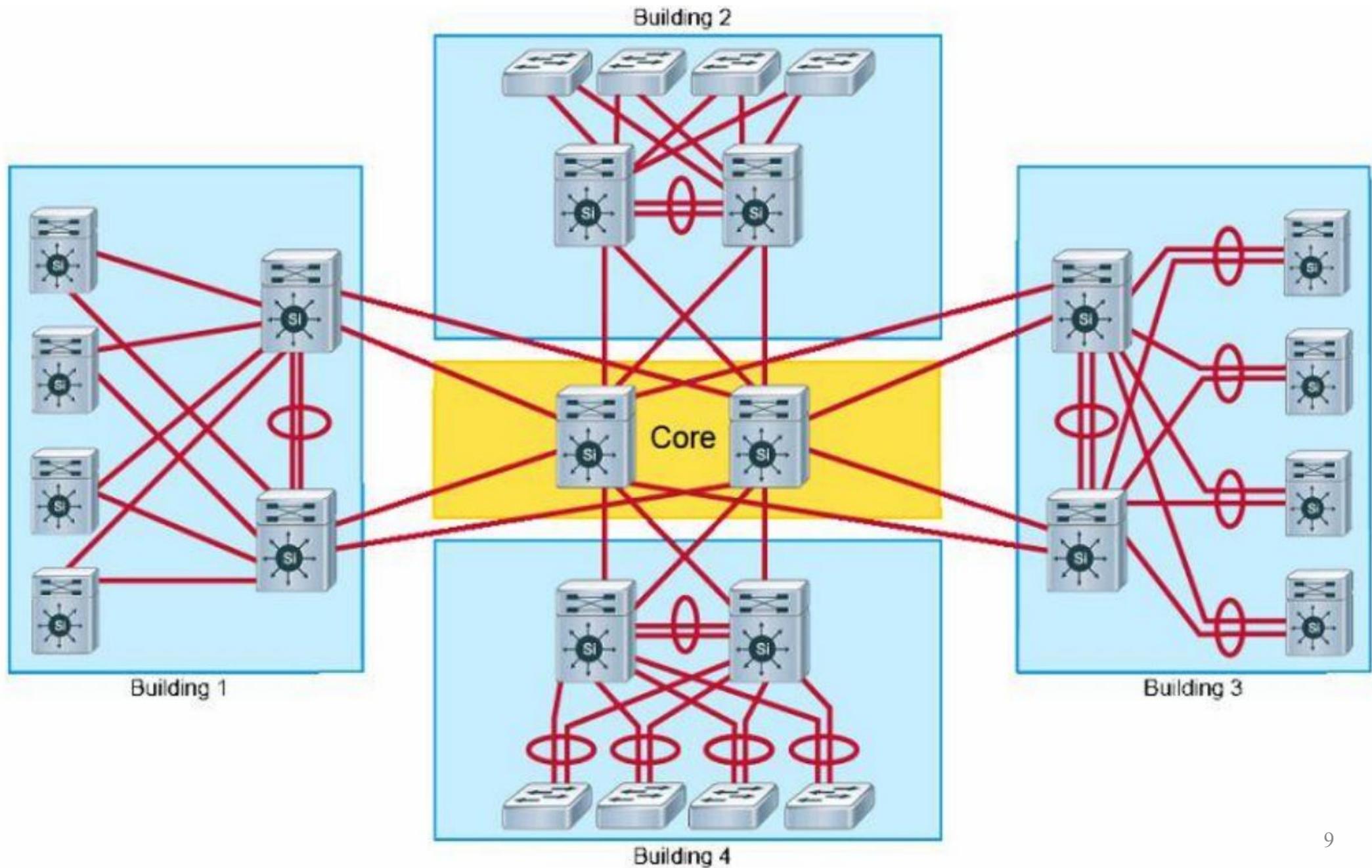
② 구성도



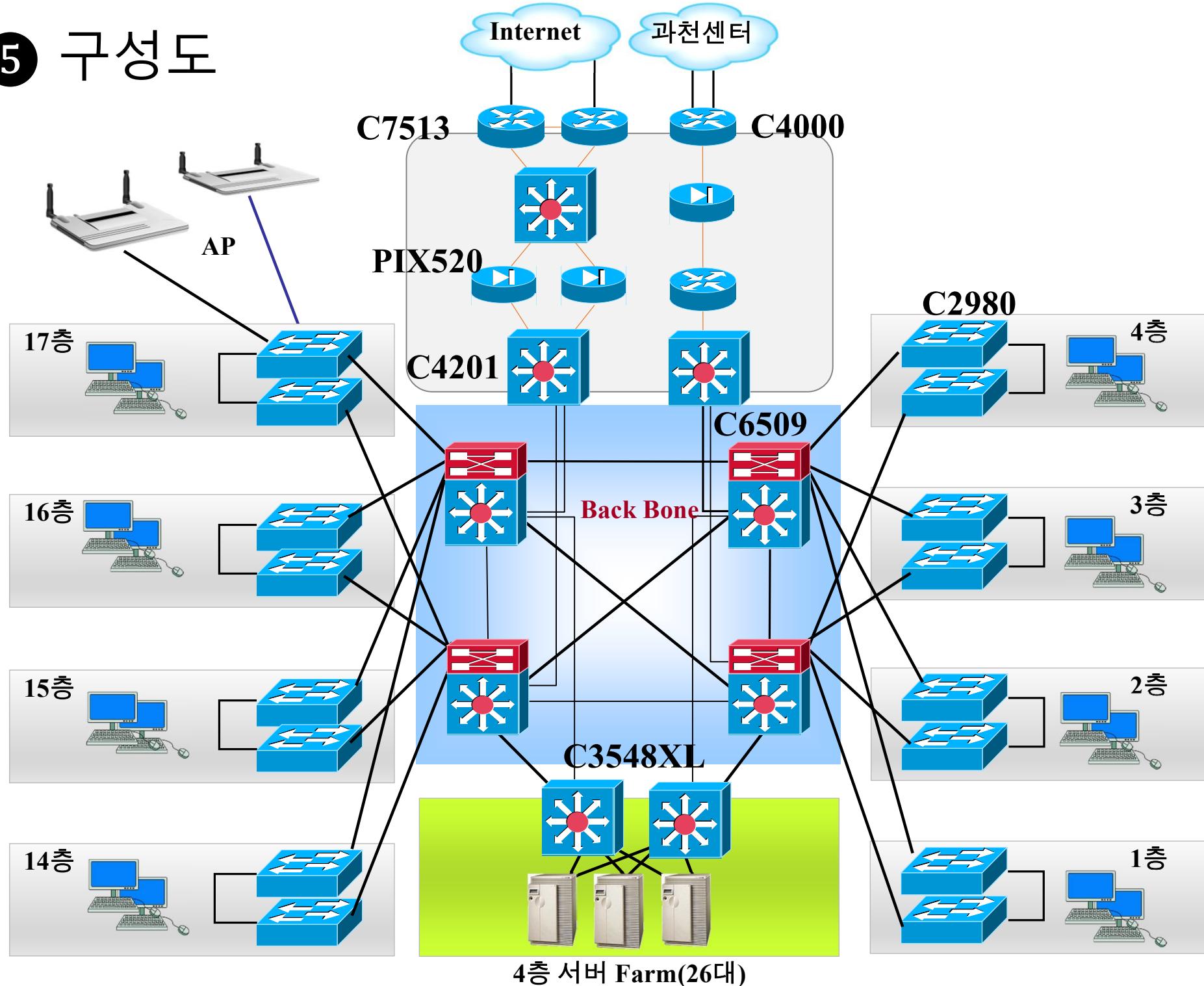
③ 구성도



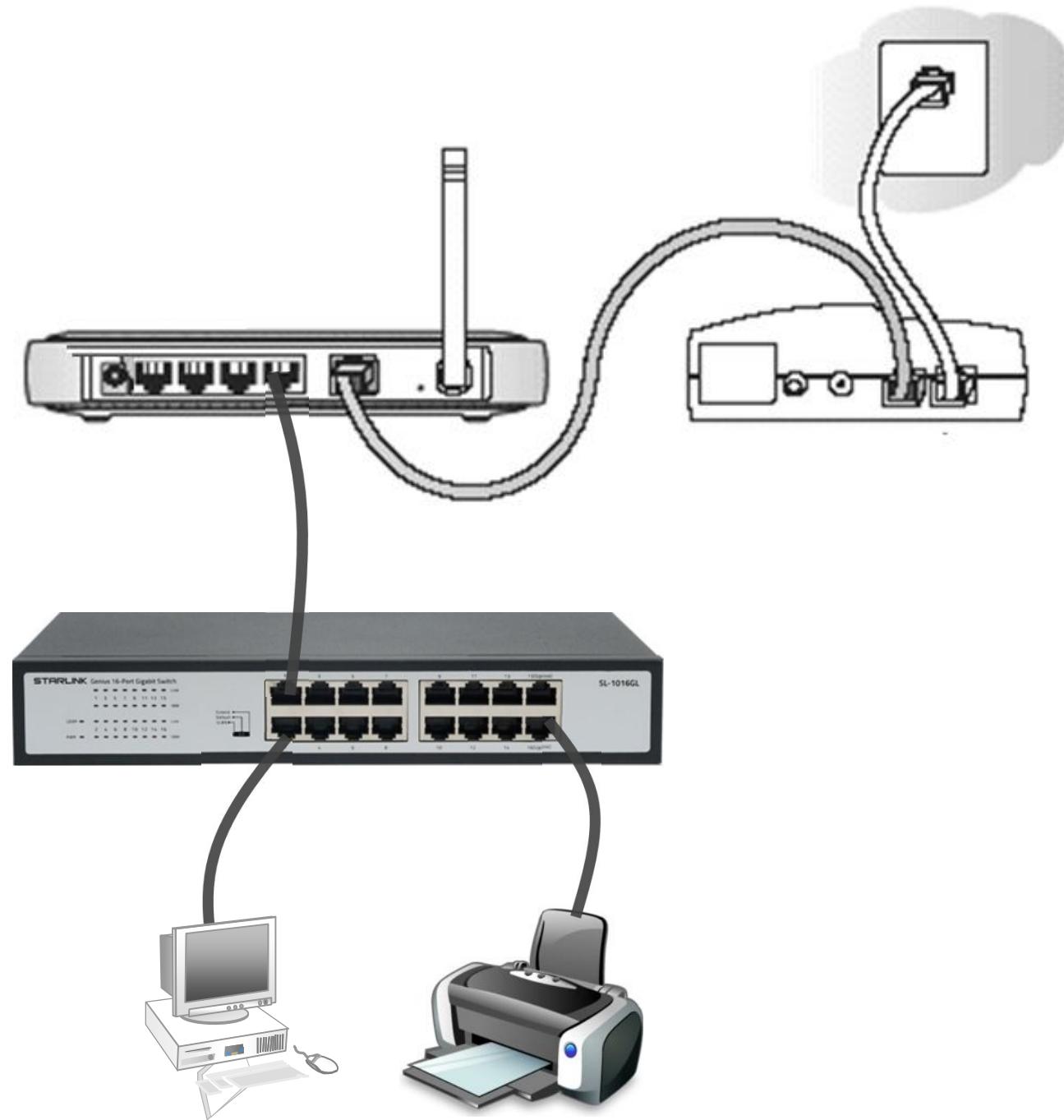
④ 구성도



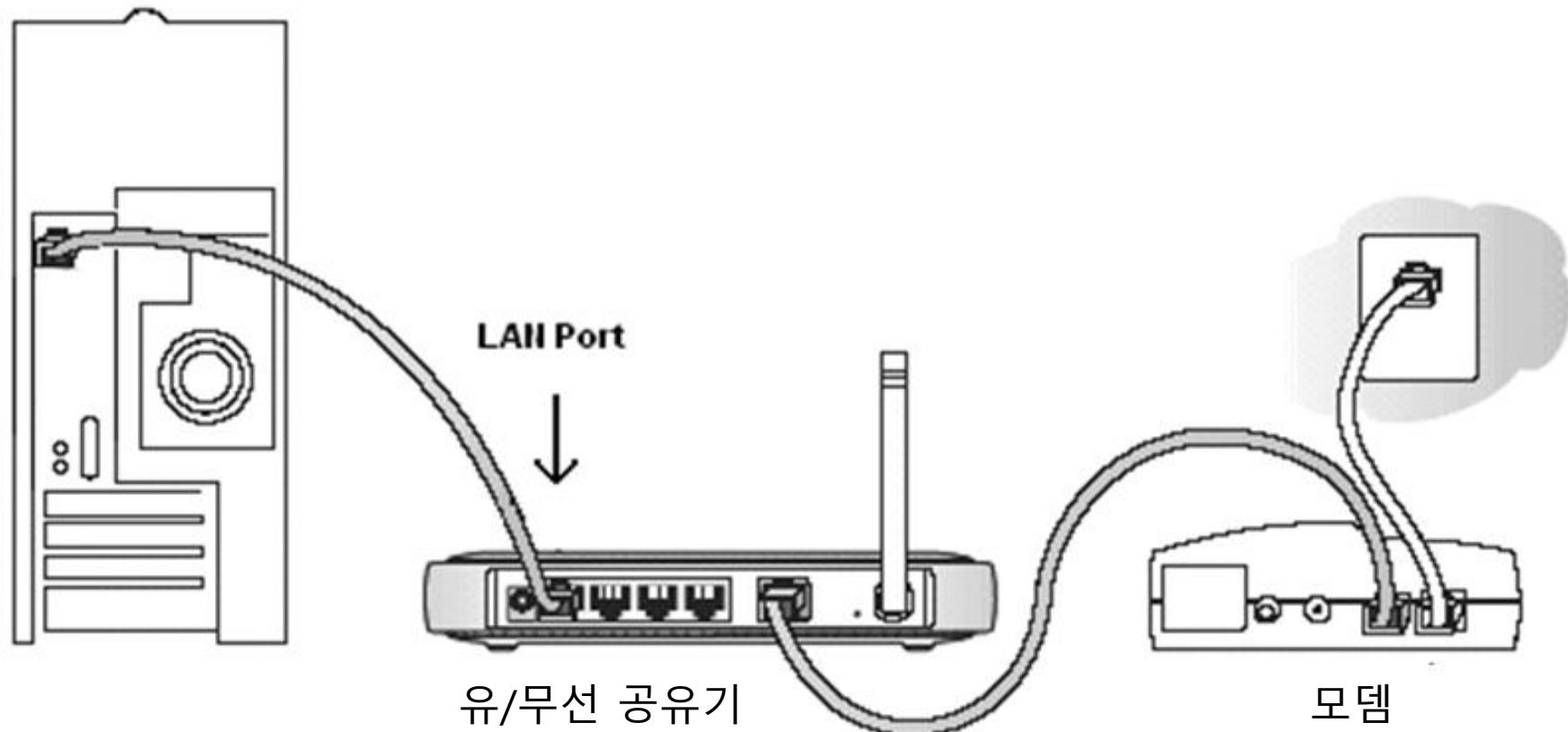
5 구성도



⑥ 구성도

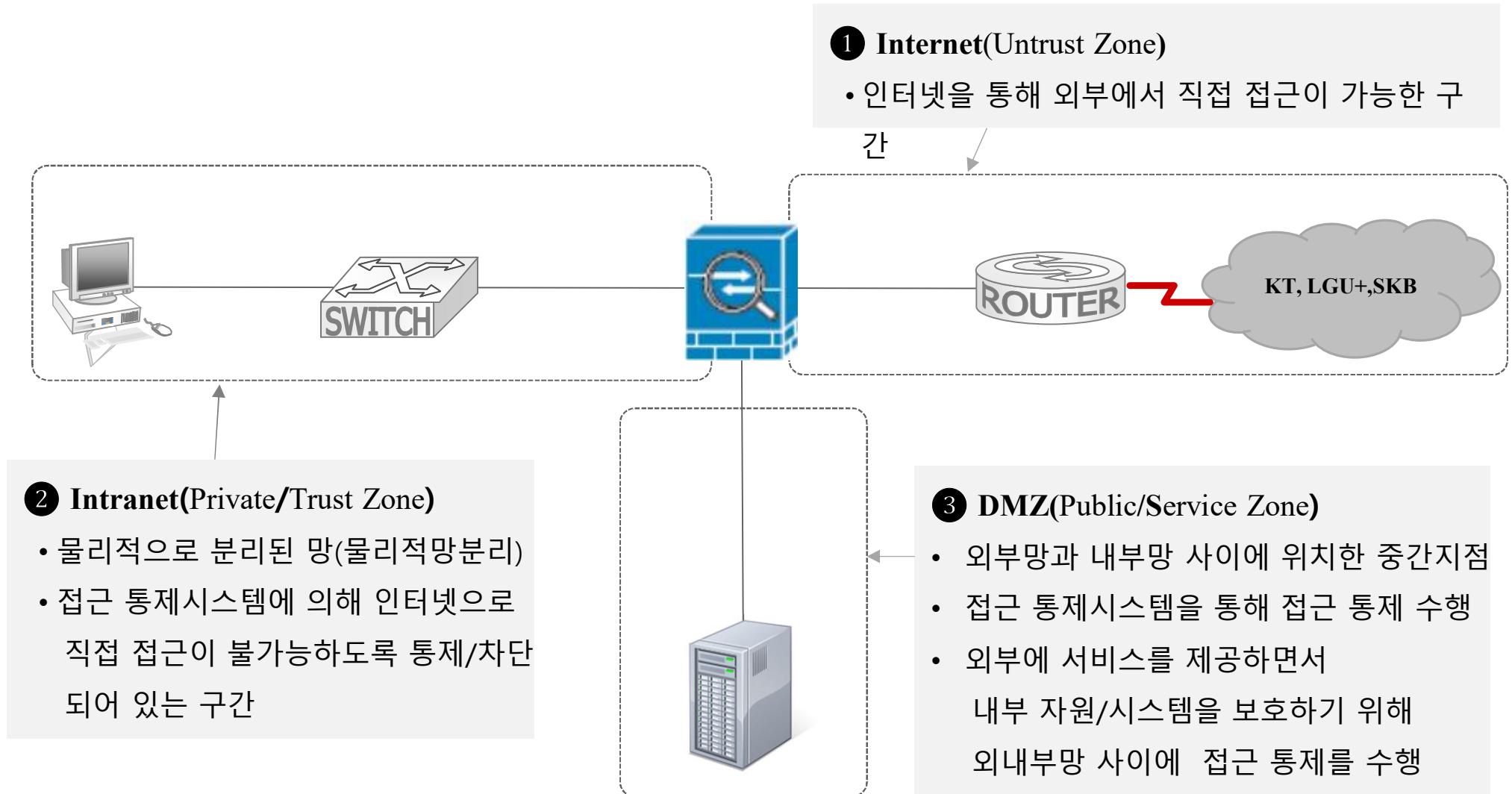


7 구성도



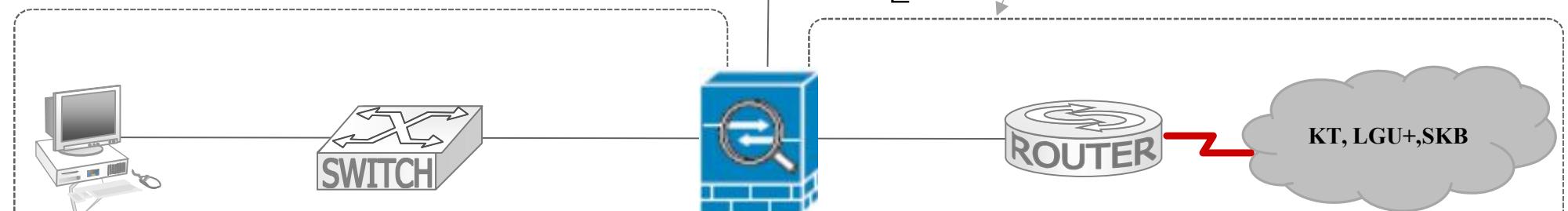
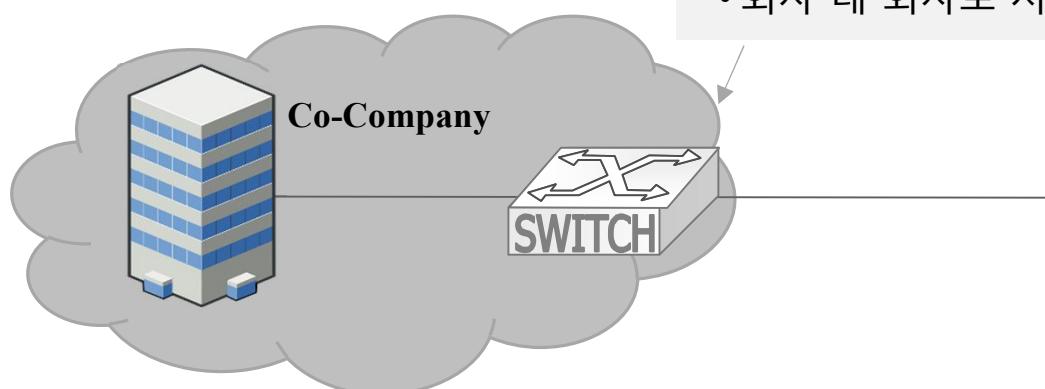
보안 솔루션

구성도



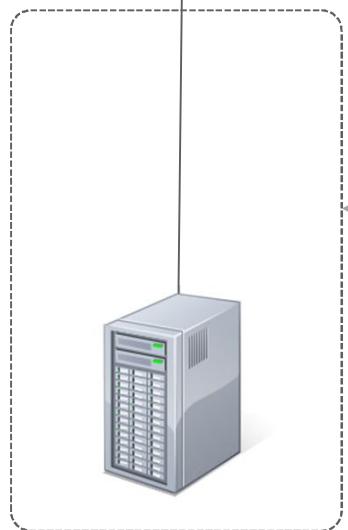
④ Extranet (대외망)

- 회사 대 회사로 서비스 연동이 필요한 경우 인터넷, 전용선, VPN등으로 연동



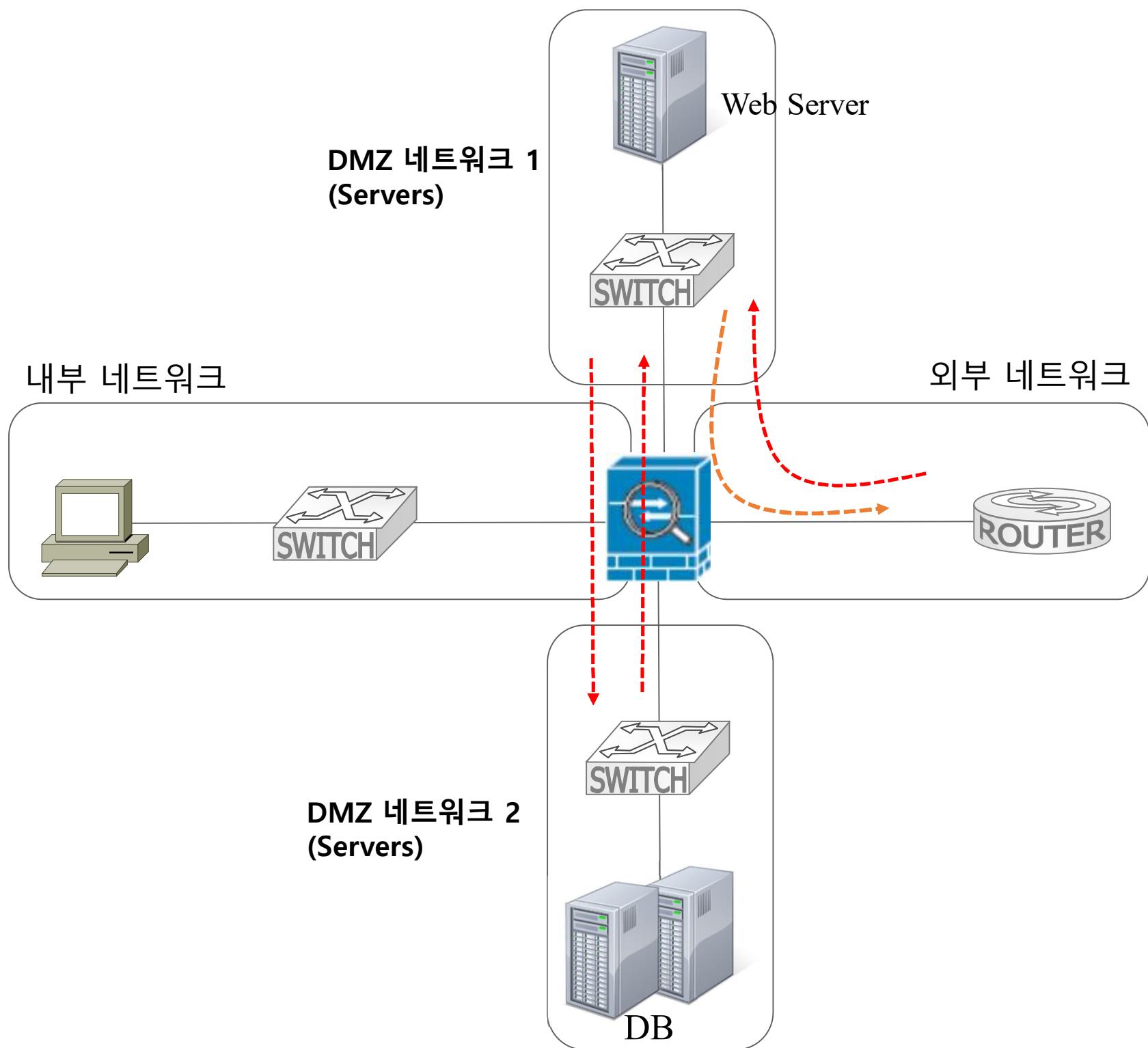
② Intranet(Private/Trust Zone)

- 물리적으로 분리된 망(물리적망분리)
- 접근 통제시스템에 의해 인터넷으로 직접 접근이 불가능하도록 통제/차단되어 있는 구간

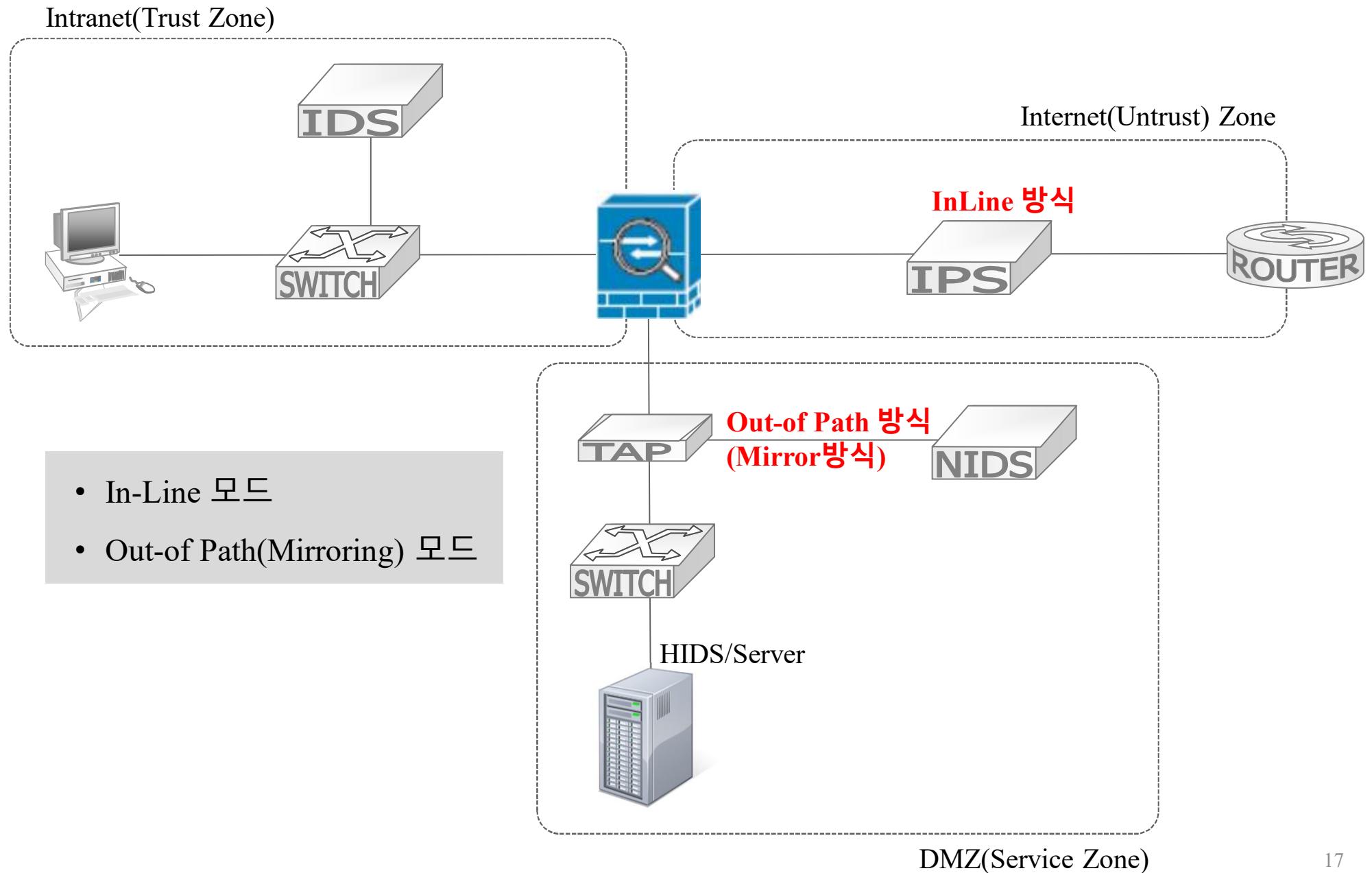


③ DMZ(Public/Service Zone)

- 외부망과 내부망 사이에 위치한 중간지점
- 접근 통제시스템을 통해 접근 통제 수행
- 외부에 서비스를 제공하면서 내부 자원/시스템을 보호하기 위해 외내부망 사이에 접근 통제를 수행

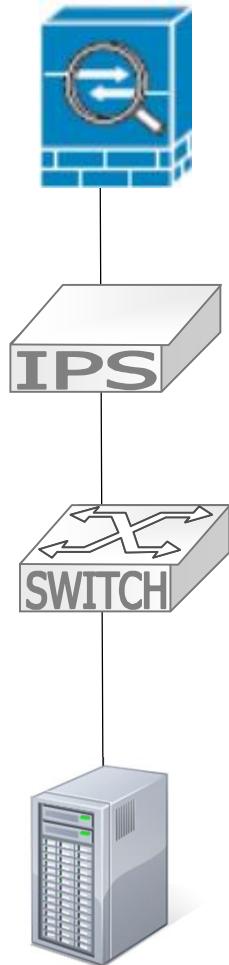


보안 장비 설치 모드



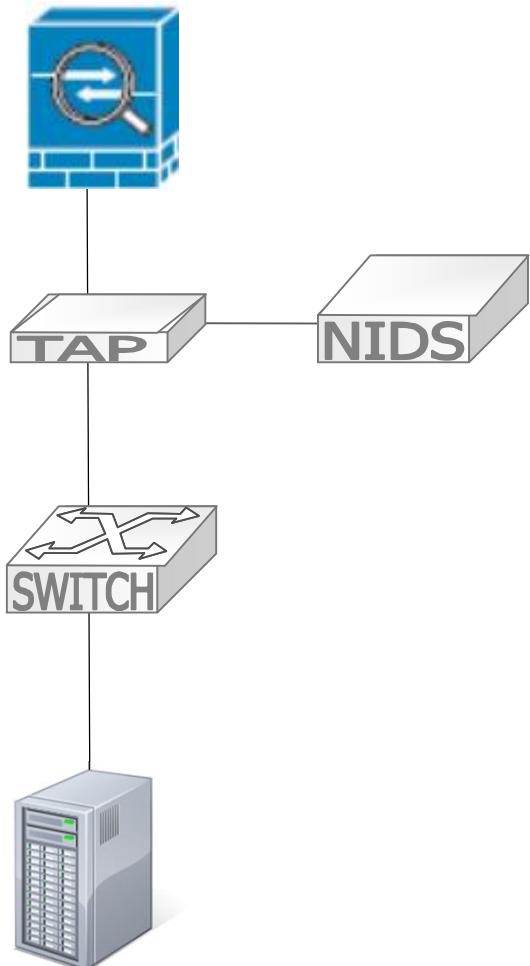
- In-Line 모드
- Out-of Path(Mirroring) 모드

InLine 모드



- 물리적 네트워크 경로 상에 보안장비를 설치
- 네트워크를 통과하는 모든 트래픽들이 보안장비를 거쳐 가도록 하는 모드
- 패킷 차단 목적의 장비에 적용 (예) Anti-DDoS, Firewall, IPS 등
- 장점 : 실시간 패킷을 탐지하고 차단
- 단점 : 장비에 장애가 발생 할 경우 전체 네트워크 장애로 확산 될 위험성
(전체 네트워크 가용성에 영향을 줄 수 있음)

Out of Path(Mirror) 모드



- 미러링 장비(예. TAP)를 통해 복제된 패킷을 받아서 탐지하는 모드
- 패킷 차단 기능이 없는 탐지 목적의 장비에 적용
 - IDS, Anti-APT, Network Forensic 등
- 네트워크 경로를 벗어난 곳에 위치
- 장점 : 전체 네트워크 가용성에 영향을 주지 않으면서 패킷을 탐지할 수 있음
- 단점 : 복제(복사) 된 패킷을 탐지하기 때문에 실시간 패킷을 차단하기 어려움

1) 방화벽(Firewall)

- IP주소와 Port 번호를 기반으로 방화벽 rule set(필터링 정책)에 따라 패킷 필터링을 수행하는 보안 장비
 - 접근 제어(Access Control)/ 패킷 필터링
 - NAT(Network Address Translation)
 - 액세스 기록 기능
 - 사용자 인증(Authentication)
 - 암호화 + 터널링

방화벽(Firewall) 정책 설정(rule set) 예제 표

*상태 검사(stateful inspection) 기능

트래픽방향	사용자	송신지IP	수신지IP	허용포트	시간대	Permit /Deny
외부→내부		몇몇 서비스를 제외한 모든 서비스 불가				
외부→DMZ	모든 사용자	모든 네트워크	DMZ 네트워크	HTTP, SMTP POP3	모든 시간대	Permit
내부→외부	내부 네트워크 모든 사용자	내부 네트워크	모든 네트워크	의심포트 권고 사항을 제외한 대부분 모든 포트 허용	특정 커뮤니티 웹 사이트 근무 시간대 제외	
내부→DMZ	인증을 거친 사용자	내부 네트워크	DMZ 네트워크	HTTP, SMTP POP3	모든 시간대	
DMZ→외부	DMZ 네트워크 사용자	DMZ 네트워크	모든 네트워크	HTTP, SMTP POP3	모든 시간대	
DMZ→내부	VOIP SIP를 제외한 모든 서비스 불가					

* P2P 사용 포트

서비스	TCP	UDP
소리바다	22322, 22323, 7675	8719, 4665, 4672
구루구루	9292, 9293, 8282, 31200	22321, 7674
파일구리	9493	9493

* 메신저 사용 포트

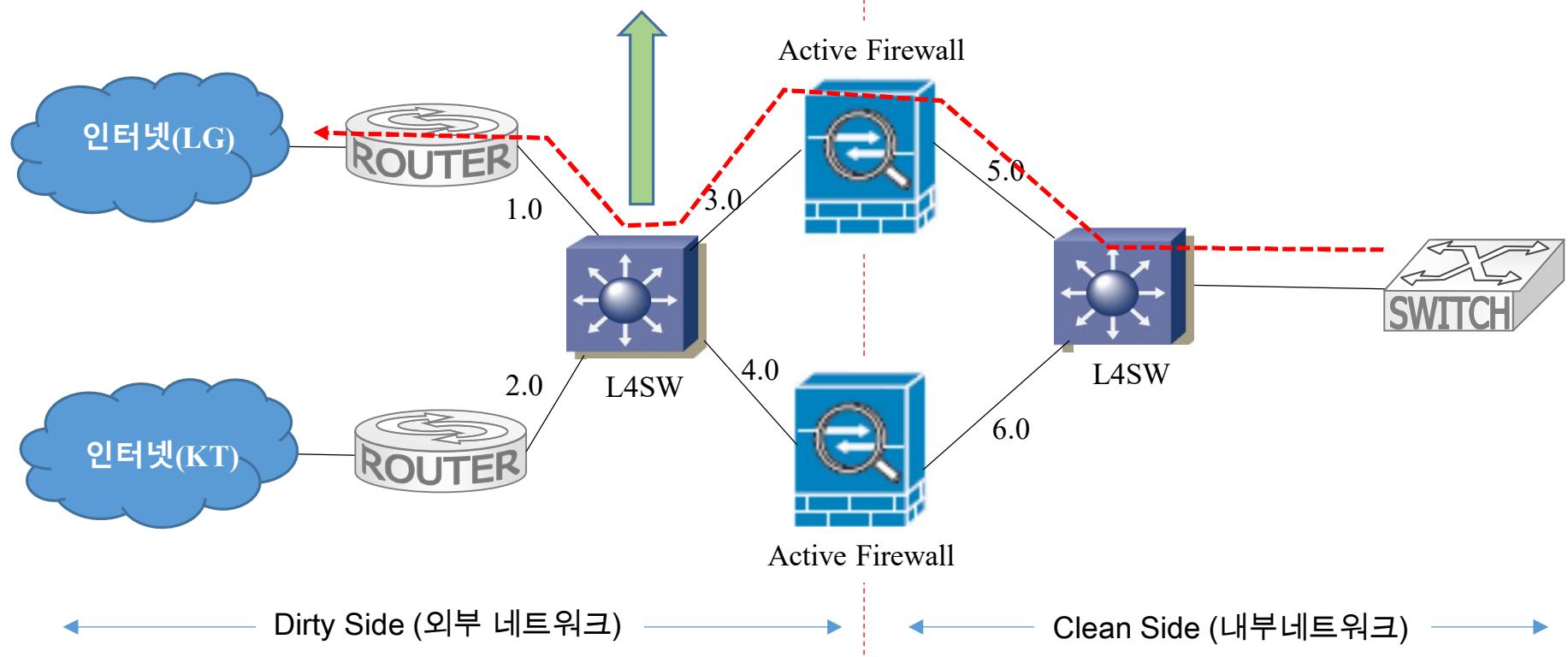
서비스	사용 하는 포트	서버 IP 주소 (변경될수 있음)
Kakaotalk	TCP 80, 43 TCP 8080 5223, 5228 9282 10000 – 10010	210.103.248.0/21 203.133.160.0/19 113.27.148.0/23 61.251.98.128/25 203.238.180.0/24 etc

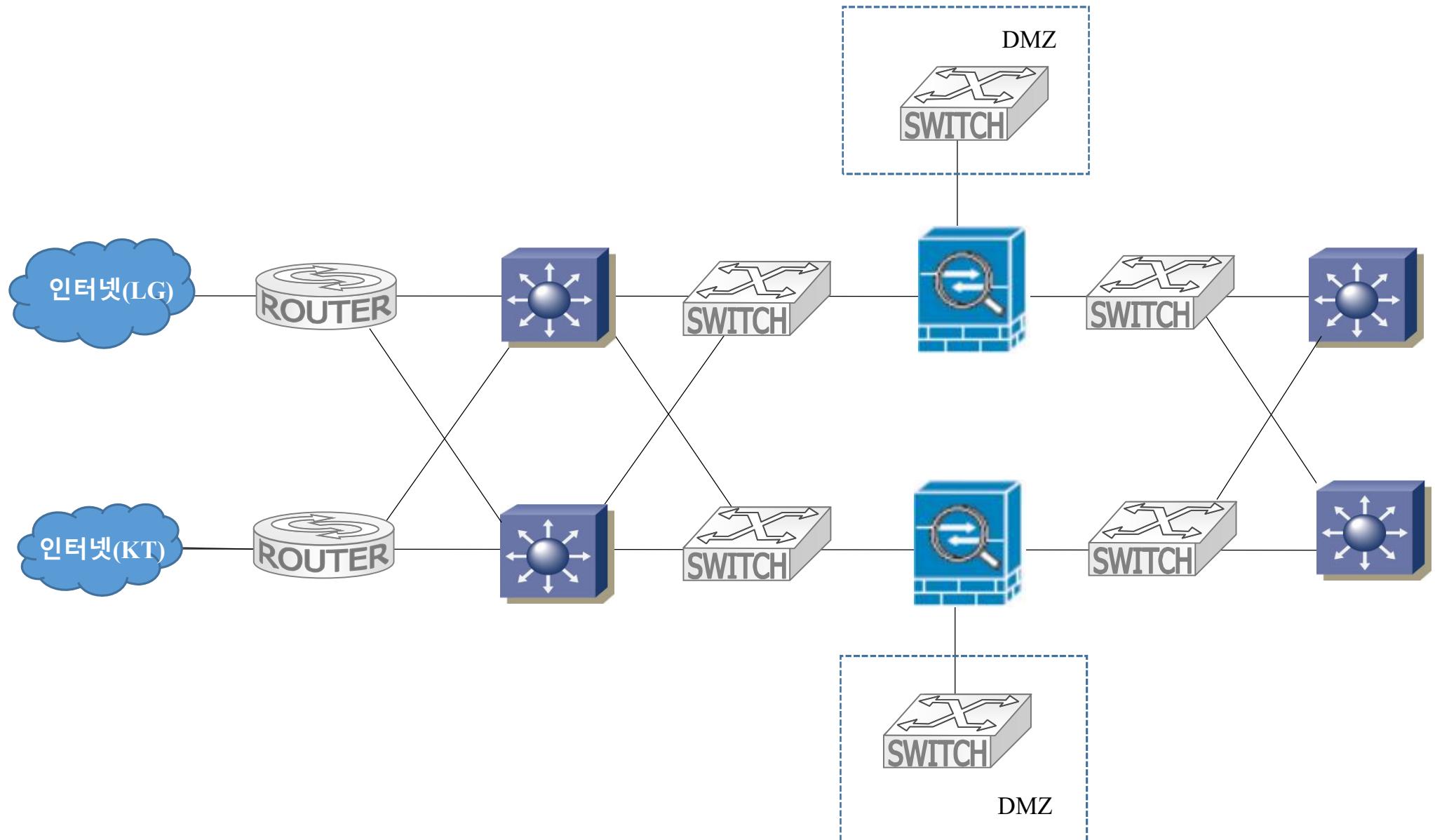
Firewall Load Balancing (FLB)

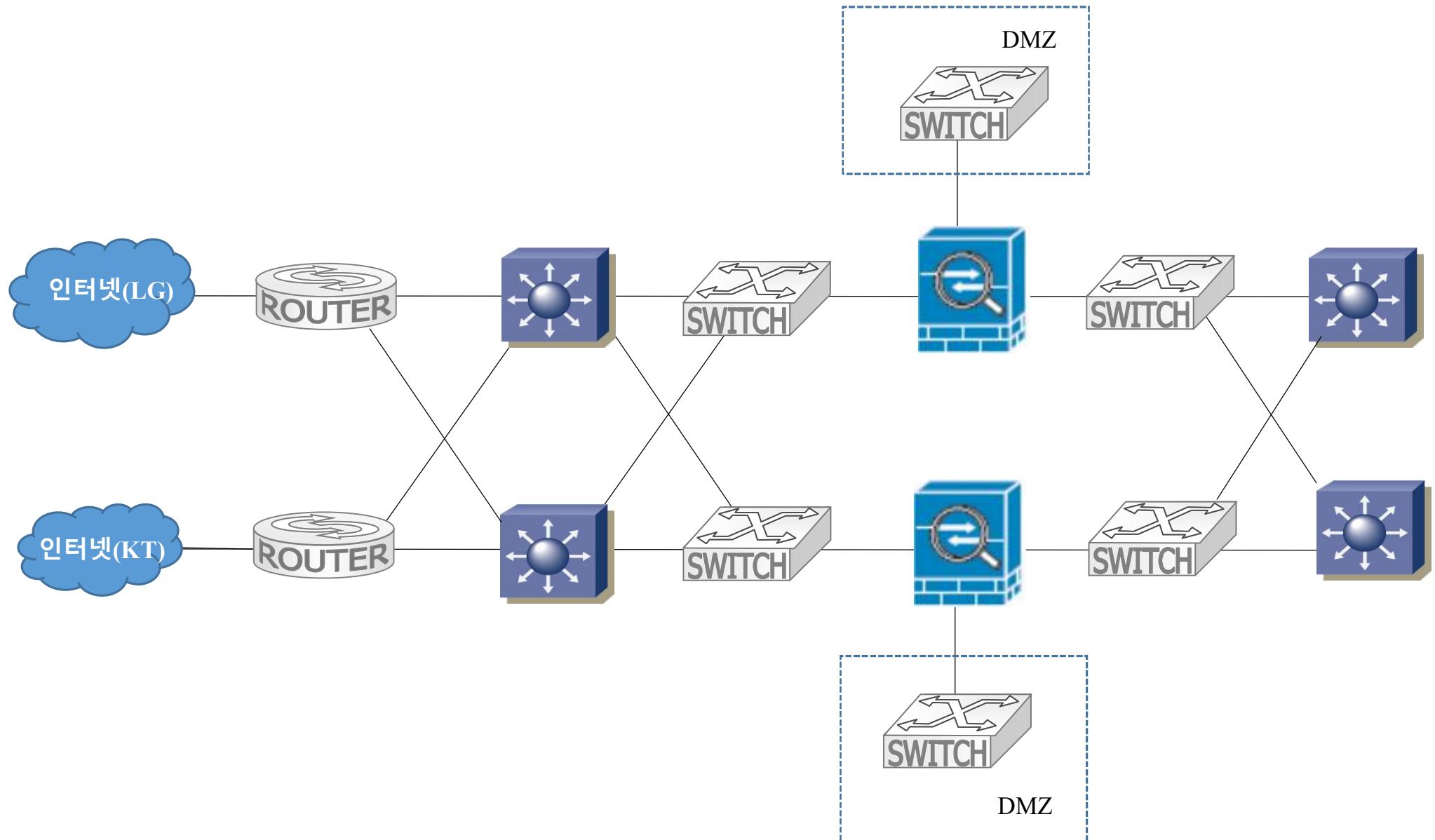
■ L4 스위치 기반의 로드 밸런싱

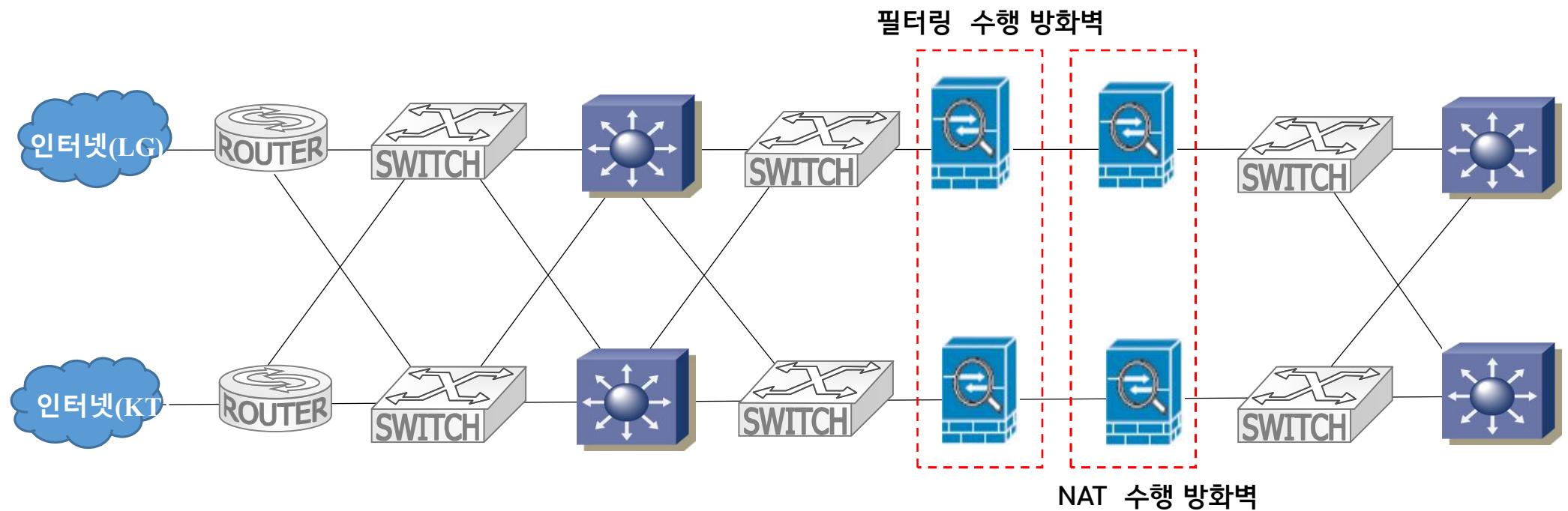
L4 스위치의 세션 기억 테이블 구성 항목(Sticky mode)

송신지IP	수신지 IP	송신포트	수신 포트	프로토콜	거친 방화벽
-------	--------	------	-------	------	--------









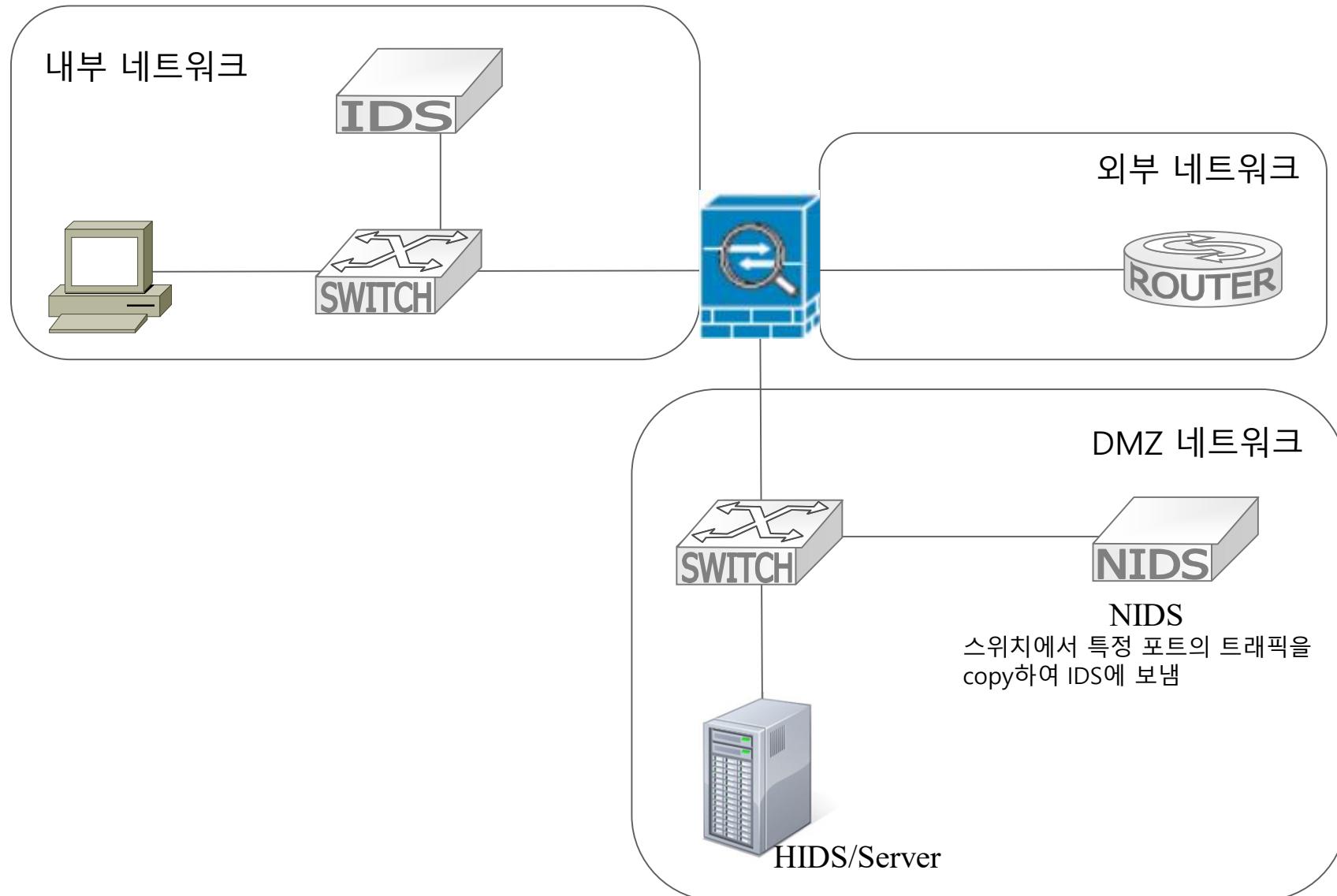
방화벽(Firewall) 한계

- 내부 네트워크에 존재하는 악의적인 공격을 막을 수 없음
- 방화벽을 경유하지 않는 공격을 막을 수 없음
- 방화벽에 방어 규칙에 포함되지 않는 공격을 막을 수 없음
- 데이터에 실려 있는 악성코드나 바이러스를 막을 수 없음
 - 메일에 첨부된 악성 코드를 막을 수 없음
- DoS와 DDoS 공격을 막을 수 없다.
 - 열린 포트를 통한 공격을 막을 수 없음

2) 침입 탐지 시스템 (Intrusion Detection System)

- 공격을 탐지하고 관리자에게 공격 알림을 통해 공격에 대처할 수 있게 해 주는 보안 시스템
- 전달하는 패킷의 내용이나 로그를 분석하여 공격 여부를 탐지
 - 악성코드 탐지 가능
- HIDS(Host-based IDS)와 NIDS(Network-based IDS)로 분류

*침입 탐지 시스템 (Intrusion Detection System)



HIDS(Host-based IDS)

- 서버에 직접 설치됨에 따라 네트워크 환경과 무관
- 호스트의 자원 사용 실태, 로그 등을 분석하여 침입 여부 탐지
- 무결성 체크 기능이 주요 기능
 - 무결성 점검에 의해 침입여부 식별
 - 최초 설치 시 초기 데이터베이스에 중요 파일들에 대한 해시값 저장
 - 주기적으로 중요 파일의 해시값 변조 유무를 검사/탐지/분석하여 결과 보고
- 오픈 소스 IDS : Tripwire(트립와이어)

NIDS(Network-based IDS)

- 네트워크 상에서 일어나는 침입 시도를 탐지
- 네트워크 세그먼트 당 하나의 장비만 설치하면 되므로 설치 용이
- 패킷 수집을 위해 mirroring 기능 이용
 - Mirroring : 패킷을 복사한 다음 복사한 패킷을 NIDS 장비로 전달
 - 스위치의 미러링 포트를 이용하거나 TAP 장비를 통해 패킷 복사
- 수집된 패킷은 분석을 위해 필터링과 축약과정(reduction)이 필요
 - 필터링은 불요한 정보를 제거하는 과정으로 지정된 수준의 데이터만 수집
 - 축약은 통계적/수학적 기법을 적용하여 반복되는 데이터를 줄이는 과정
- 오픈 소스 NIDS : Snort

False Negative & False Positive

- 미탐지(False Negative)

- 공격을 탐지하지 못하는 경우
 - 시그니처 기반의 탐지 시스템의 경우 미탐지가 높음

- 오탐지(False Positive)

- 공격이 아닌 것을 공격으로 탐지하는 경우
 - 행동 기반의 탐지 시스템의 경우 오탐지가 높음

IDS 탐지 방법

	오용탐지(Misuse Detection)	이상탐지(Anomaly Detection)
특징	<ul style="list-style-type: none">• 시그니처 기반의 탐지• 알려진 공격법이나 보안 정책에 위반하는 행동에 대한 패턴 탐지• 공격 분석 결과를 바탕으로 패턴 설정• 패턴(시그니처)과 비교하여 일치하는 경우 불법 침입으로 간주	<ul style="list-style-type: none">• 행동 기반의 탐지• 정상 범위(normal)을 벗어나는 데이터를 탐지하는 방법• 정량적인 분석, 통계적 분석을 사용• 형태 관찰, 프로파일 생성, 프로파일 기반으로 이상여부를 확인• I/O 사용량, 로그인 횟수, 패킷양 등

IDS 탐지 방법

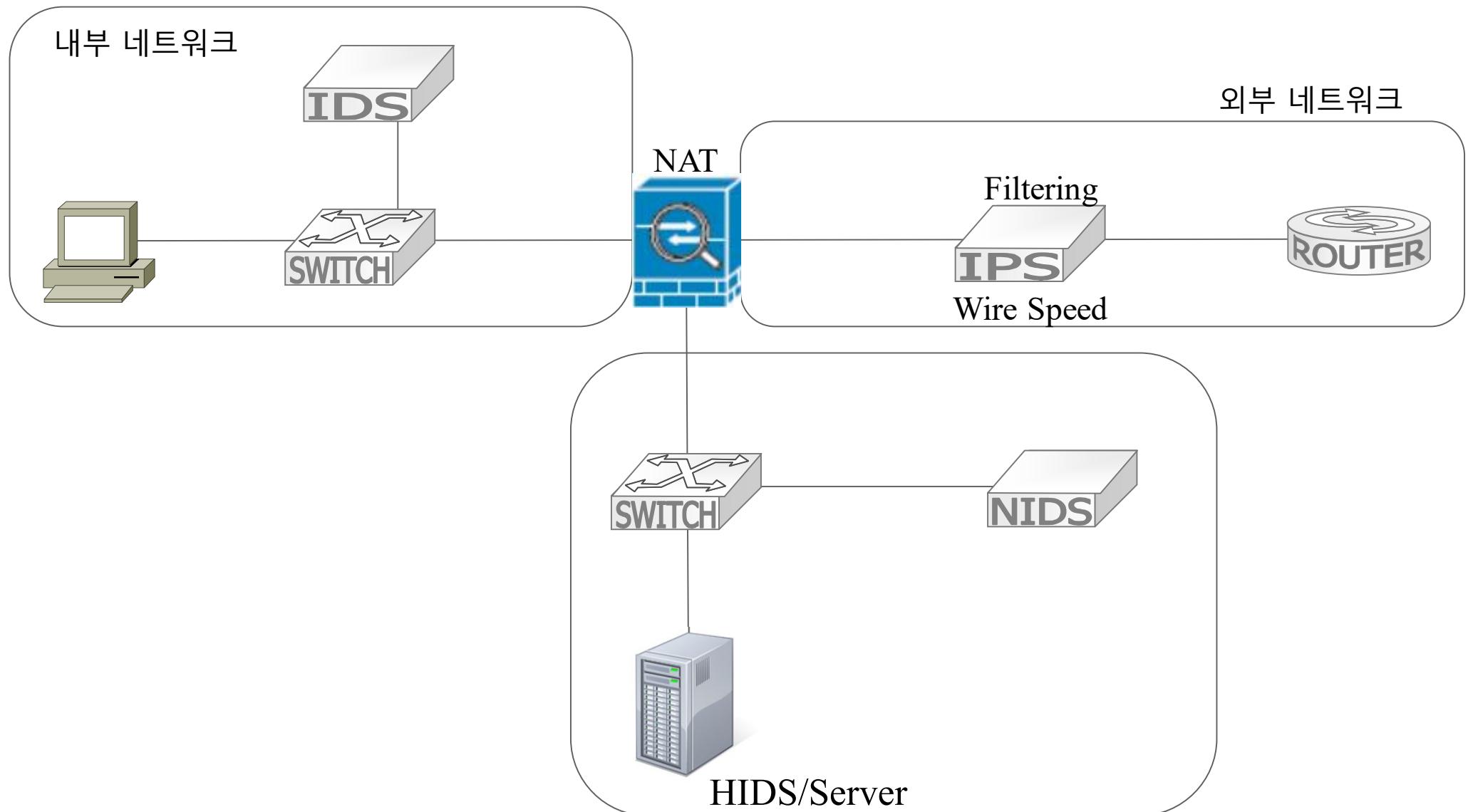
	오용탐지(Misuse Detection)	이상탐지(Anomaly Detection)
장점	<ul style="list-style-type: none">• 오탐률(false positive)이 낮음• 트로이 목마, 백도어 공격 탐지 가능	<ul style="list-style-type: none">• 미탐률(false negative)이 낮음• 인공지능 알고리즘 사용으로 스스로 판단하여 수작업의 패턴 업데이트 불필요• 알려지지 않는 새로운 공격 탐지 가능
단점	<ul style="list-style-type: none">• 미탐률(false negative)이 높음• 새로운 공격 탐지를 위해 지속적인 공격 패턴 갱신 필요• 패턴에 없는 새로운 공격에 대해서는 탐지 불가능	<ul style="list-style-type: none">• 오탐률(false positive)이 높음• 정상과 비정상 구분을 위한 임계치 설정이 어려움

침입 탐지 시스템 한계

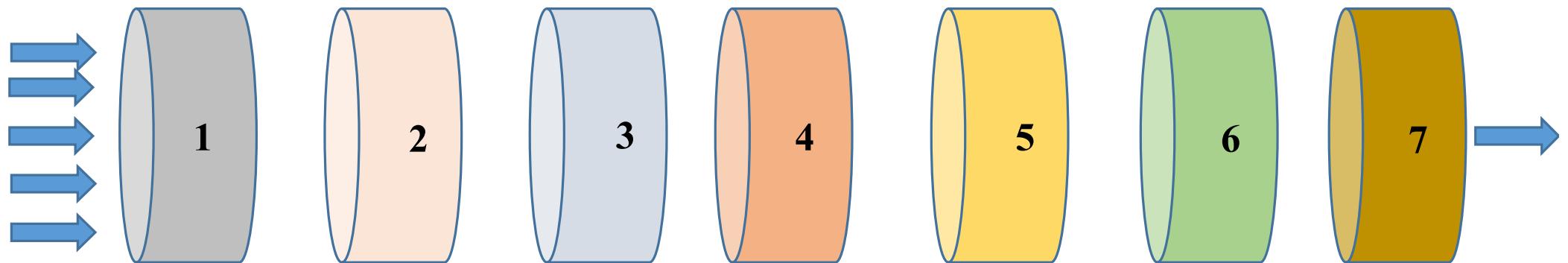
- 오탐지(false positive)와 미탐지(false negative) 문제 발생
 - 공격에 대한 패턴을 모르다면 분석과 탐지가 어려움
- 실시간 공격을 막을 수 없음
- 단편화(fragmentation), 난독화, 암호화와 같은 기술은 감지하지 어려움

3) 침입 방지 시스템 (Intrusion Prevention System)

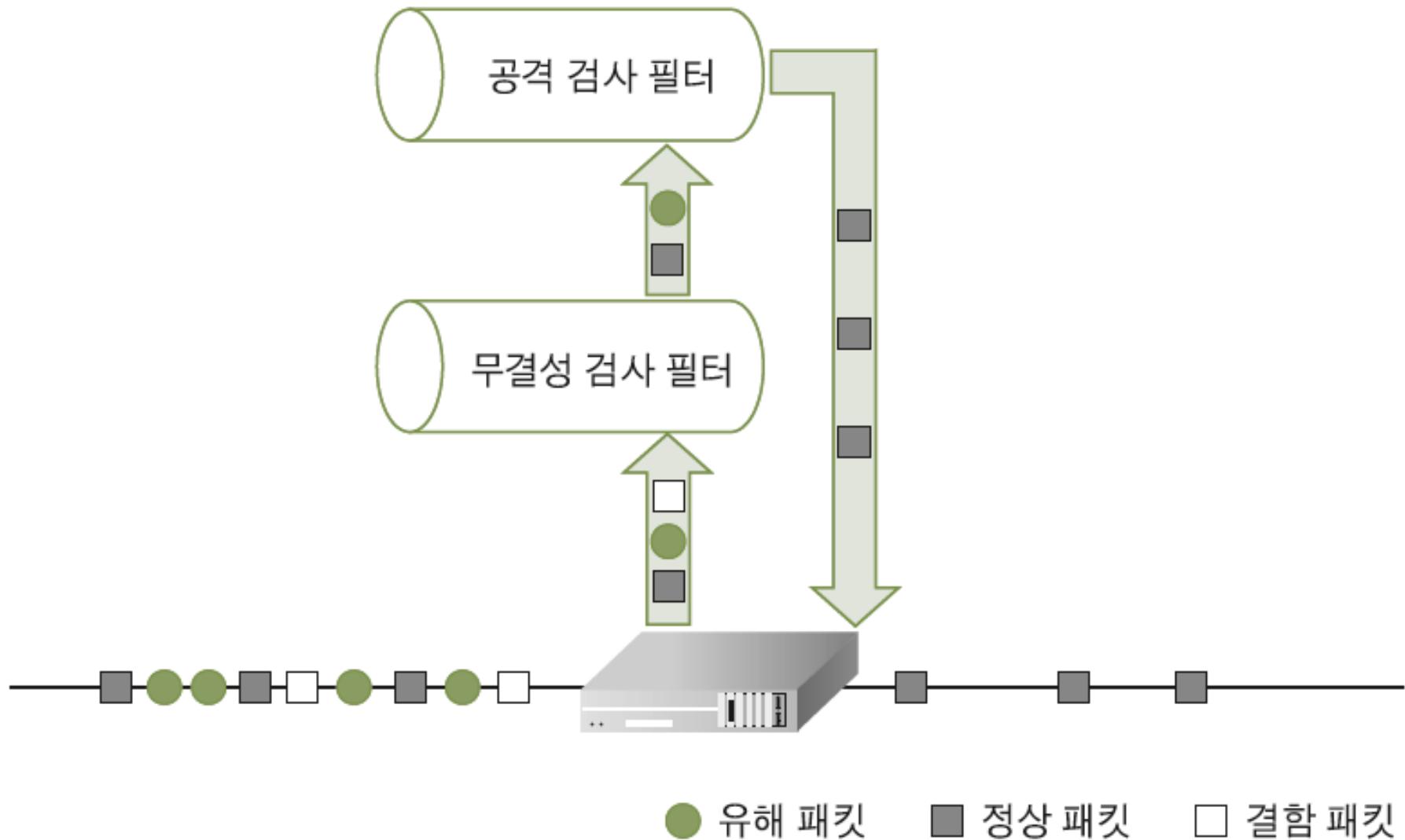
- 침입탐지시스템의 detection 기능과 방화벽의 차단(blocking) 기능 결합
- 이상 행위 탐지(anomaly detection)를 통해 알려지지 않은 공격 패턴에 대응
- 공격에 대한 사전 방지를 조치하는 것으로 in-line 방식으로 설치 및 운영
- 실시간 침입차단, 인터넷 웜, 악성 코드 및 해킹에 기인한 유해 트래픽 차단
- 능동형 보안 솔루션
 - IDS : 탐지 후 사후에 조치를 취하는 기술
 - IPS : 예방적이고 사전에 조치를 취하는 기술



침입 차단 시스템 필터들

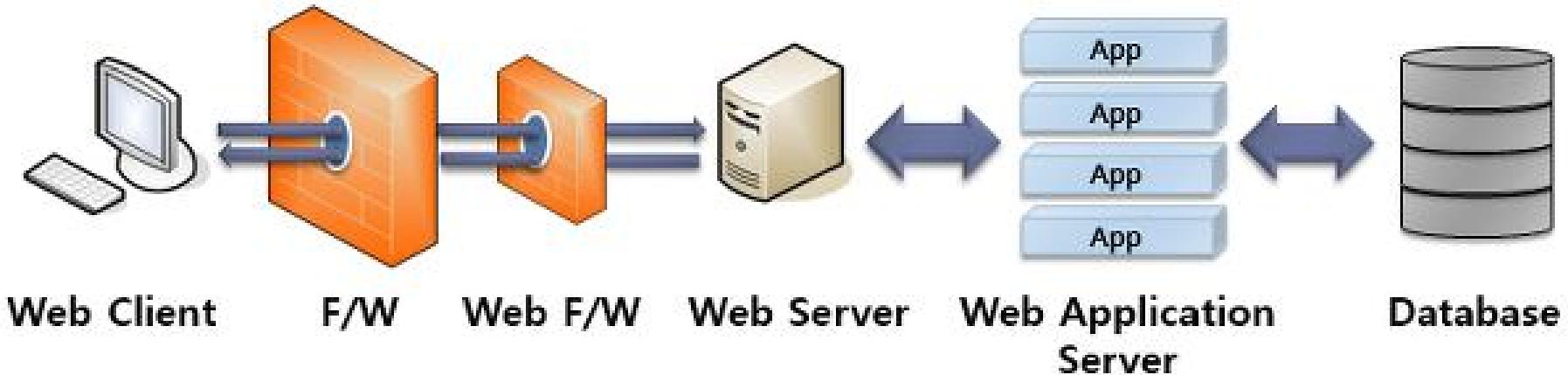


필터	기능
1	방화벽필터 - 액세스 제어 및 패킷 필터링 기능 (IP, 포트 등 패킷 필드별로 막을 패킷 정의)
2	트래픽 모니터링 및 QoS 필터 - 프로토콜별, 서비스별, IP 영역별 QoS 기능 제공
3	프로토콜 무결성 확인 필터 - FTP, DNS, 메일, 웹 등 TCP/IP 프로토콜 동작 표준에 위반하는 패킷 조사
4	Signature 이상 감시 필터 : 악성 코드, 취약성, 웜에 대한 탐지 및 차단
5	DoS/DDoS 스캔 필터
6	L7 필터 : TCP /IP 단편화, 웹 우회 공격 등 L7 프로토콜 디코딩을 통한 필터
7	데이터 콘텐츠 내용을 기준으로 필터링 여부 결정



4) Web Application Firewall(WAF)

- 웹 컨텐츠(HTTP/HTTPS) 를 분석하여 공격을 탐지 및 차단하는 기능을 가진 방화벽
 - OWASP Top 10의 웹 공격에 사용되는 요청 파라미터 패턴을 분석



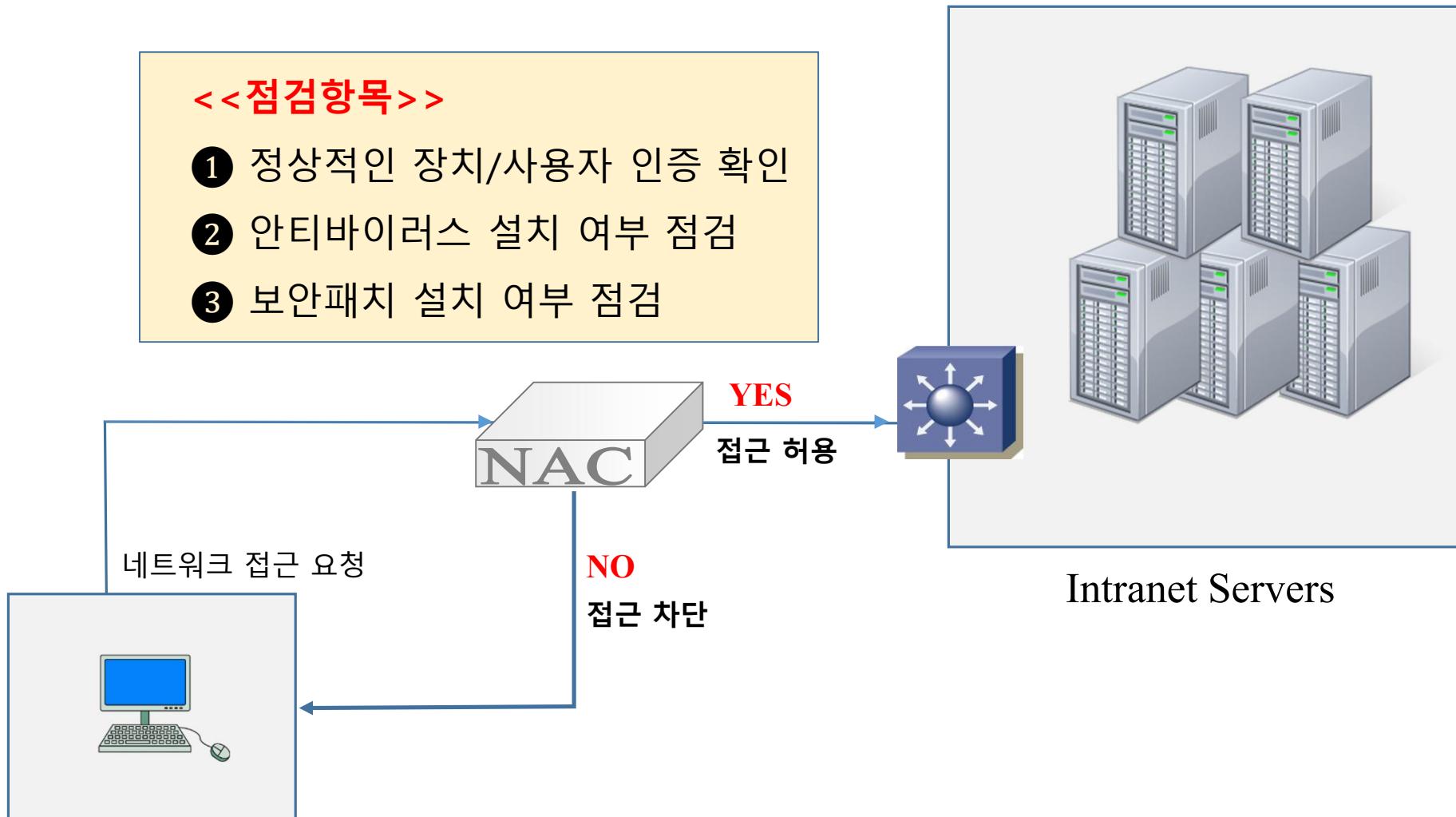
* WAF 기능

- 서버의 정보와 개인 정보 등의 중요한 정보 유출 차단 (service out)
 - 정보유출 방지, 부정 로그인 방지, 웹 사이트 위변조 방지등에 활용

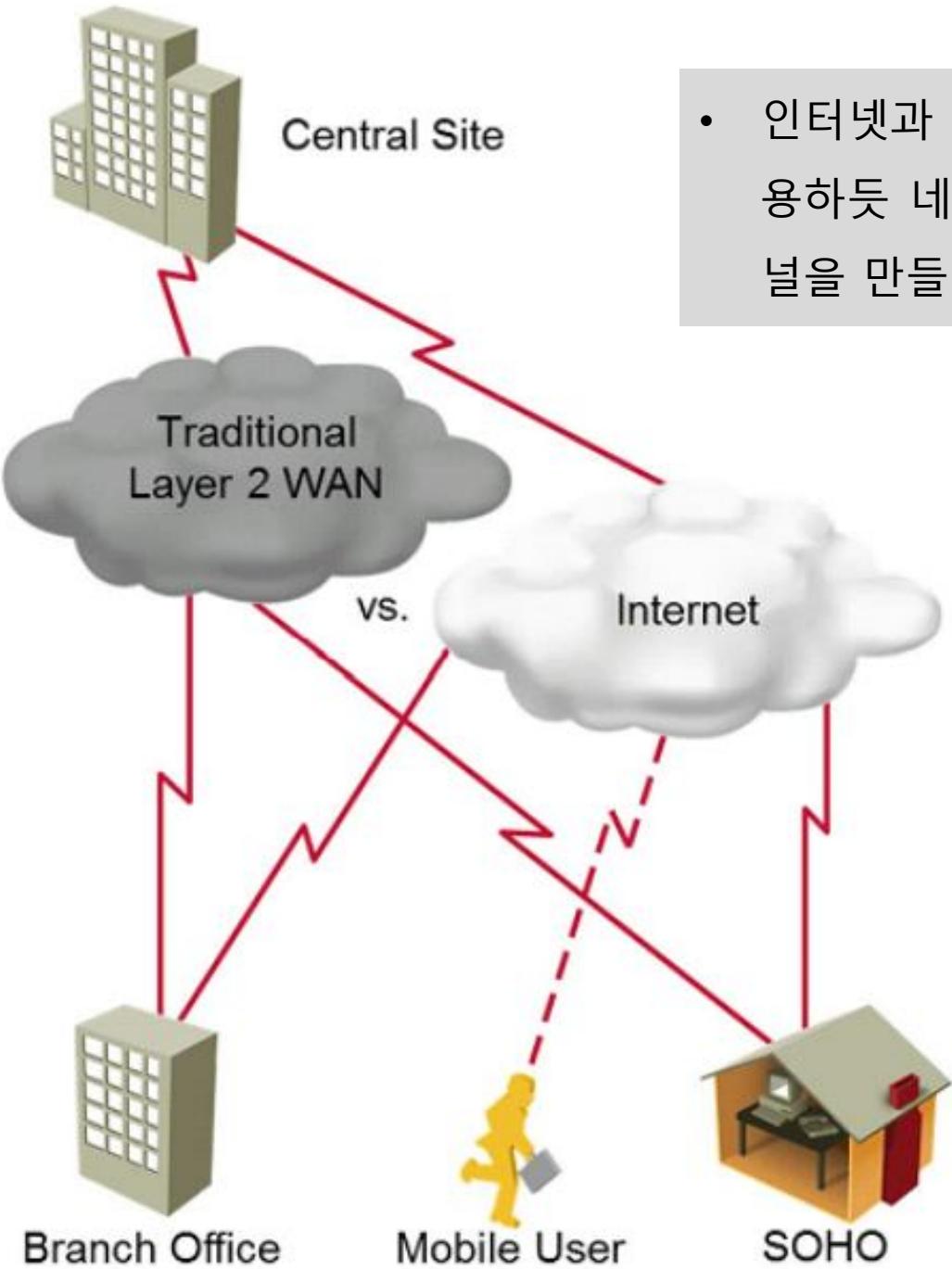
정보 유출 방지	개인 정보가 웹 게시판에 게시되거나 개인정보가 포함된 파일 등이 웹을 통해 업로드 및 다운로드 되는 경우에 대해 탐지하고 대응
부정 로그인 방지	무작위 대입 등의 방식으로 웹사이트 로드인을 시도하는 경우와 같이 비정상적인 접근에 대한 제어
웹사이트 위변조 방지	해킹 후 웹사이트를 위변조 하는 경우 이를 탐지하고 대응

5) NAC(Network Access Control)

* NAC 기반 구성도



6) VPN (Virtual Private Network)



- 인터넷과 같은 공중망을 이용하여 마치 사설망을 사용하듯 네트워크를 안전하게 연결하기 위한 통신 터널을 만들어 데이터를 안전하게 전송하는 시스템

계층별 암호화 프로토콜과 VPN

*VPN : 캡슐화 기술(암호화 header를 추가시킴)

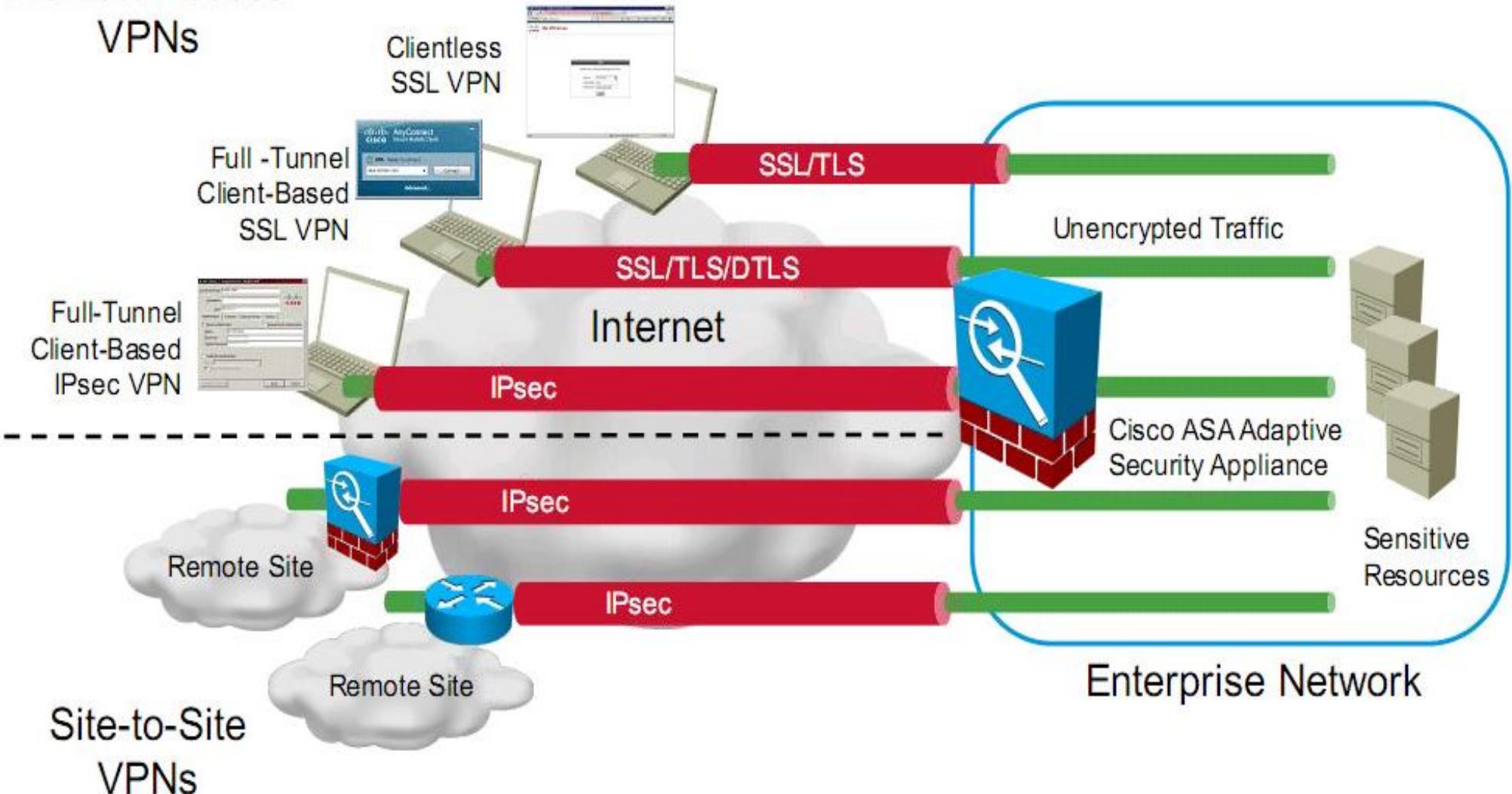
- header : 제어 정보

계층	암호화 프로토콜	VPN
2계층	L2TP, PPTP	L2TP VPN PPTP VPN
3계층	IPSec	IPSec VPN
4계층	TLS	SSL VPN
5계층	SSL	
7계층	HTTPS, SSH etc	

Cisco ASA VPN

*VPN = 캡슐화 기술 = 터널 기술

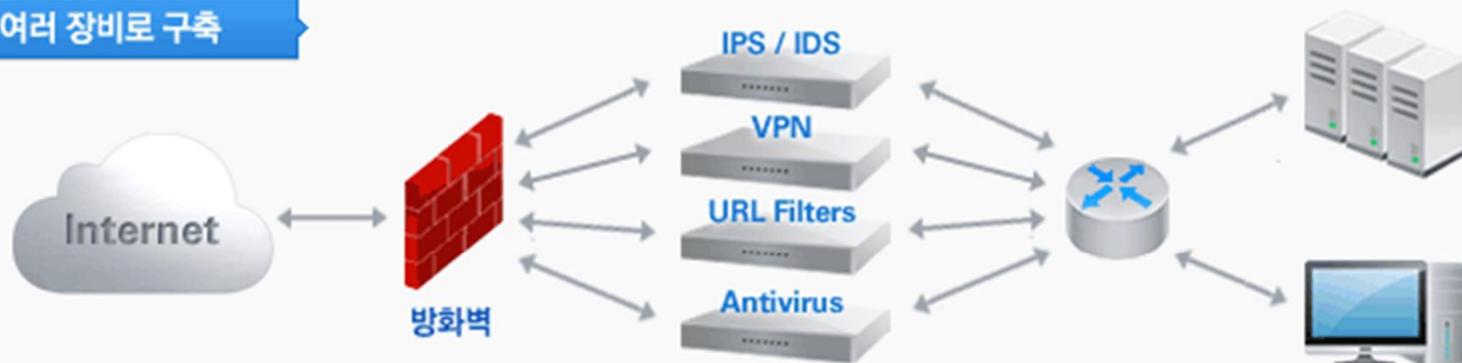
Remote Access VPNs



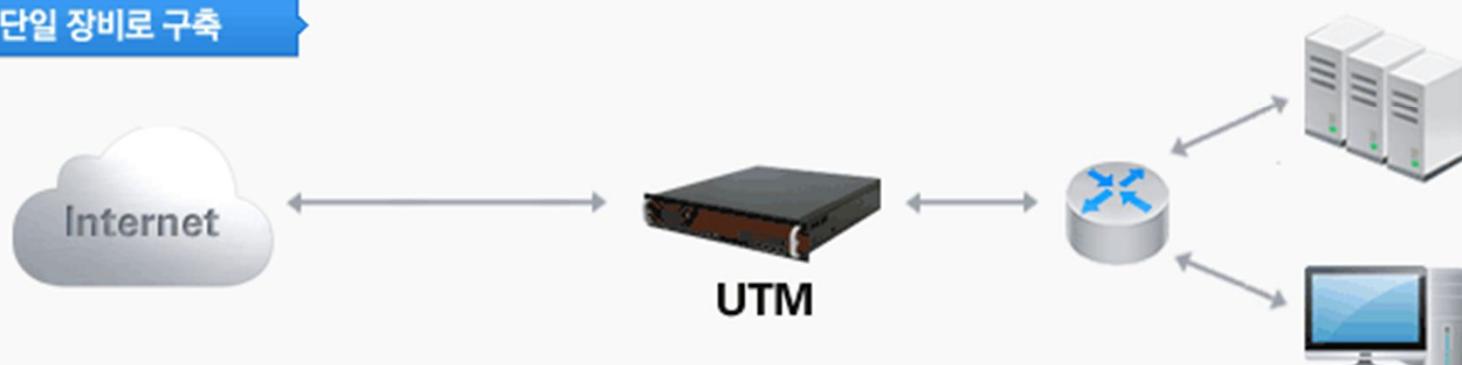
7) UTM (Universal Threat Management)

- 다양한 보안 기능을 하나의 장비로 통합하여 제공하는 보안 솔루션
- 네트워크는 간단해져서 투자 비용은 줄고 관리는 쉬워짐
- 중소 규모의 네트워크를 중심으로 많이 적용되고 있는 장비

복잡한 여러 장비로 구축



UTM 단일 장비로 구축



보안망 구성도

