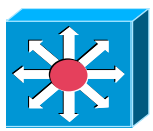
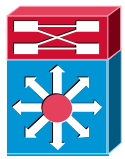
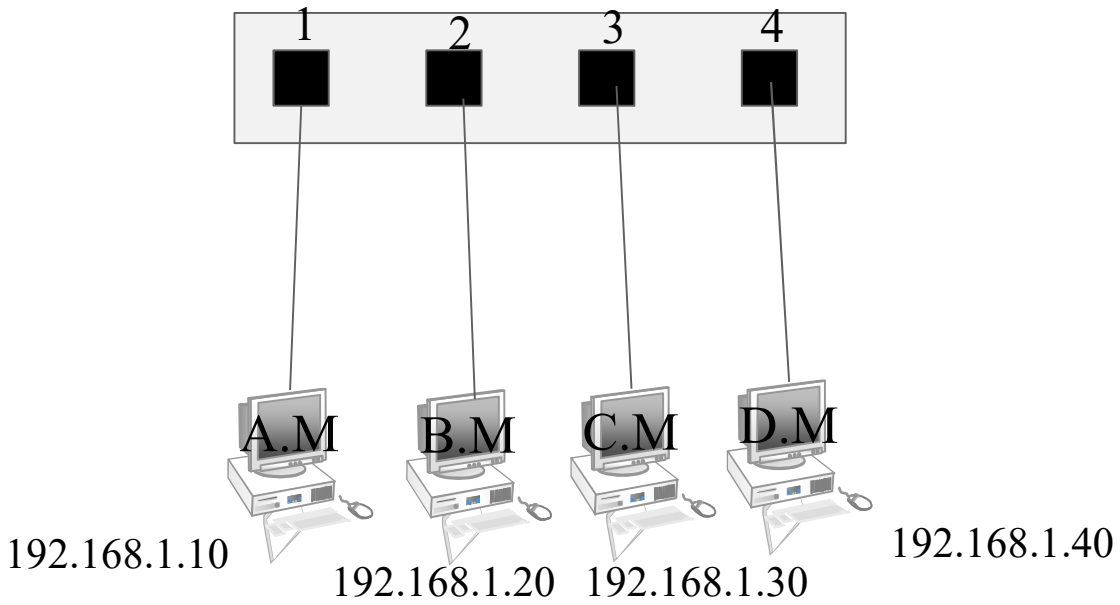
Multilayer Switch & 사내망 구성도

Multilayer Switch(다계층스위치)

구분	L2 Switch	L3 Switch	L4 Switch	L7 Switch
포워딩기준	2계층 (MAC Address)	3계층 (IP Address)	4계층 (IP address + Port 번호)	7계층 (IP address + Port 번호+ Content)
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

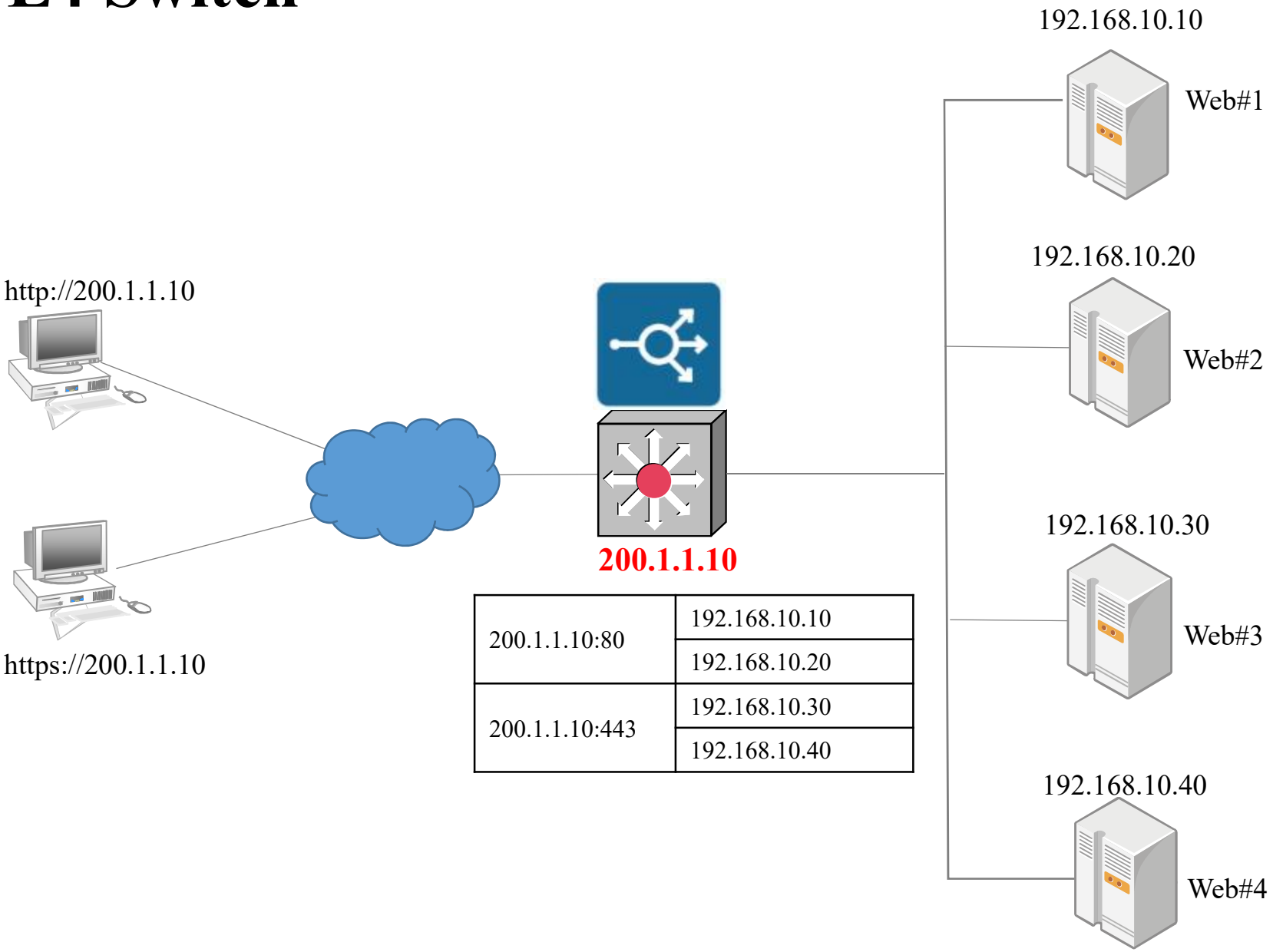






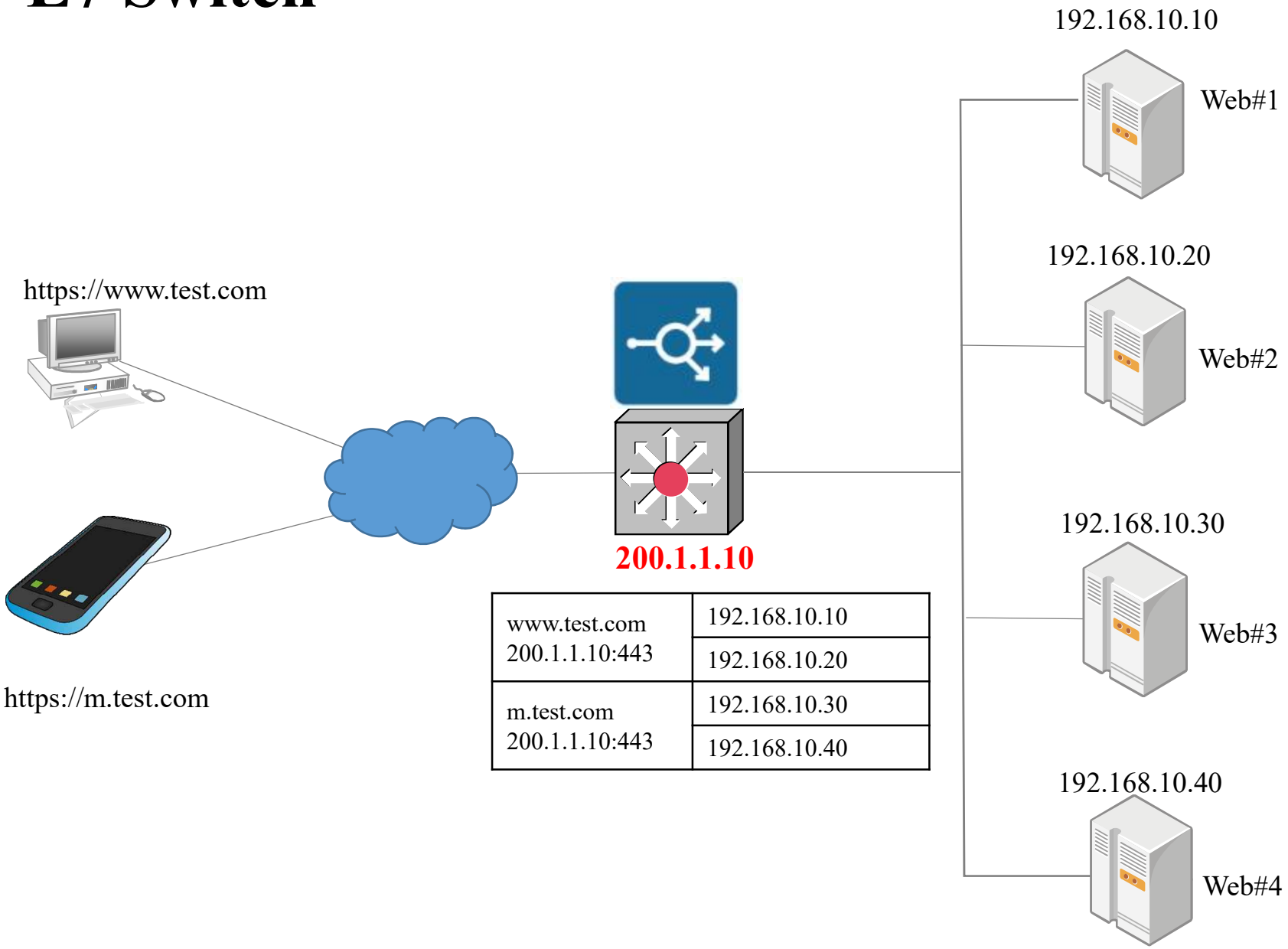
www.test.com	50010	80	192.168.1.10	192.168.4.10	A.M	D.M
	송Port	수Port	송신지IP	수신지IP	송MAC	수MAC

L4 Switch



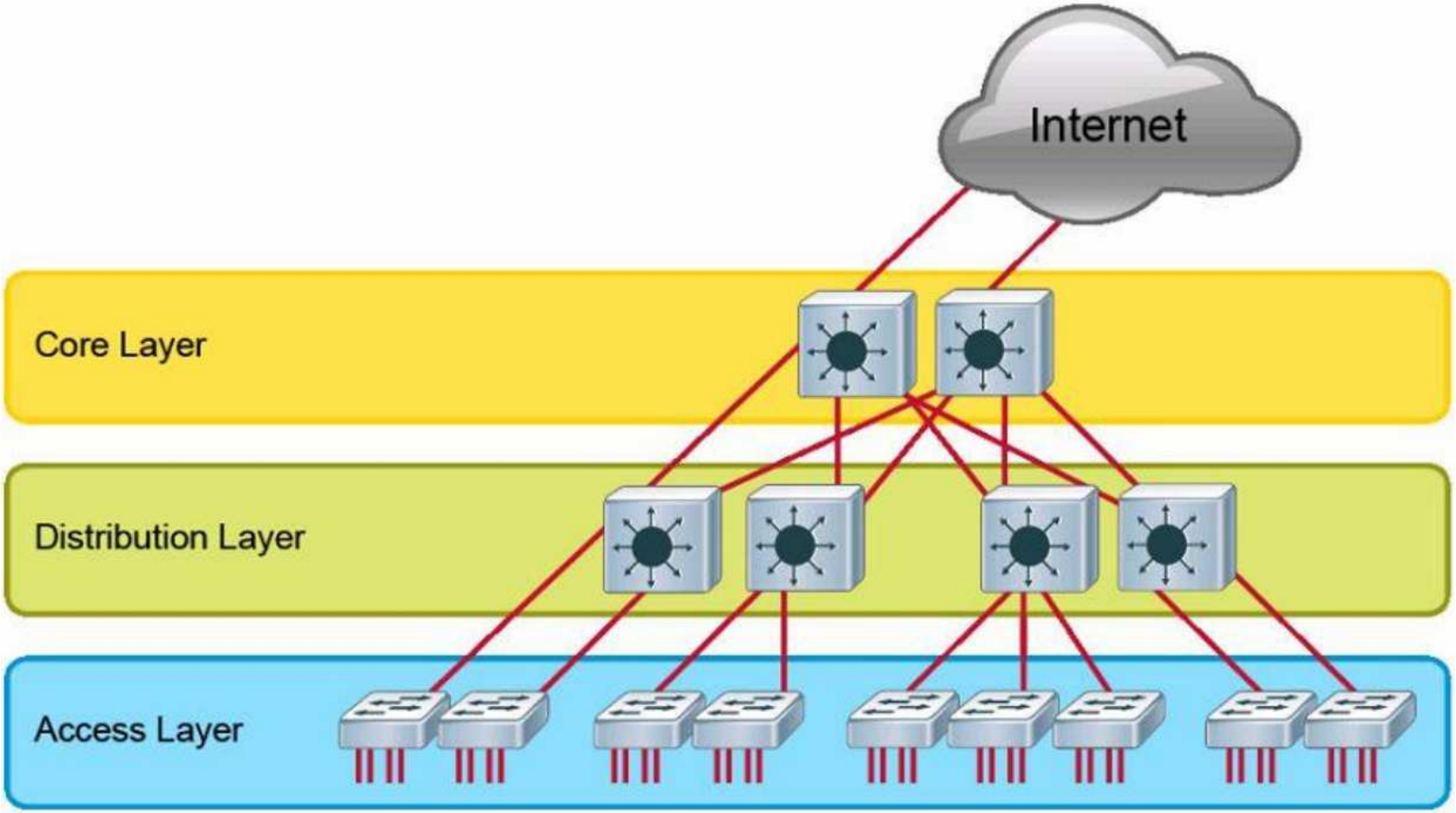
200.1.1.10:80	192.168.10.10
	192.168.10.20
200.1.1.10:443	192.168.10.30
	192.168.10.40

L7 Switch

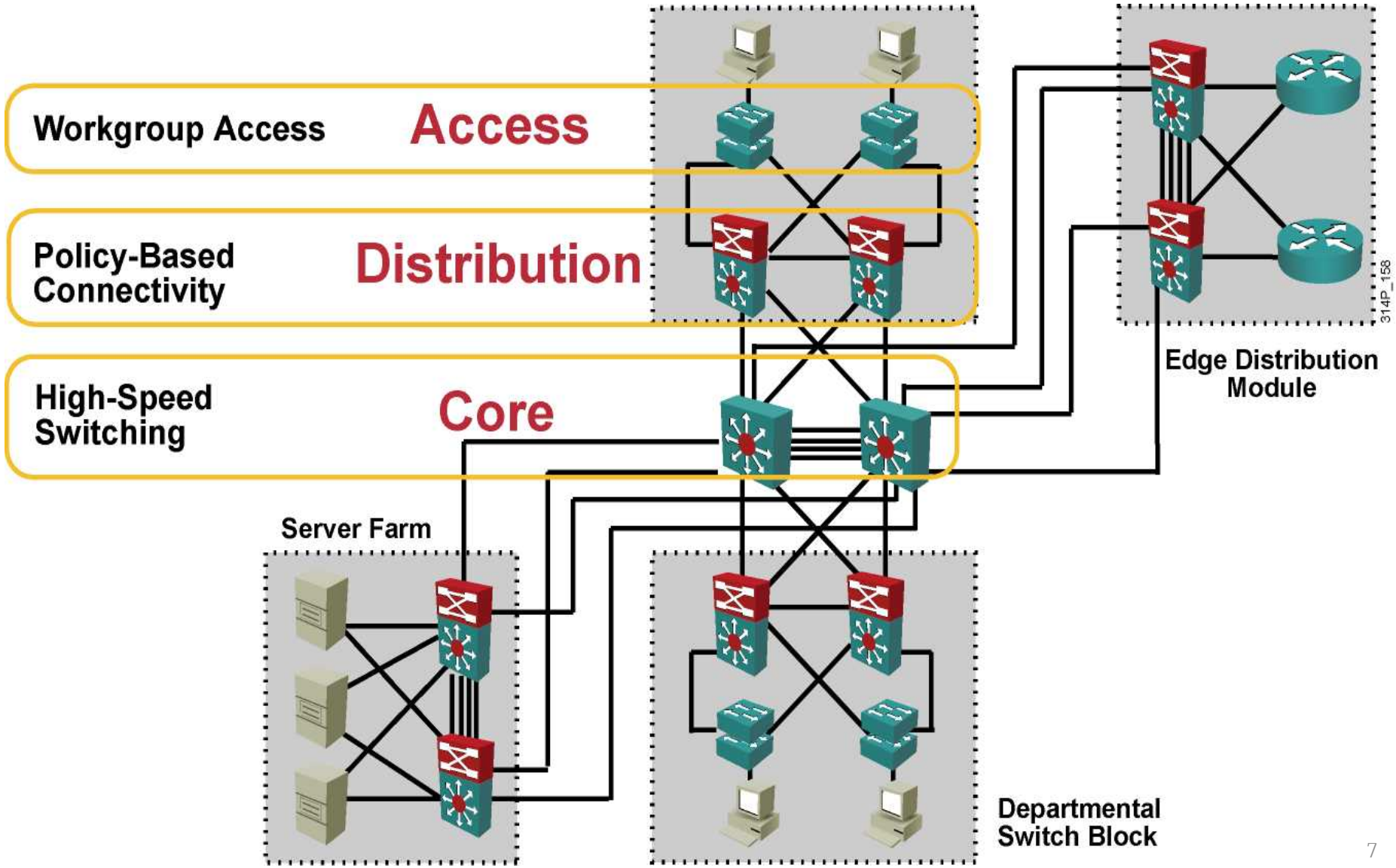


www.test.com 200.1.1.10:443	192.168.10.10
	192.168.10.20
m.test.com 200.1.1.10:443	192.168.10.30
	192.168.10.40

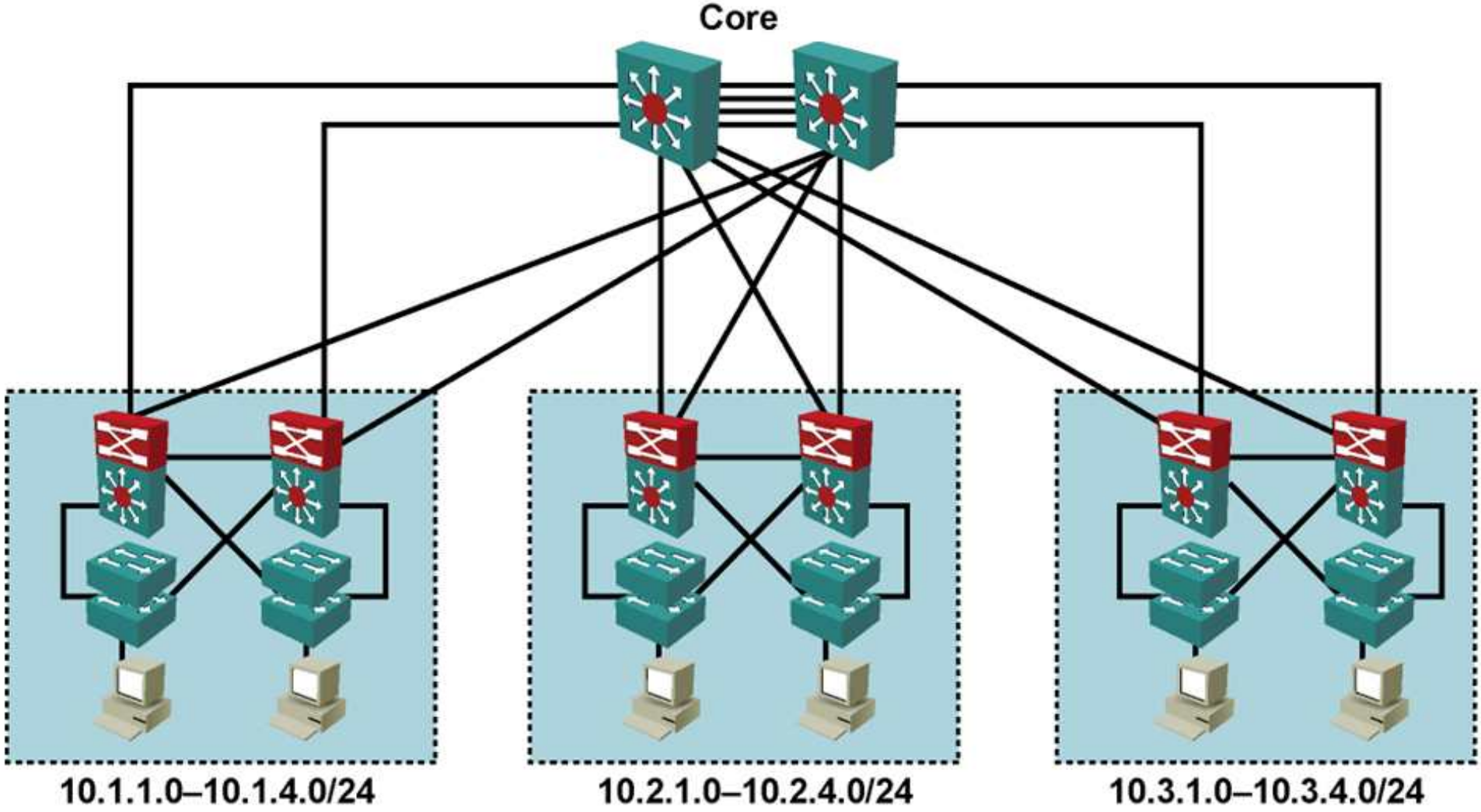
사내망 구성도



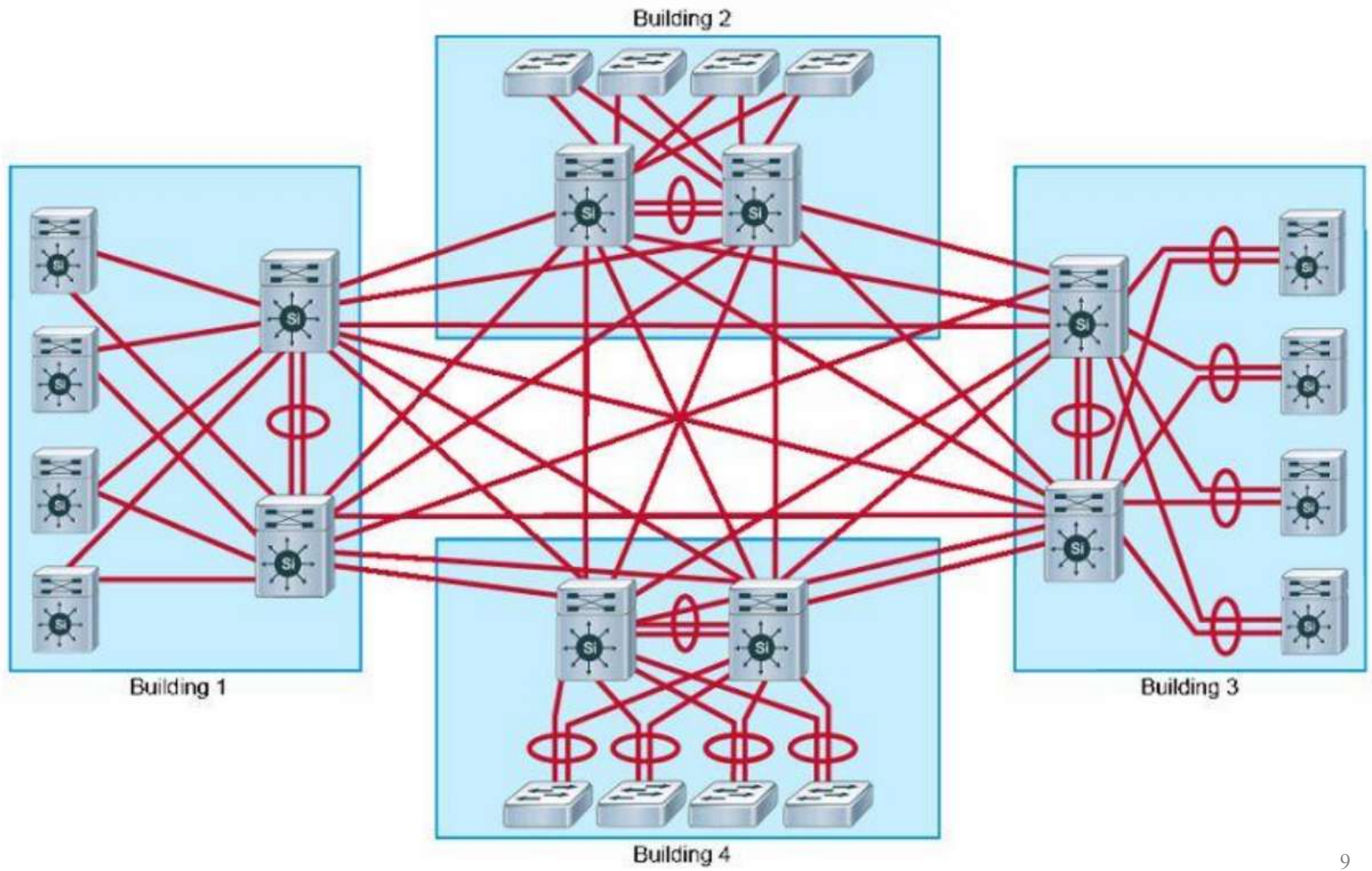
❶ 구성도


Workgroup Access
Access
Policy-Based Connectivity
Distribution
High-Speed Switching
Core
Server Farm
Edge Distribution Module
Departmental Switch Block
314P_158

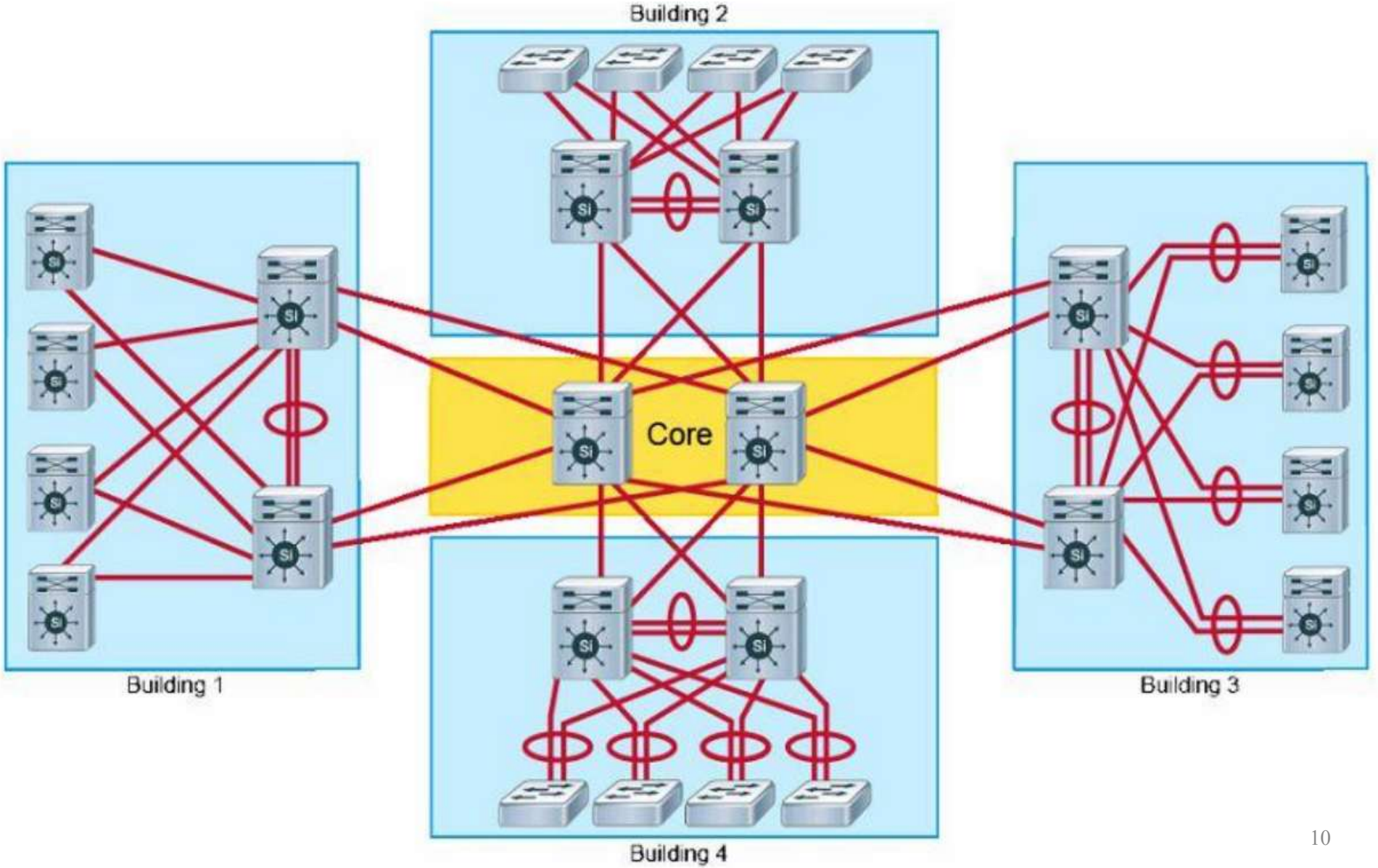
❷ 구성도



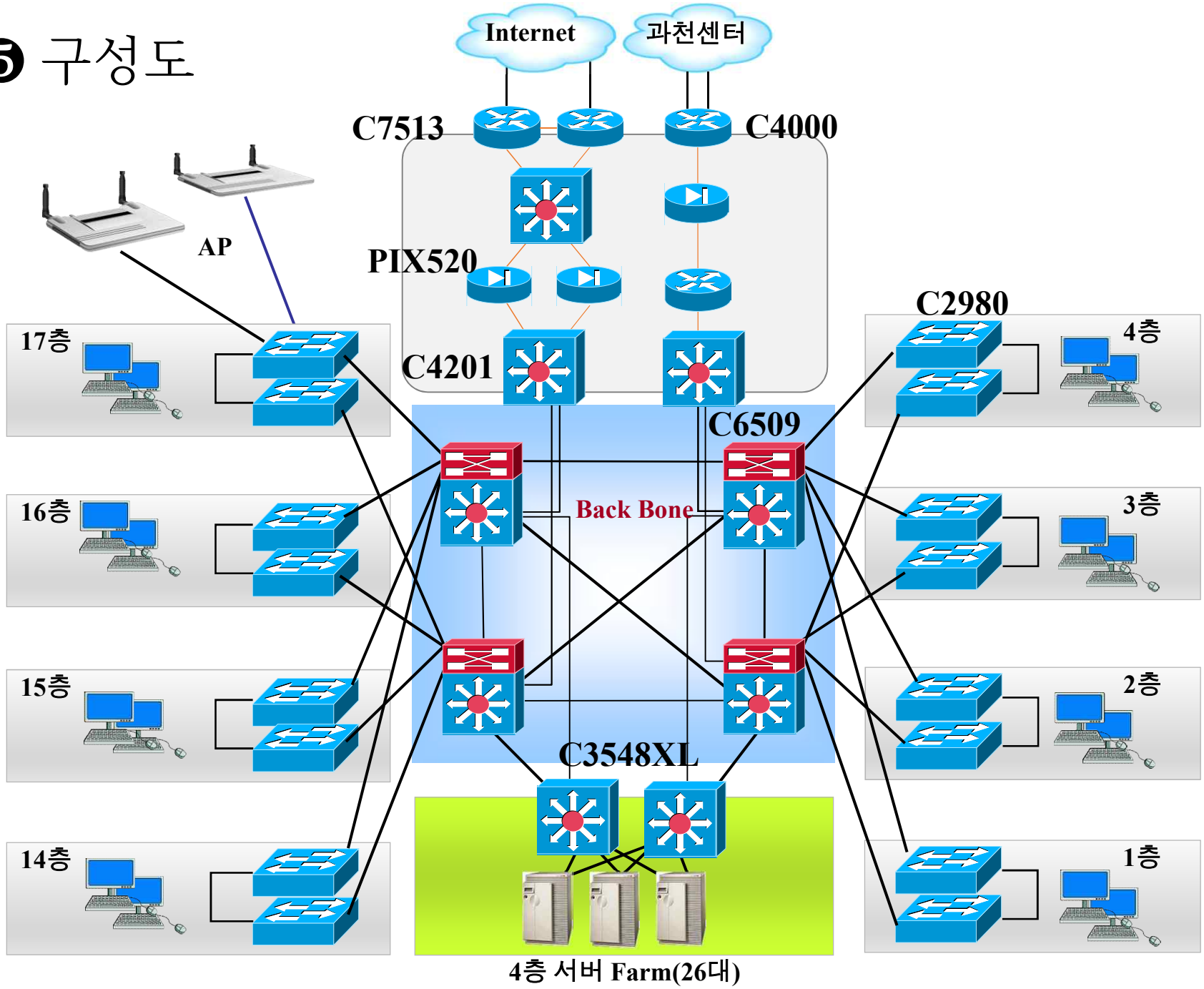
❸ 구성도



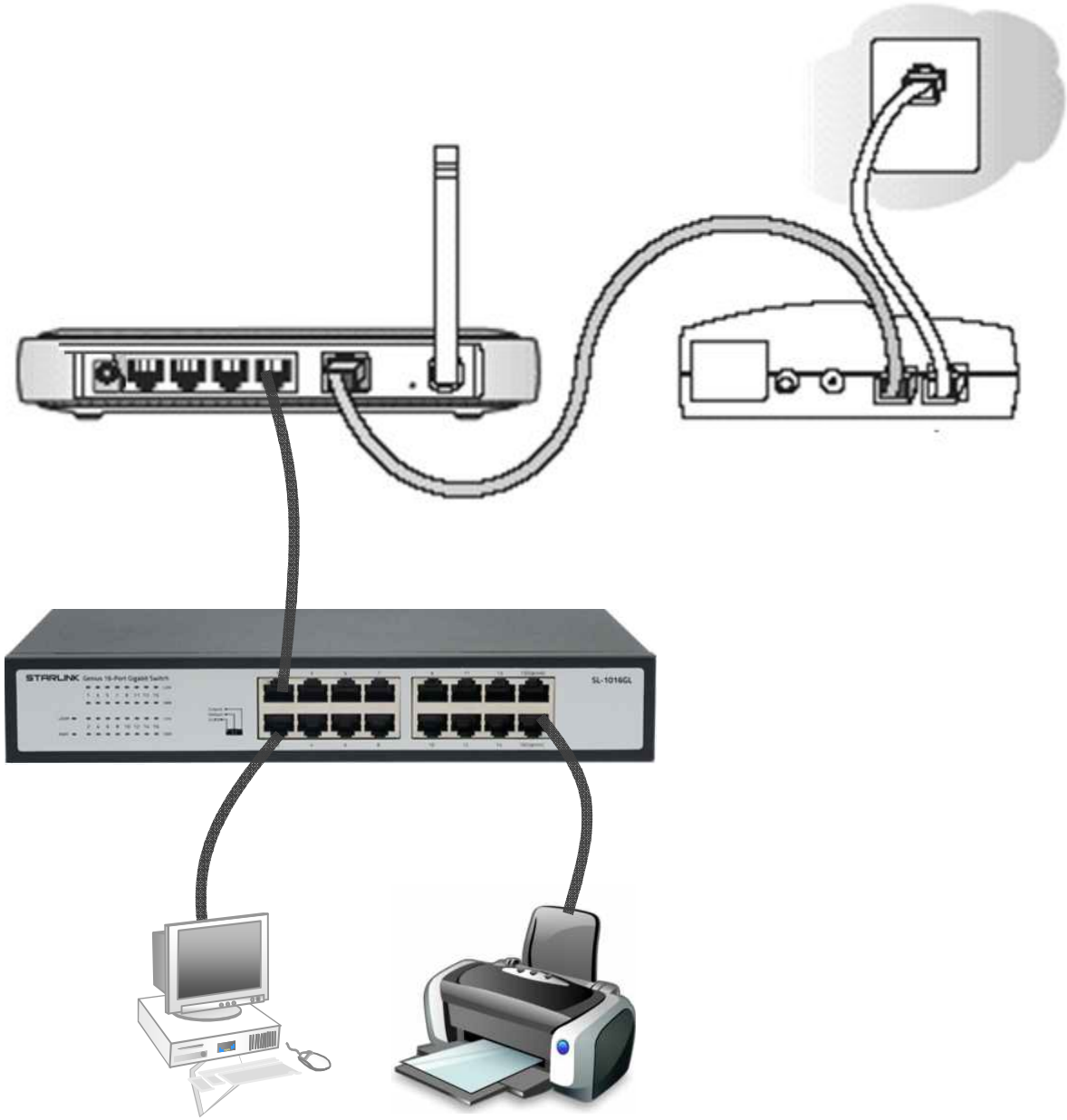
❹ 구성도



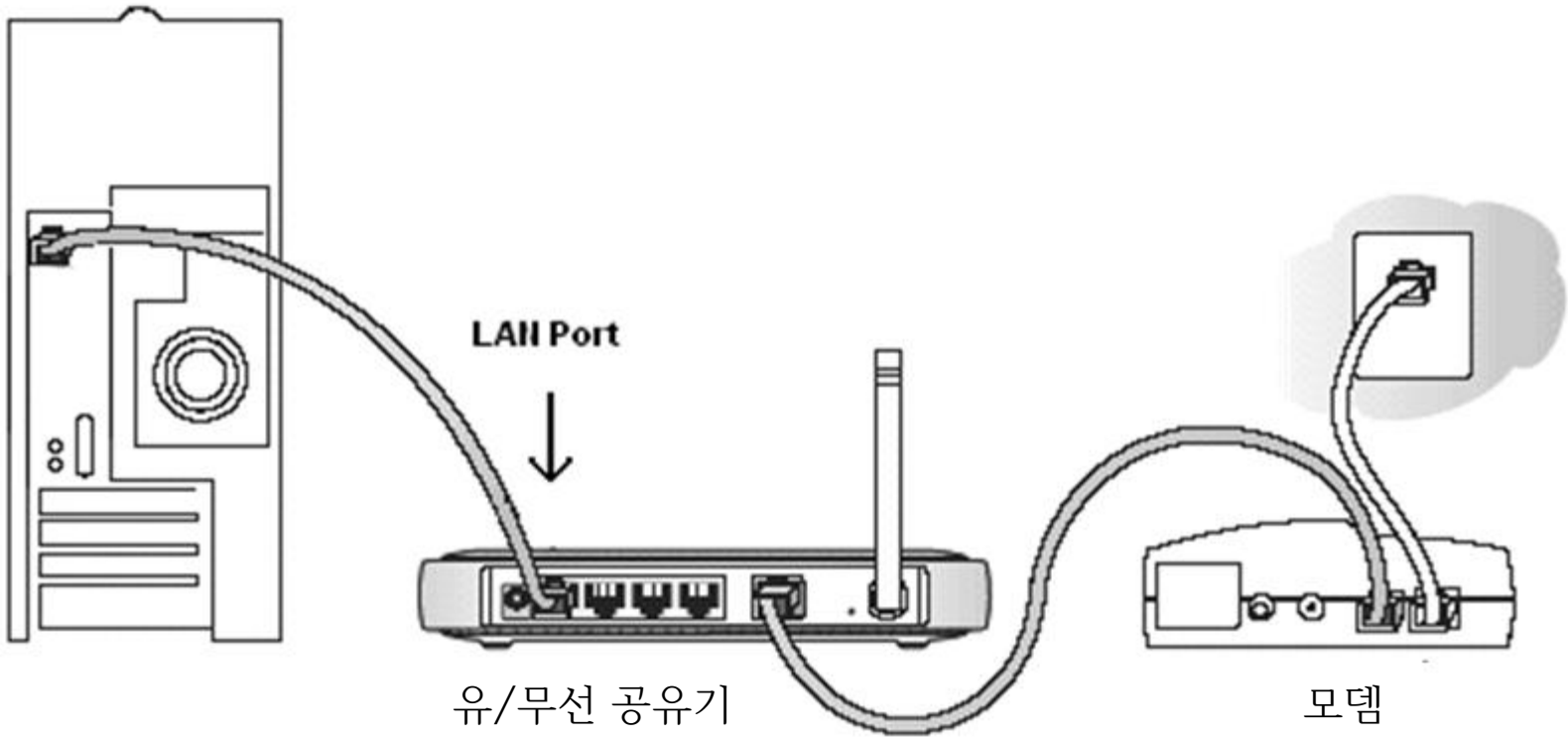
❺ 구성도


Internet
과천센터
C7513
C4000
AP
PIX520
C4201
C2980
C6509
17층
16층
15층
14층
4층
3층
2층
1층
Back Bone
C3548XL
4층 서버 Farm(26대)

❻ 구성도



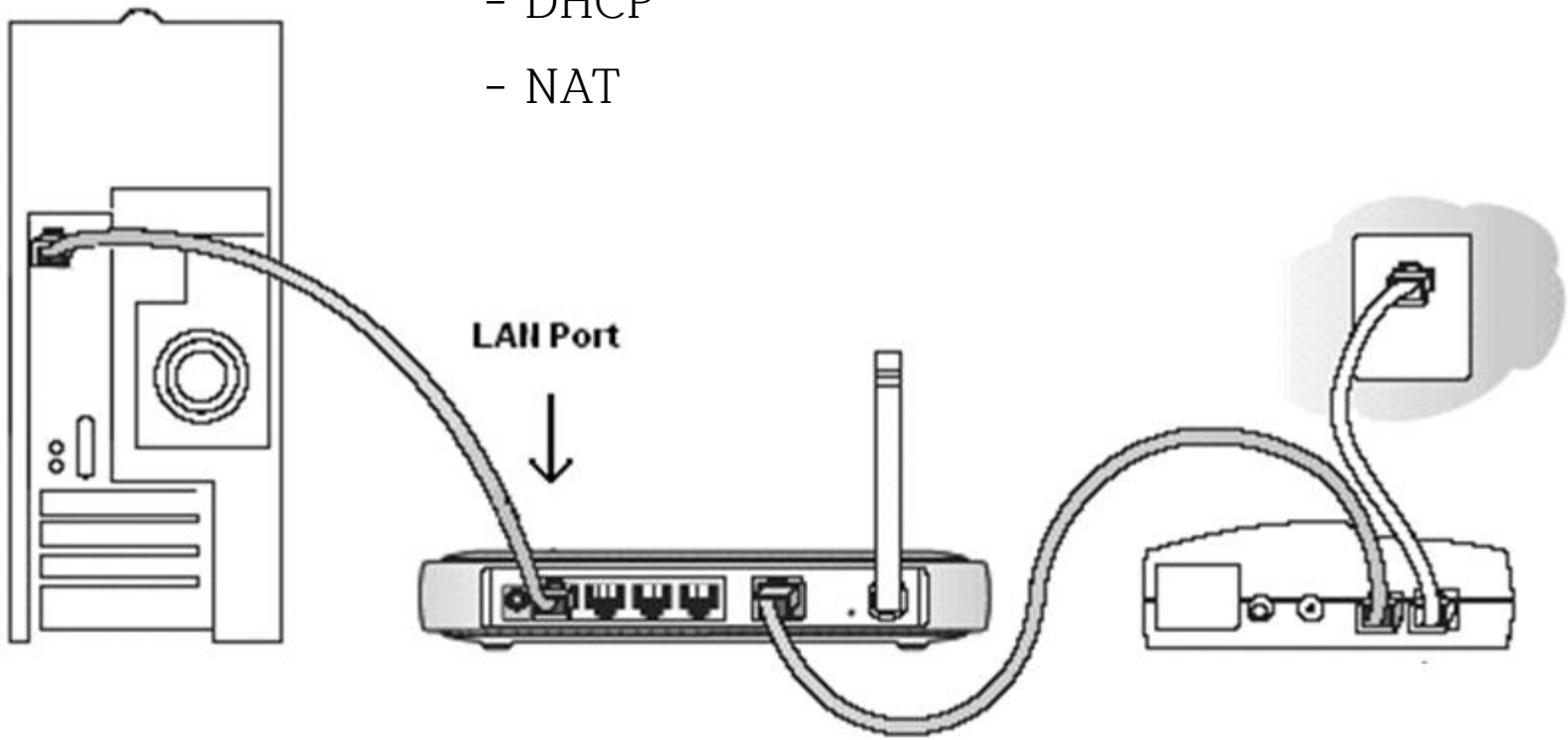
❼ 구성도



NAT(Network Address Translation)

SoHo(Small office/home office)에서의 NAT

- 공유기 기능
  - 패킷 전달
  - DHCP
  - NAT



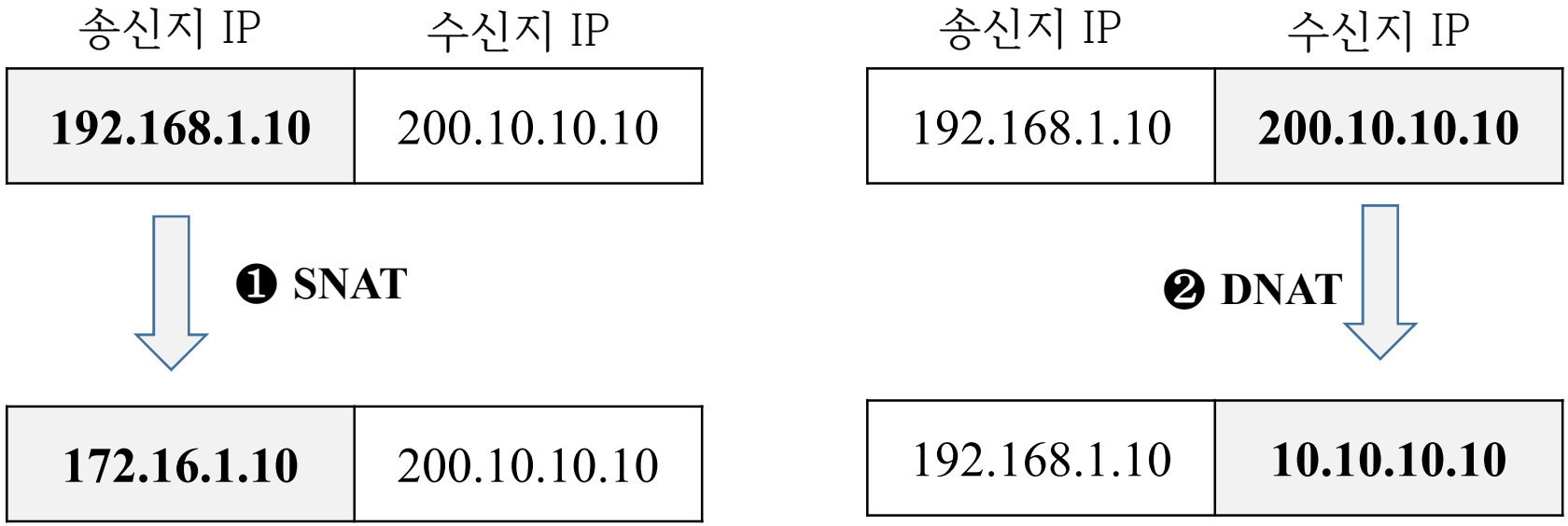
❶ 컴퓨터 ❷ 유/무선 공유기 ❸ 모뎀

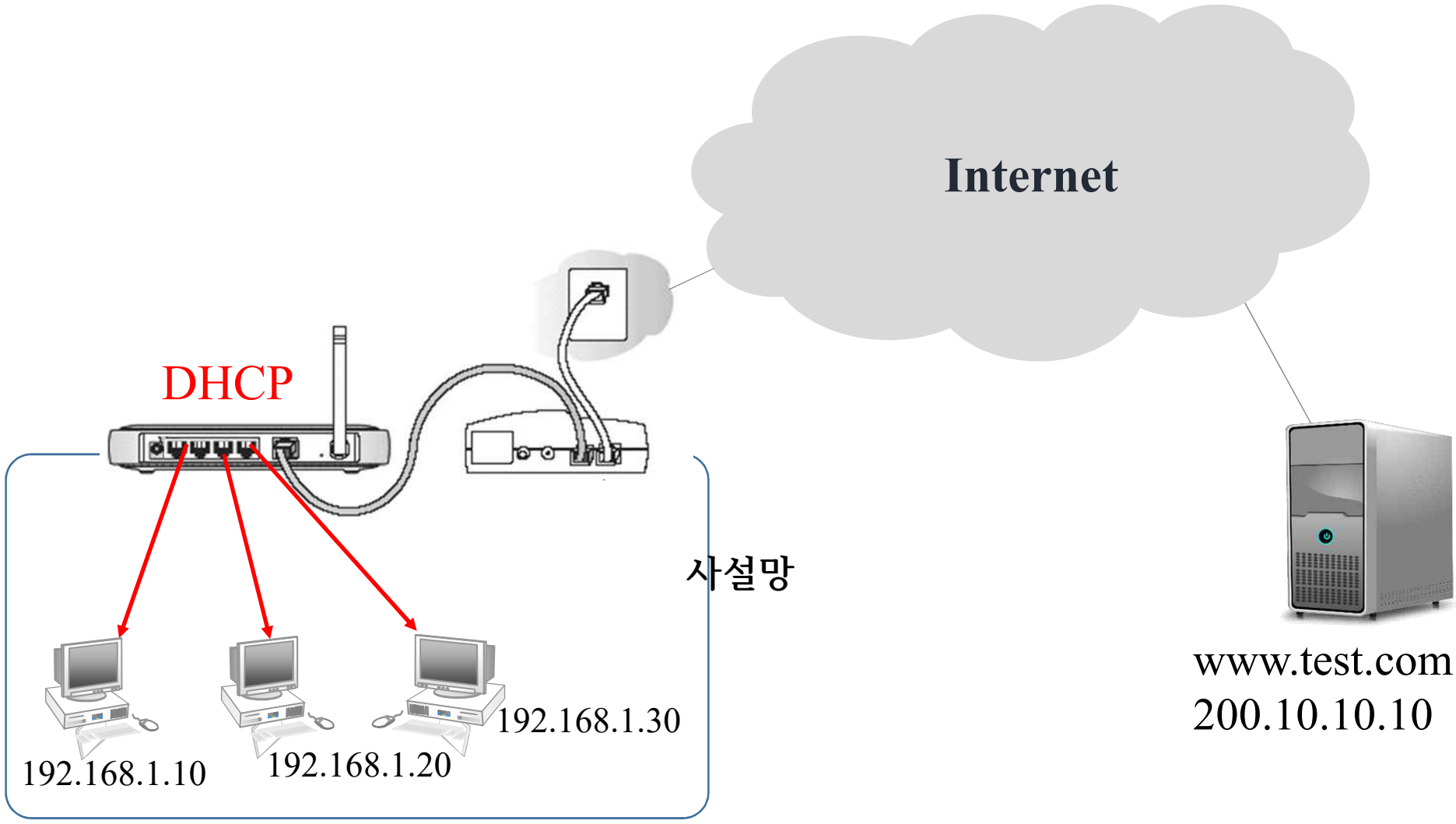
사설/공인 IP Address

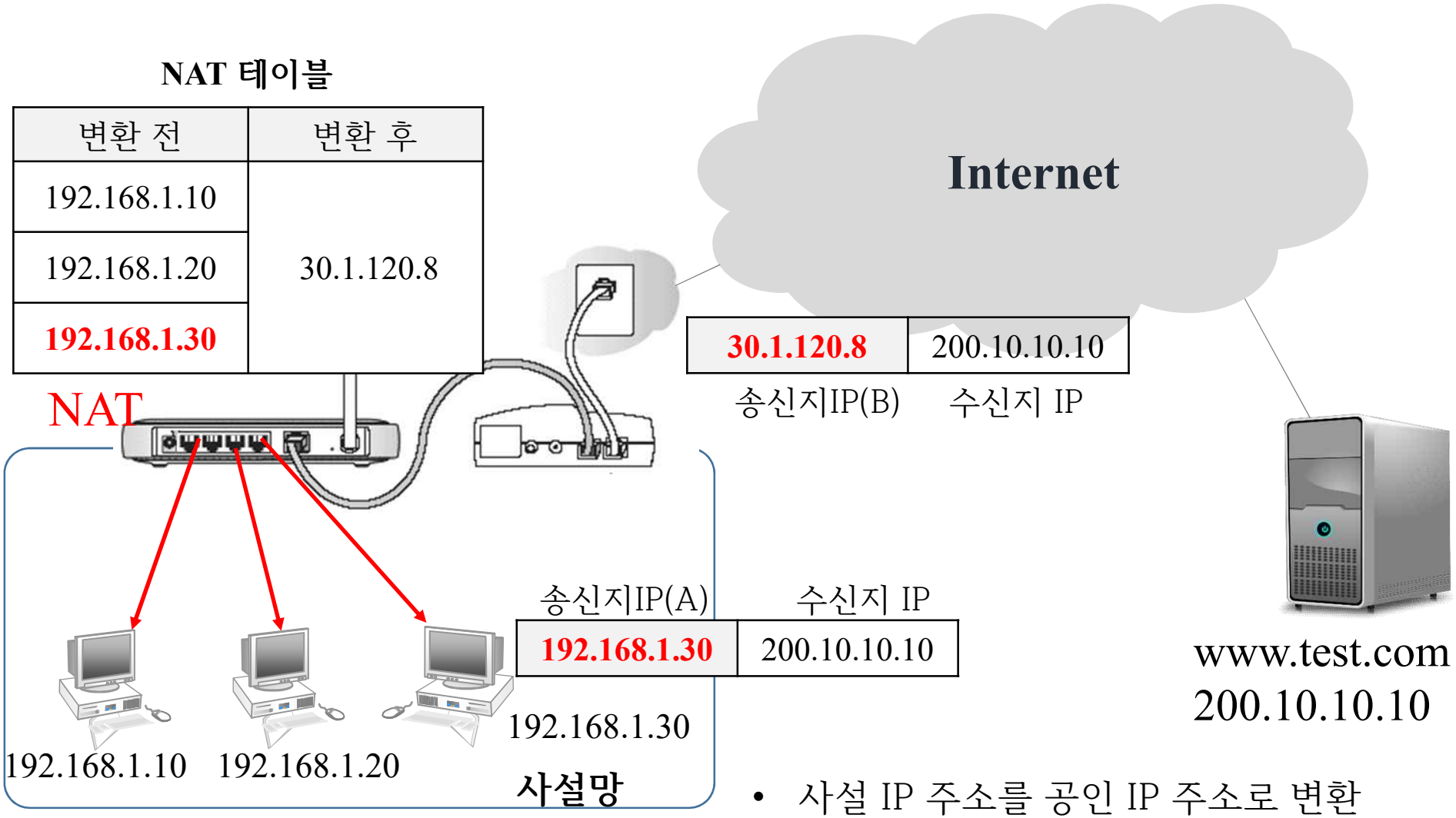
- **사설 IP 주소**
  - 인터넷과 연동되지 않은 사적인 독립 네트워크(Private IP Network)에서 사용되는 사적인 주소
  - 인터넷 상에서 사용할 수 없음을 의미
  - Class 별 사설 IP 주소 대역(IETF RFC 1918)
    ① A Class : 10.x.x.x
    ② B Class : 172.16.x.x ~ 172.31.x.x
    ③ C Class : 192.168.x.x
- **공인 IP주소**
  - 사설 IP주소를 제외한 주소

NAT 기능

- 네트워크 주소 변환 (Network Address Translation)
- 송신지 또는 수신지 IP address를 다른 주소로 변환
- Source NAT(SNAT)와 Destination NAT(DNAT)

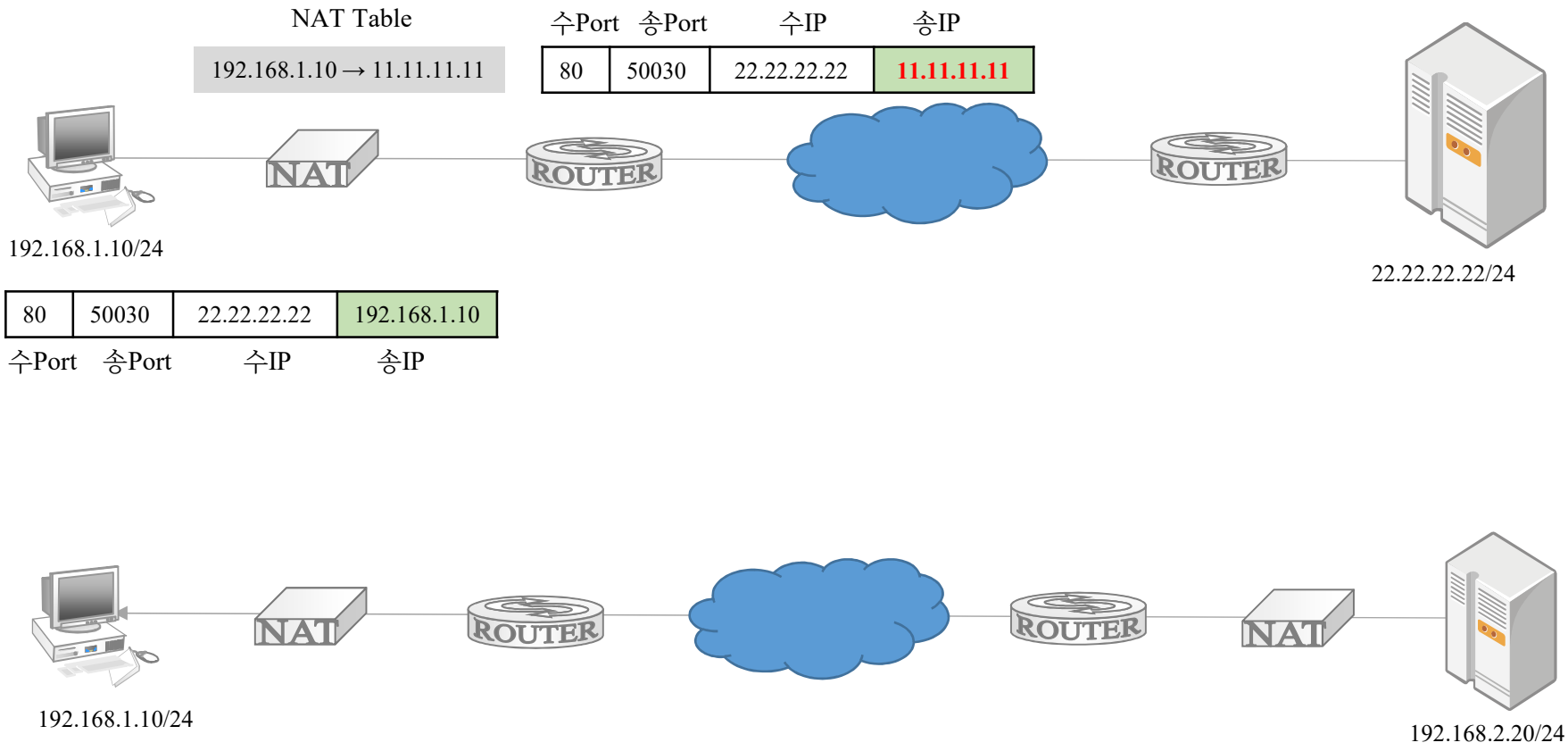


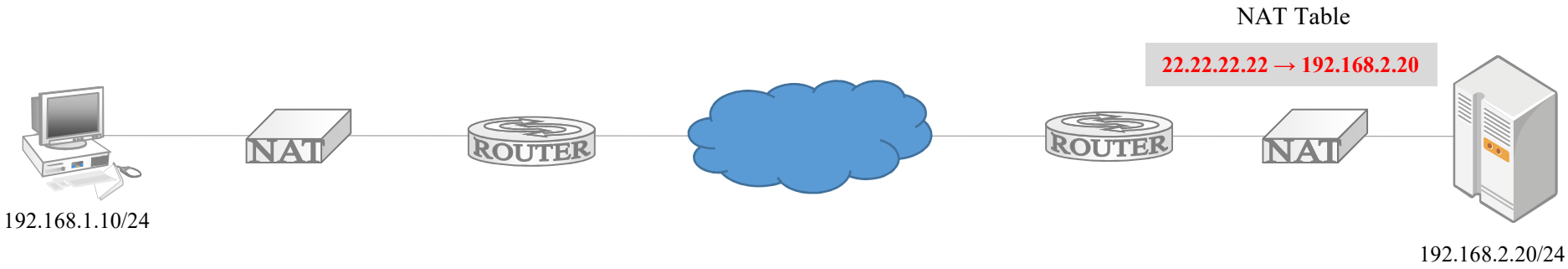

Internet
DHCP
사설망
192.168.1.10
192.168.1.20
192.168.1.30
www.test.com
200.10.10.10



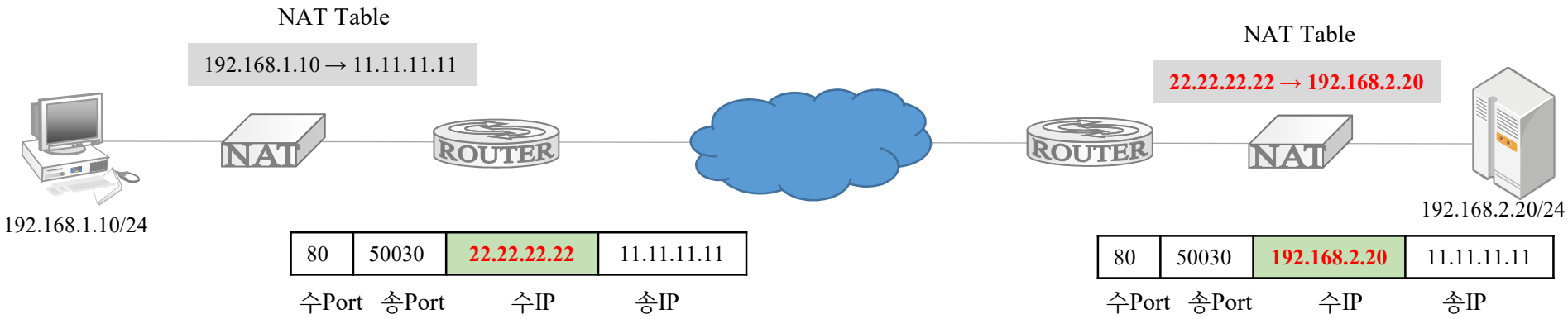
- 사설 IP 주소를 공인 IP 주소로 변환

Source NAT

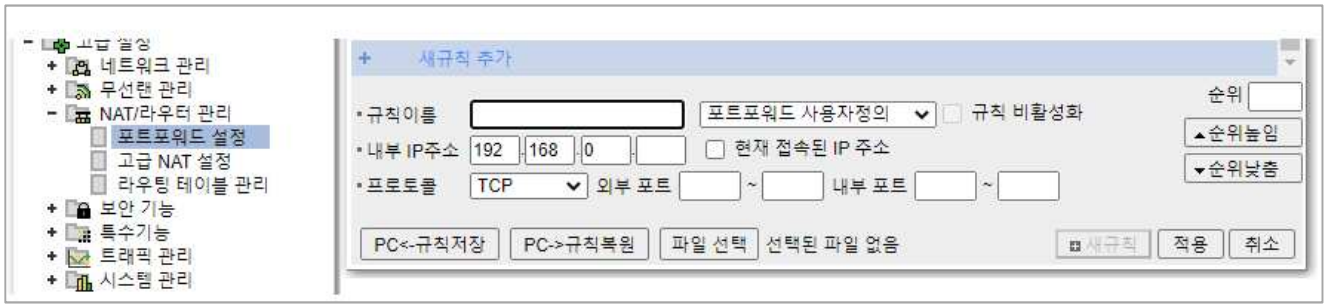

NAT Table
192.168.1.10 → 11.11.11.11
수Port 송Port 수IP 송IP
80 50030 22.22.22.22 11.11.11.11
NAT
ROUTER
ROUTER
192.168.1.10/24
22.22.22.22/24
80 50030 22.22.22.22 192.168.1.10
수Port 송Port 수IP 송IP
NAT
ROUTER
ROUTER
NAT
192.168.1.10/24
192.168.2.20/24



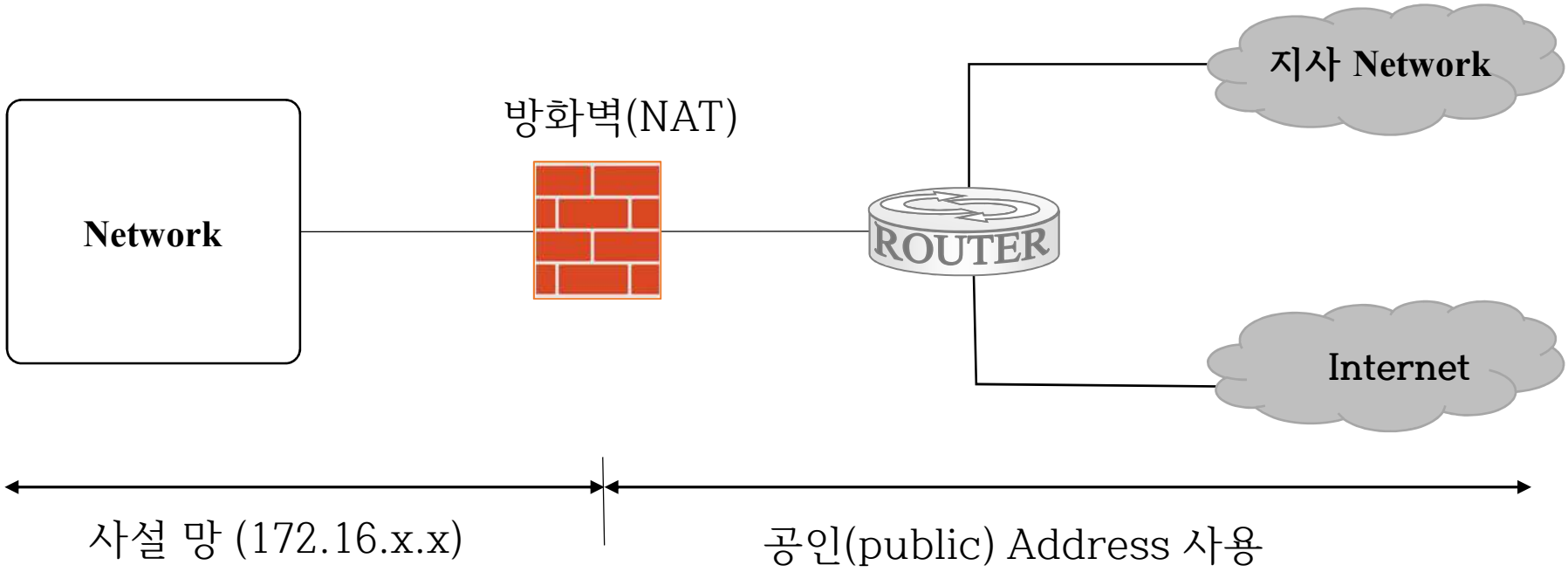
Destination NAT



NAT Port Mapping (Port Forwarding)



기업망에서의 NAT

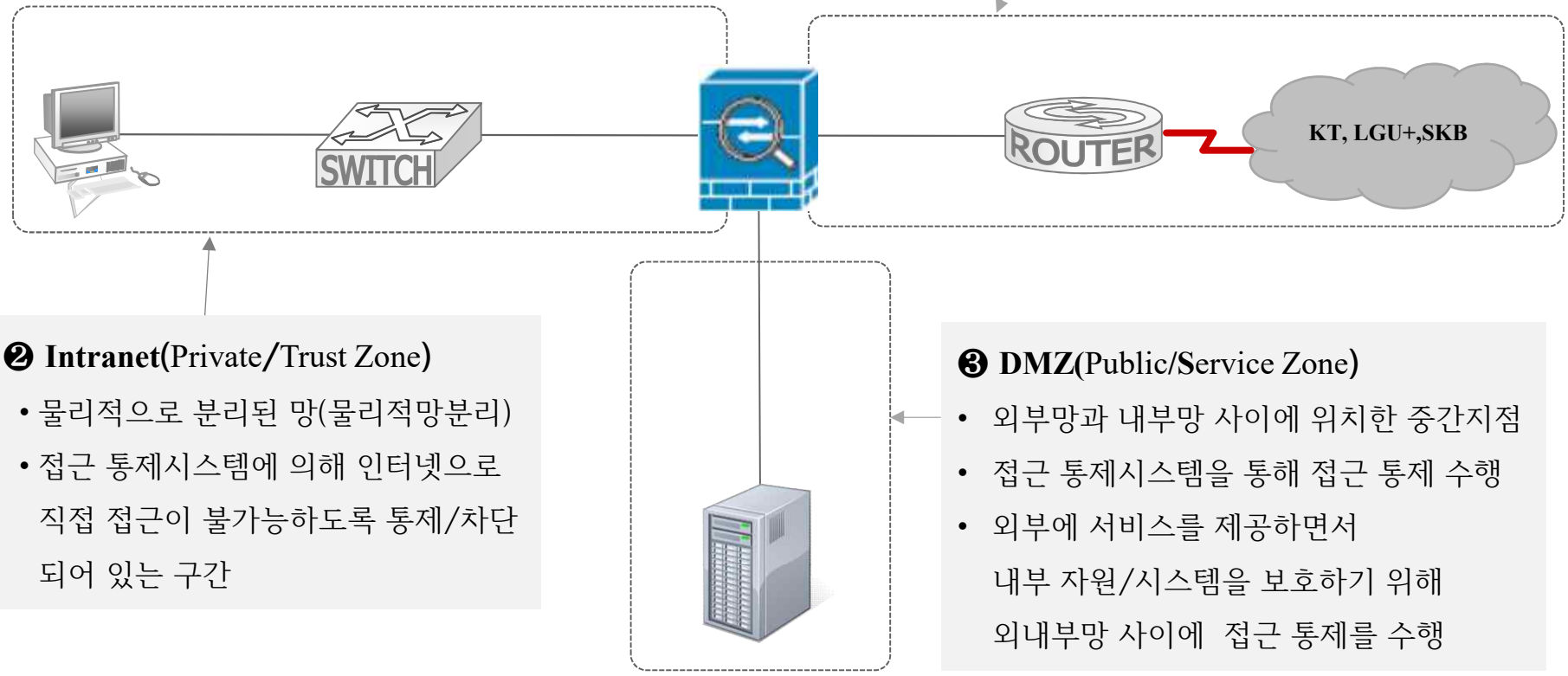

Network
방화벽(NAT)
ROUTER
지사 Network
Internet
사설 망 (172.16.x.x)
공인(public) Address 사용

보안망 구성(1)

보안망 구성도

❶ Internet(Untrust Zone)

• 인터넷을 통해 외부에서 직접 접근이 가능한 구간



❷ Intranet(Private/Trust Zone)

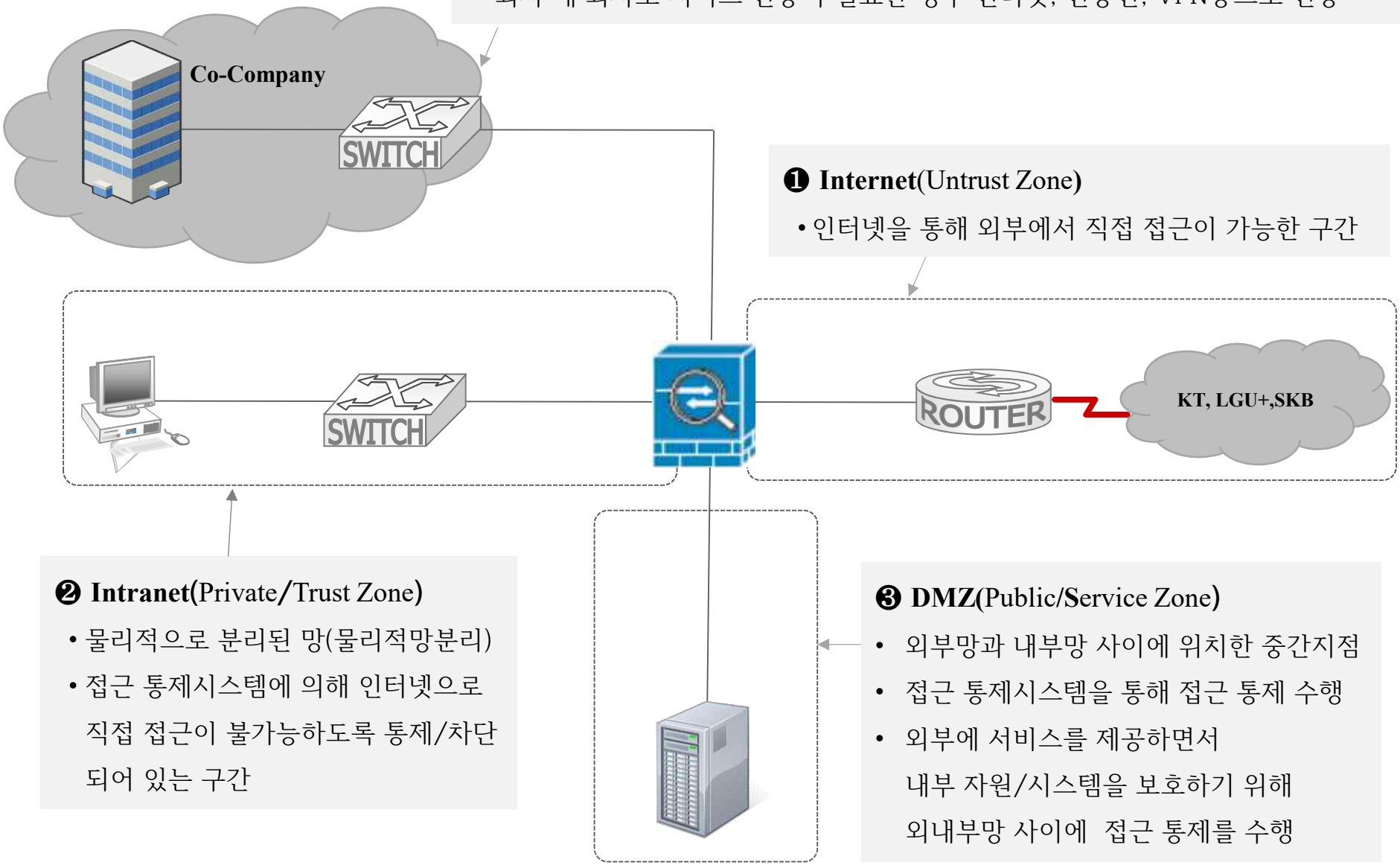
- 물리적으로 분리된 망(물리적망분리)
- 접근 통제시스템에 의해 인터넷으로 직접 접근이 불가능하도록 통제/차단 되어 있는 구간

❸ 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

❹ Extranet (대외망)

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



❶ Internet(Untrust Zone)

• 인터넷을 통해 외부에서 직접 접근이 가능한 구간

❷ Intranet(Private/Trust Zone)

• 물리적으로 분리된 망(물리적망분리)

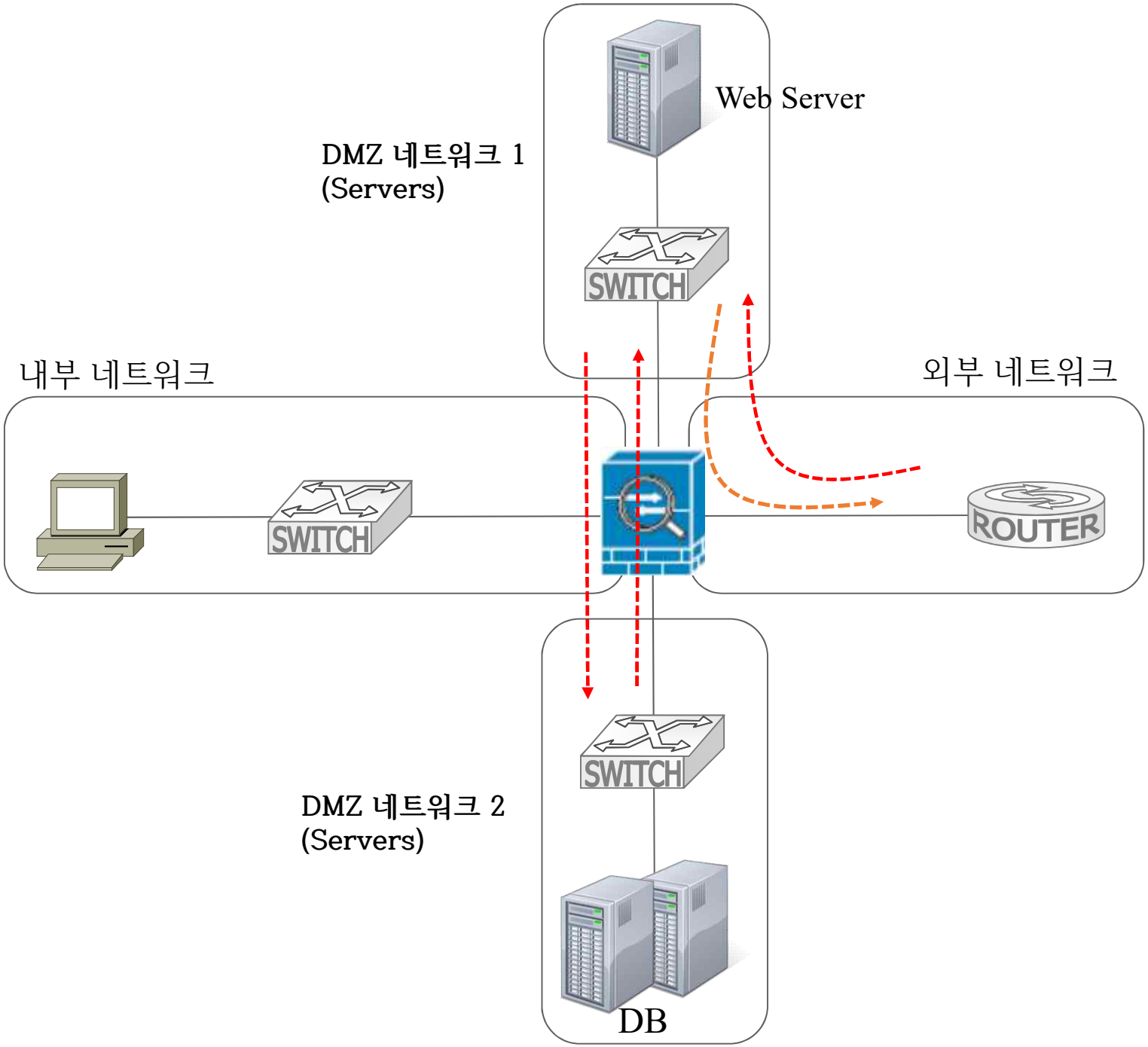
• 접근 통제시스템에 의해 인터넷으로 직접 접근이 불가능하도록 통제/차단 되어 있는 구간

❸ DMZ(Public/Service Zone)

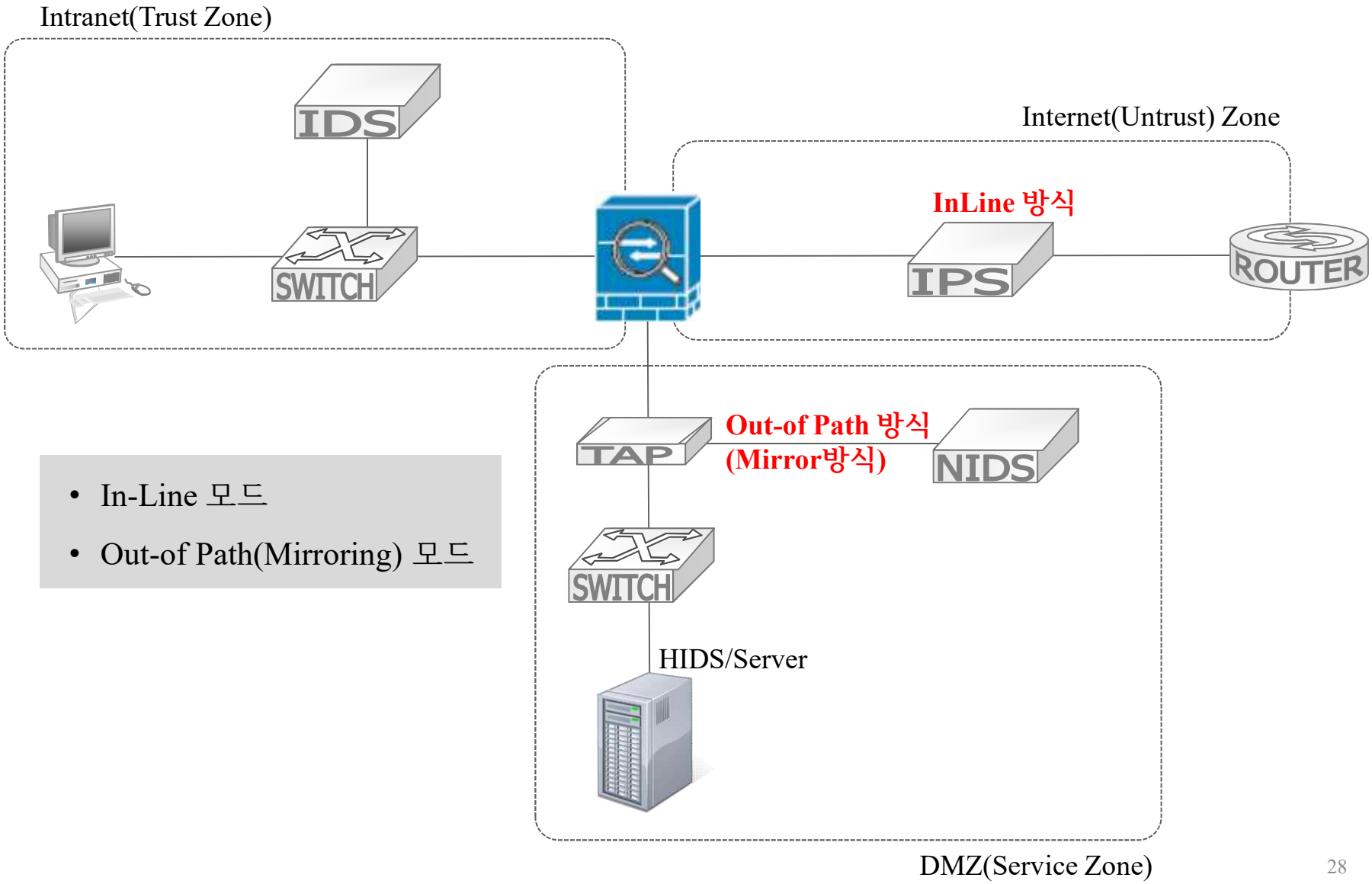
• 외부망과 내부망 사이에 위치한 중간지점

• 접근 통제시스템을 통해 접근 통제 수행

• 외부에 서비스를 제공하면서 내부 자원/시스템을 보호하기 위해 외내부망 사이에 접근 통제를 수행

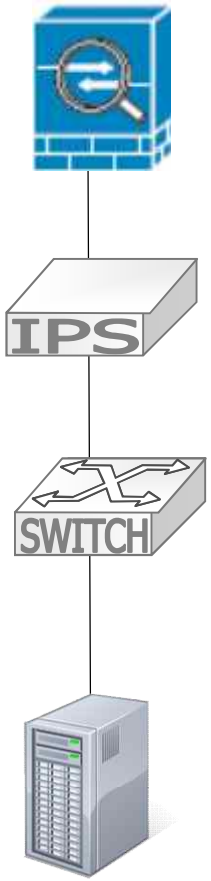

Web Server
DMZ 네트워크 1
(Servers)
SWITCH
내부 네트워크
외부 네트워크
SWITCH
ROUTER
SWITCH
DMZ 네트워크 2
(Servers)
DB

보안 장비 설치 모드



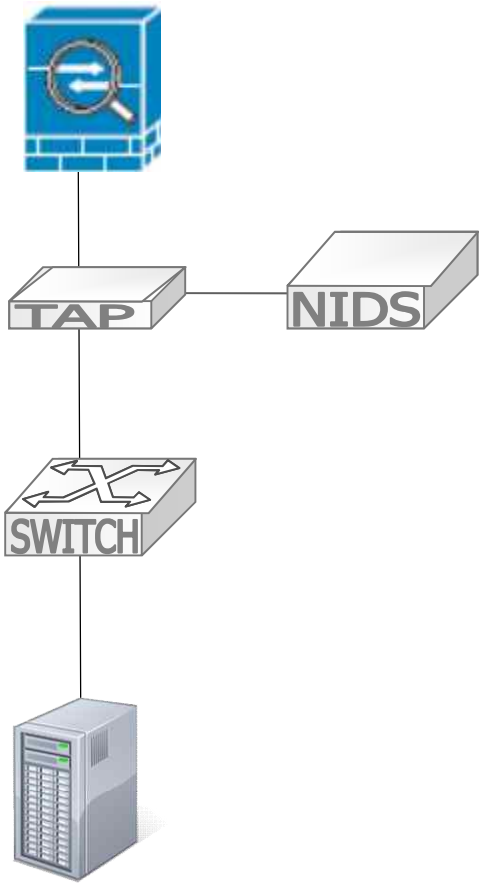
- In-Line 모드
- Out-of Path(Mirroring) 모드

InLine 모드



- 물리적 네트워크 경로 상에 보안장비를 설치
- 네트워크을 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



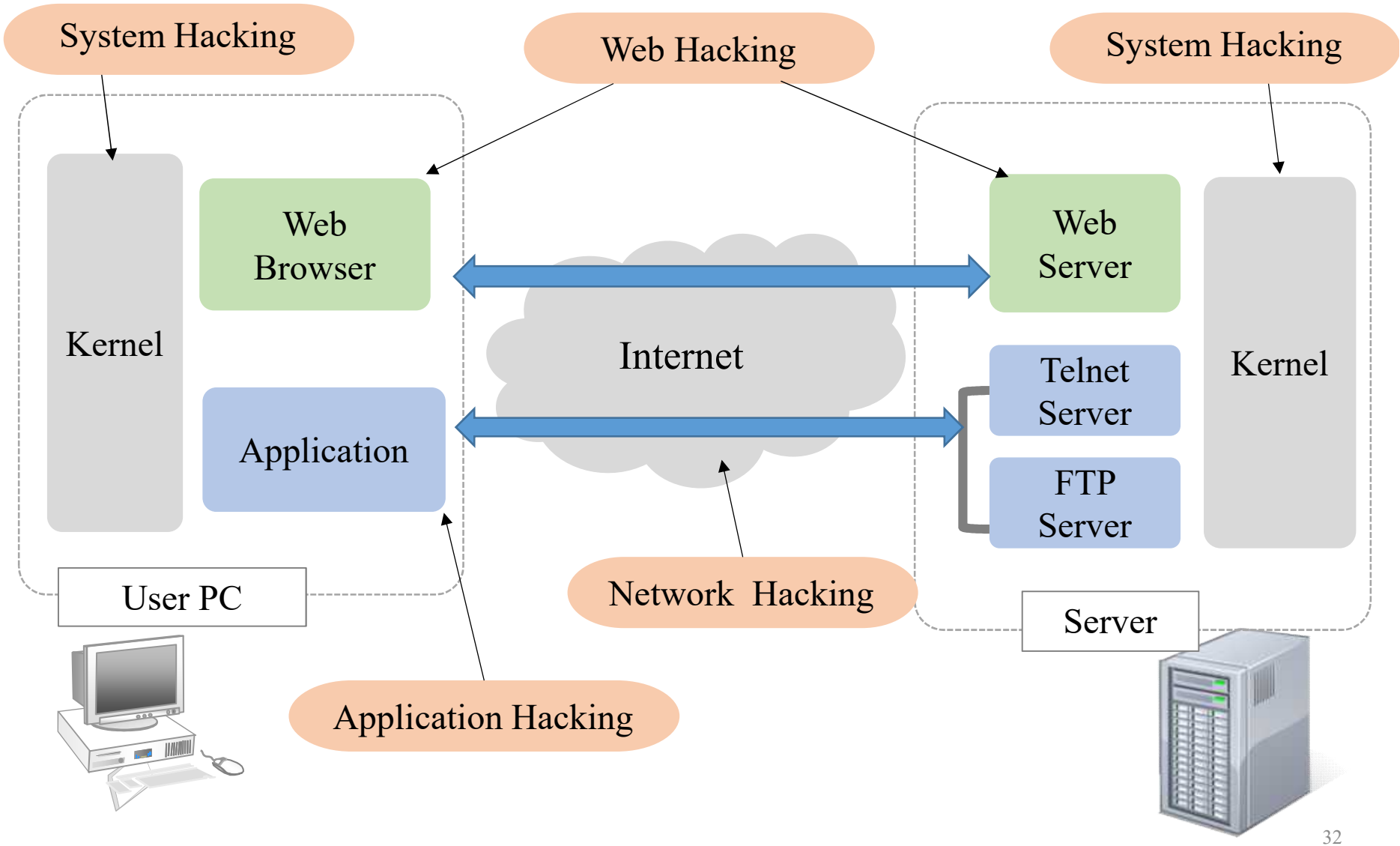
- 미러링 장비(예. TAP)를 통해 복제된 패킷을 받아서 탐지하는 모드
- 패킷 차단 기능이 없는 탐지 목적의 장비에 적용

  - 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

네트워크 보안 솔루션

공격 종류


System Hacking
Web Hacking
System Hacking
Kernel
Web
Browser
Web
Server
Internet
Application
Telnet
Server
FTP
Server
Kernel
User PC
Network Hacking
Server
Application Hacking

Hardening(하드닝)

- ‘정보를 저장하고 있는 **컴퓨터나 네트워크 등과 같은 환경을 굳건하게 한다**’는 뜻
- ‘요새화’라 부르는 경우도 있음
  - 외부에 공개하는 서비스의 국소화
  - 작동하는 있는 것의 파악
  - 불필요한 프로그램 실행 중지
  - 취약성을 수정하는 패치의 신속한 적용
  - 보안 소프트웨어나 기기의 도입
  - ‘OS나 네트워크 기기 등의 다층방어 '

네트워크 보안 솔루션

❶ Firewall

❷ IDS(Intrusion Detection System)

❸ IPS(Intrusion Prevention System)

❹ WAF(Web Application Firewall)

❺ NAC(Network Access Control)

❻ VPN(Virtual Private Network)

❼ UTM(Unified Threat Management)

❽ Anti-DDoS system

❶ 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

<table>
<tr><th>트래픽방향</th><th>사용자</th><th>송신지IP</th><th>수신지IP</th><th>허용포트</th><th>시간대</th><th>Permit /Deny</th></tr>
<tr><td>외부→내부</td><td></td><td colspan="5">몇몇 서비스를 제외한 모든 서비스 불가</td></tr>
<tr><td>외부→DMZ</td><td>모든사용자</td><td>모든 네트워크</td><td>DMZ 네트워크</td><td>HTTP, SMTP POP3</td><td>모든 시간대</td><td rowspan="4">Permit</td></tr>
<tr><td>내부→외부</td><td>내부 네트워크 모든 사용자</td><td>내부 네트워크</td><td>모든 네트워크</td><td>의심포트 권고 사항을 제외한 대부분 모든 포트 허용</td><td>특정 커뮤니티 웹 사이트 근무 시간대 제외</td></tr>
<tr><td>내부→DMZ</td><td>인증을 거친 사용자</td><td>내부 네트워크</td><td>DMZ 네트워크</td><td>HTTP, SMTP POP3</td><td>모든 시간대</td></tr>
<tr><td>DMZ→외부</td><td>DMZ 네트워크 사용자</td><td>DMZ 네트워크</td><td>모든 네트워크</td><td>HTTP, SMTP POP3</td><td>모든 시간대</td></tr>
<tr><td>DMZ→내부</td><td colspan="6">VOIP SIP를 제외한 모든 서비스 불가</td></tr>
</table>

* P2P 사용 포트

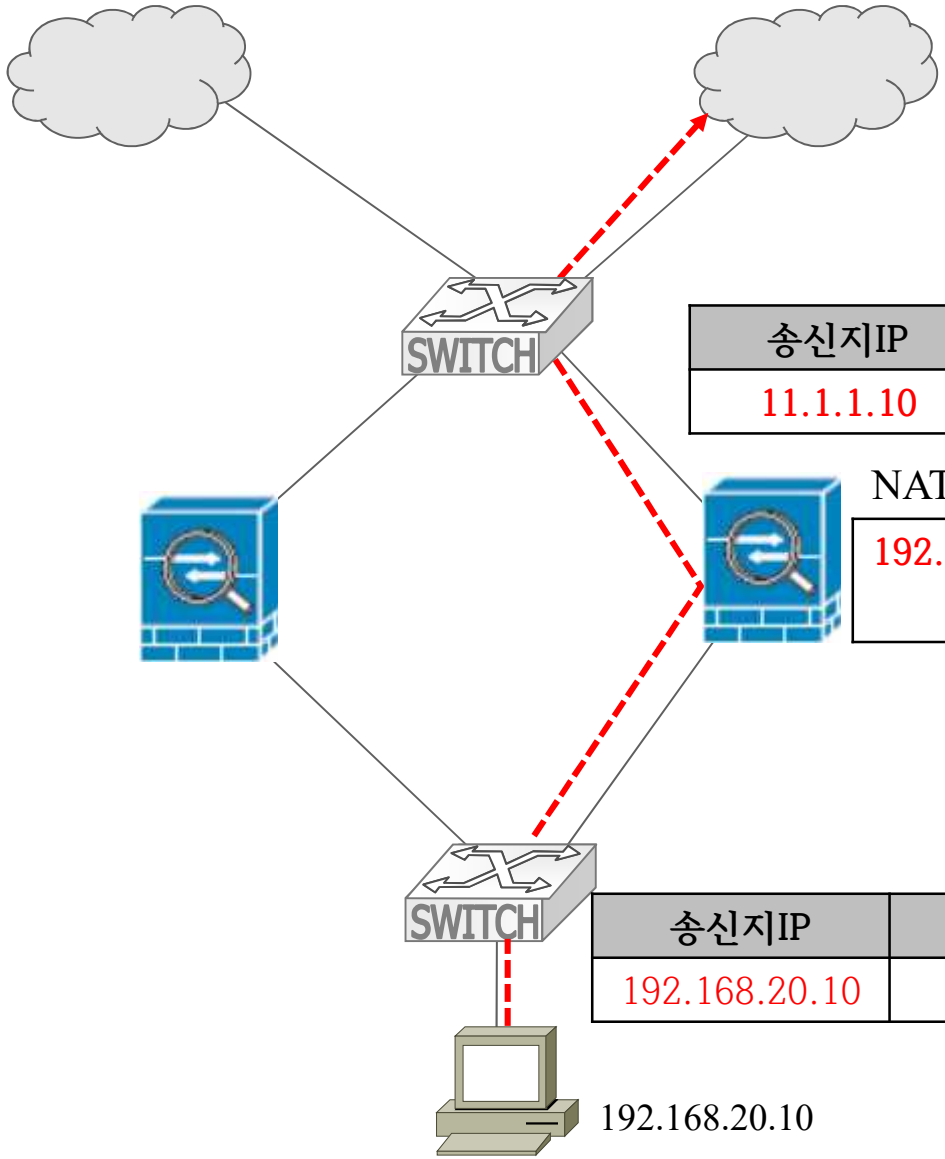
서비스	TCP	UDP
소리바다	22322, 22323, 7675	8719, 4665, 4672
구루구루	9292, 9293, 8282, 31200	22321, 7674
파일구리	9493	9493

* 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

방화벽 로드 밸런싱(FLB) - SNAT & NDAT

2.2.2.2



송신지IP	수신지IP
11.1.1.10	2.2.2.2

NAT Table

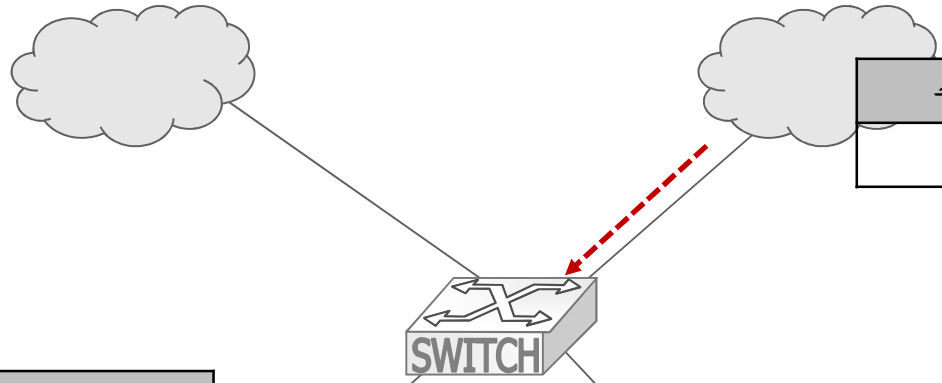
192.168.20.10 → 11.1.1.10

송신지IP	수신지IP
192.168.20.10	2.2.2.2

방화벽 로드 밸런싱(FLB) - SNAT & NDAT

2.2.2.2

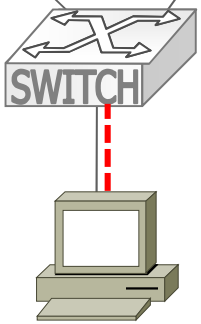
송신지IP	수신지IP
2.2.2.2	11.1.1.10



송신지IP	수신지IP
2.2.2.2	192.168.20.10

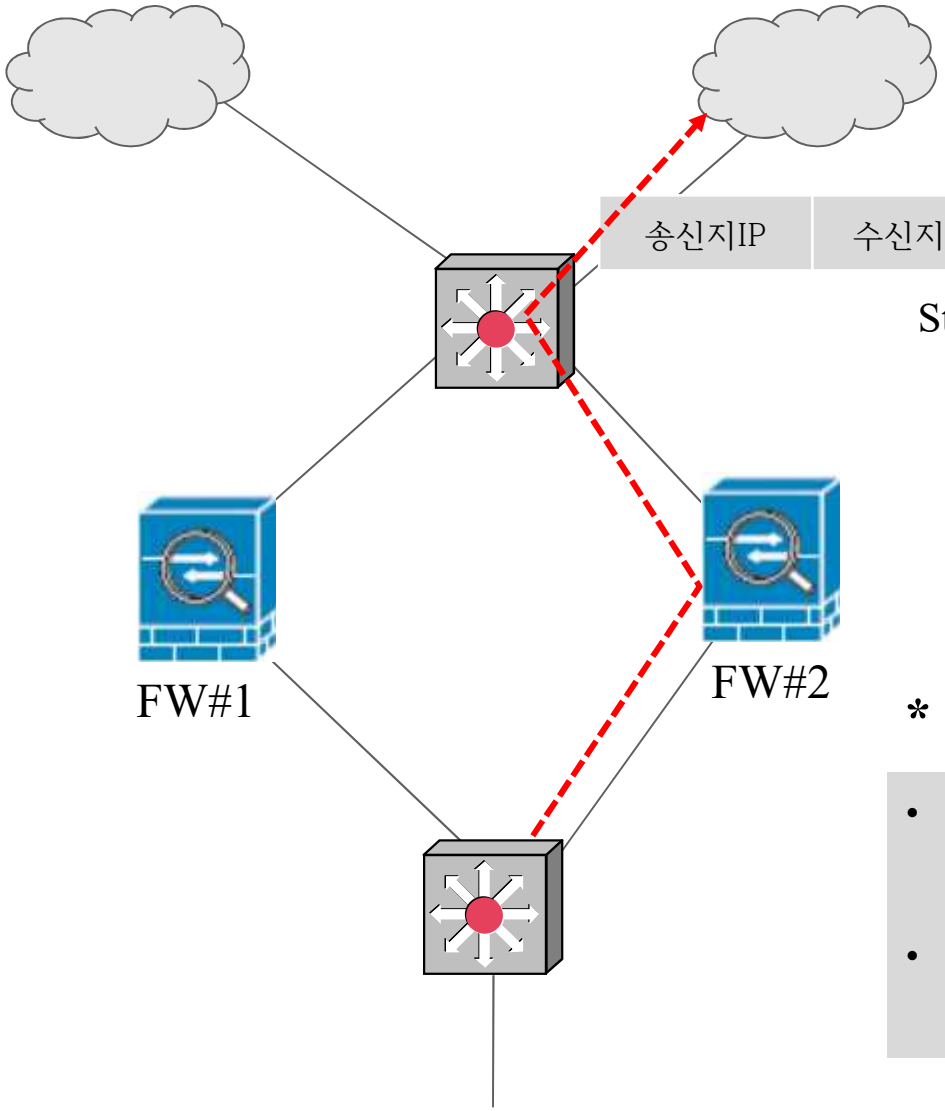
NAT Table

192.168.20.10 → 11.1.1.10



192.168.20.10

L4 스위치 기반의 방화벽 로드 밸런싱



L4 스위치의 세션 기억 테이블 구성 항목

송신지IP	수신지 IP	송신포트	수신 포트	프로토콜	거친 방화벽

Sticky mode Switch 기능 제공

* L4 Switch - Sticky mode

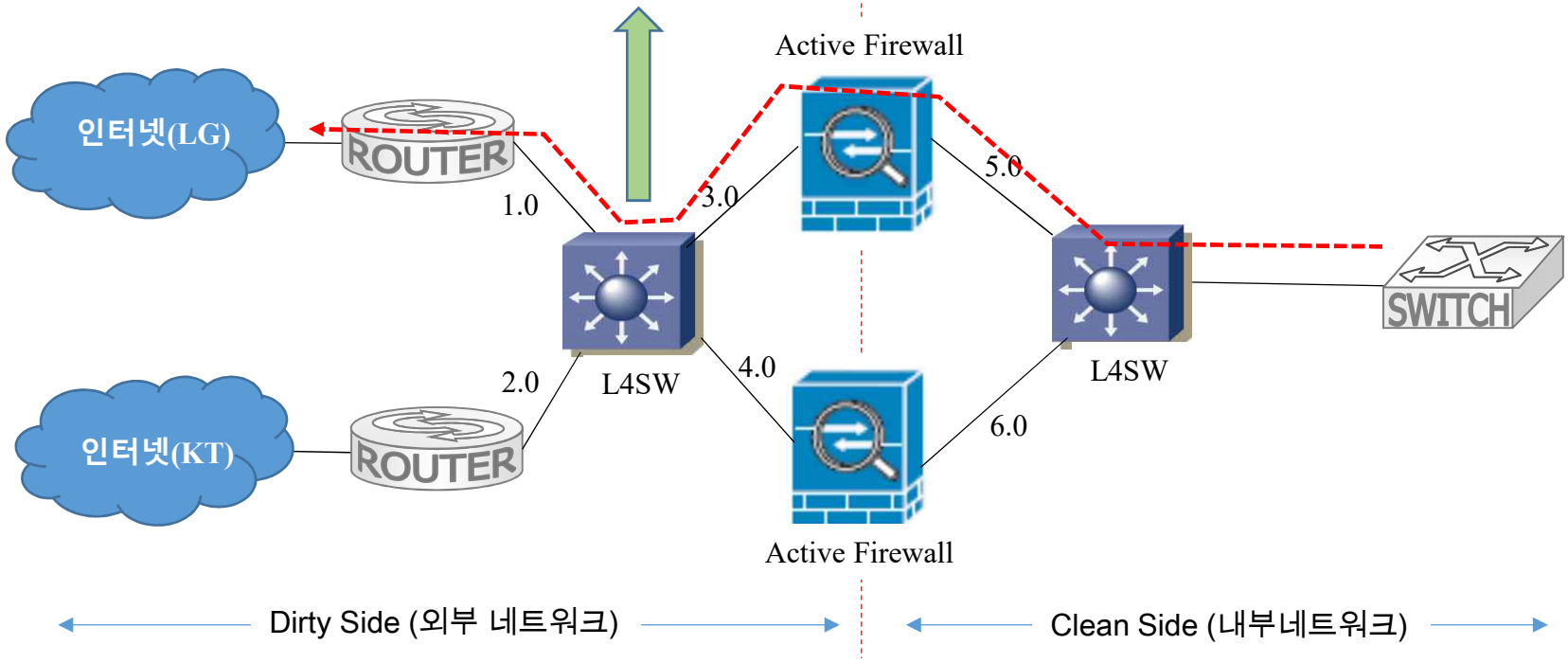
- L4 스위치는 Sticky mode를 통해 세션 별로 어떤 방화벽을 거쳐 트래픽이 전송되었는지를 저장
- Sticky mode는 방화벽의 NAT 기능을 원활하게 지원하기 위한 L4 스위치의 주요 기능

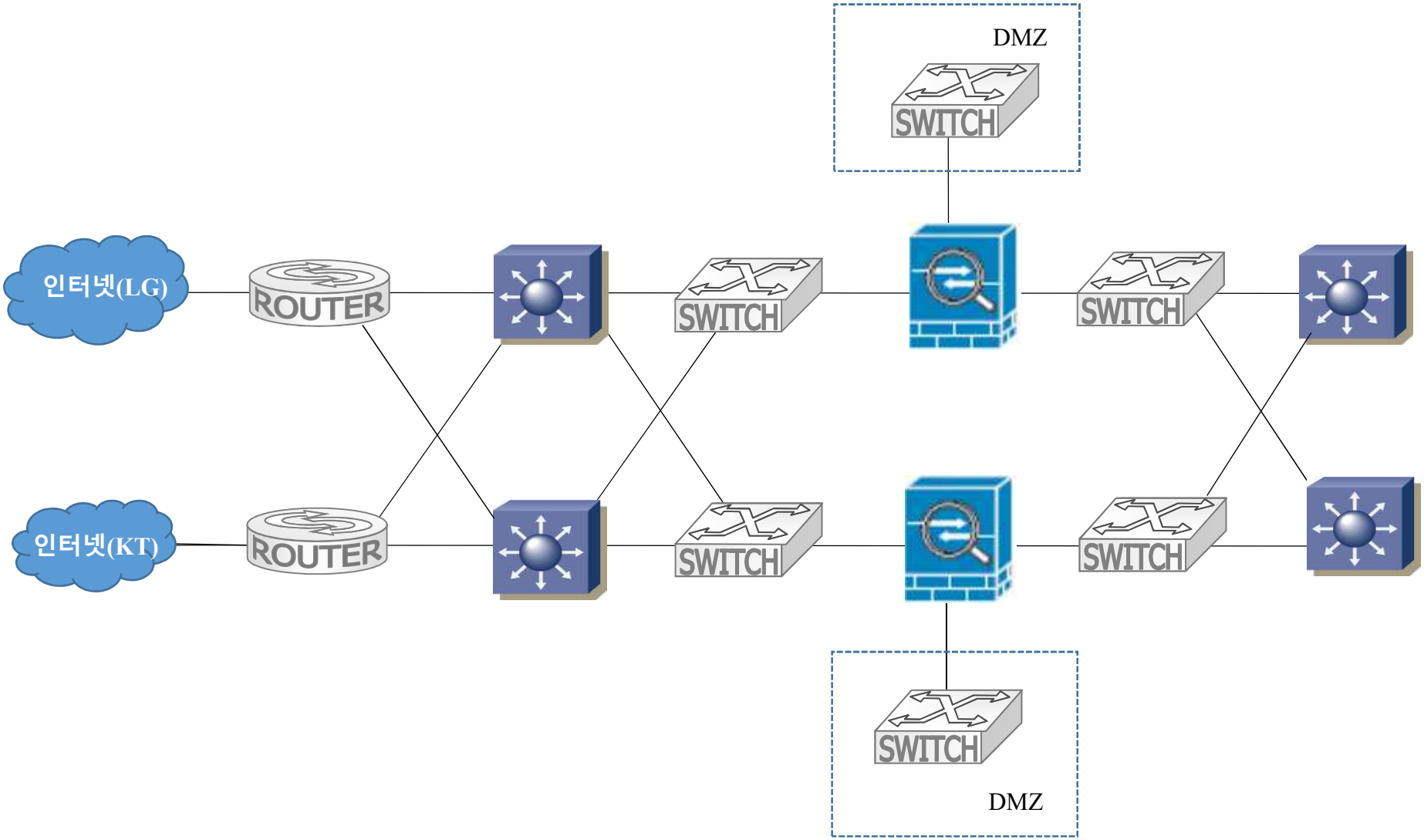
Firewall Load Balancing (FLB)

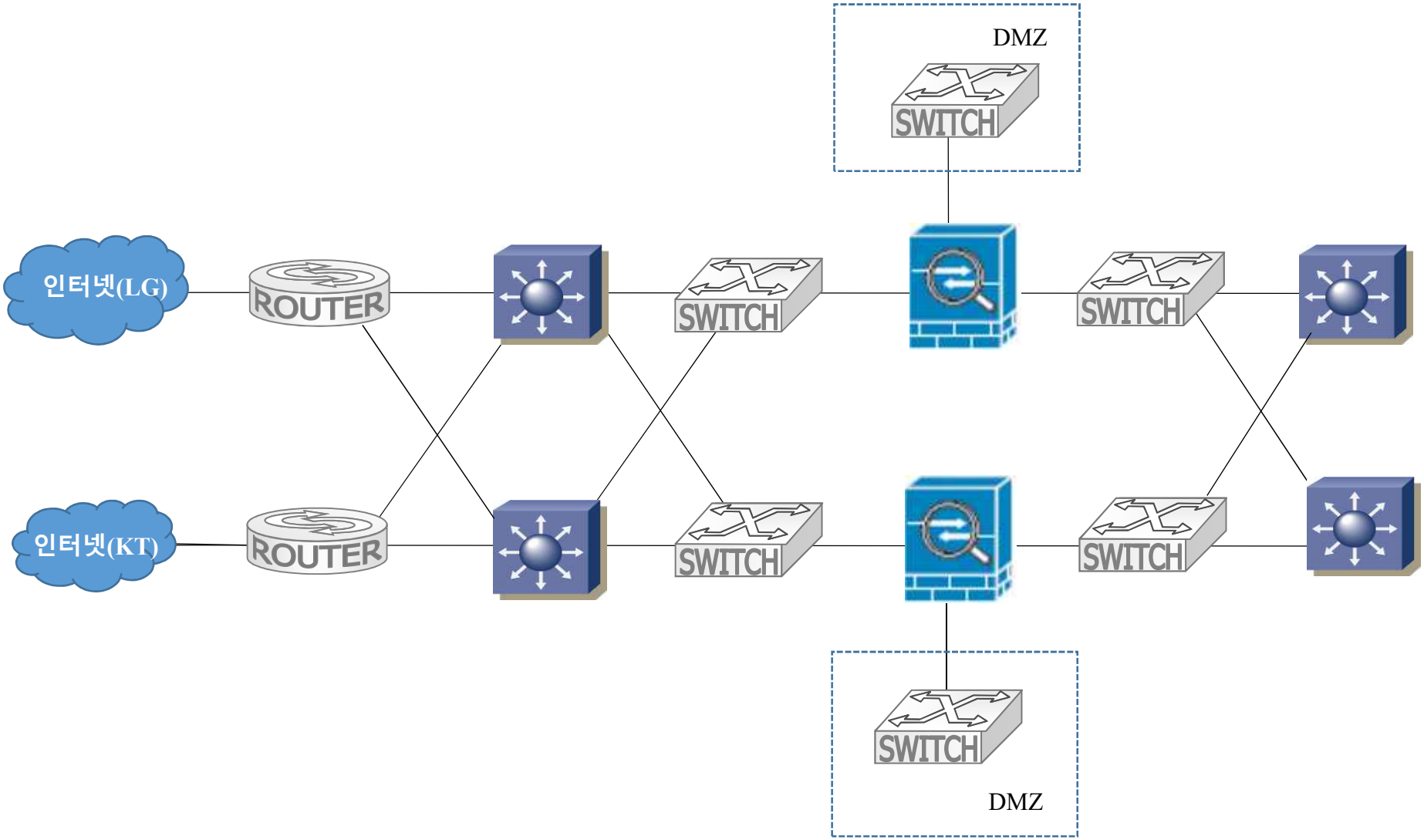
- L4 스위치 기반의 로드 밸런싱

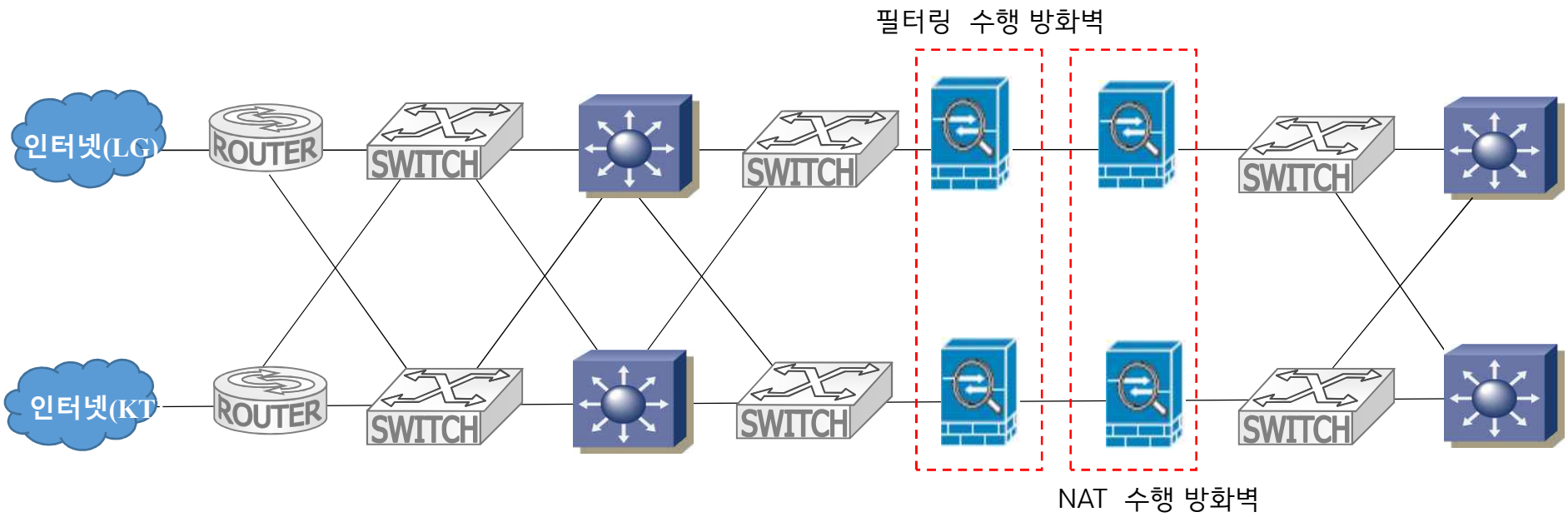
L4 스위치의 세션 기억 테이블 구성 항목(Sticky mode)

송신지IP	수신지 IP	송신포트	수신 포트	프로토콜	거친 방화벽




DMZ
SWITCH
인터넷(LG)
ROUTER
SWITCH
SWITCH
인터넷(KT)
ROUTER
SWITCH
SWITCH
SWITCH
DMZ


DMZ
SWITCH
인터넷(LG)
ROUTER
SWITCH
SWITCH
인터넷(KT)
ROUTER
SWITCH
SWITCH
SWITCH
DMZ


필터링 수행 방화벽
인터넷(LG)
인터넷(KT
ROUTER
ROUTER
SWITCH
SWITCH
SWITCH
SWITCH
SWITCH
SWITCH
NAT 수행 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

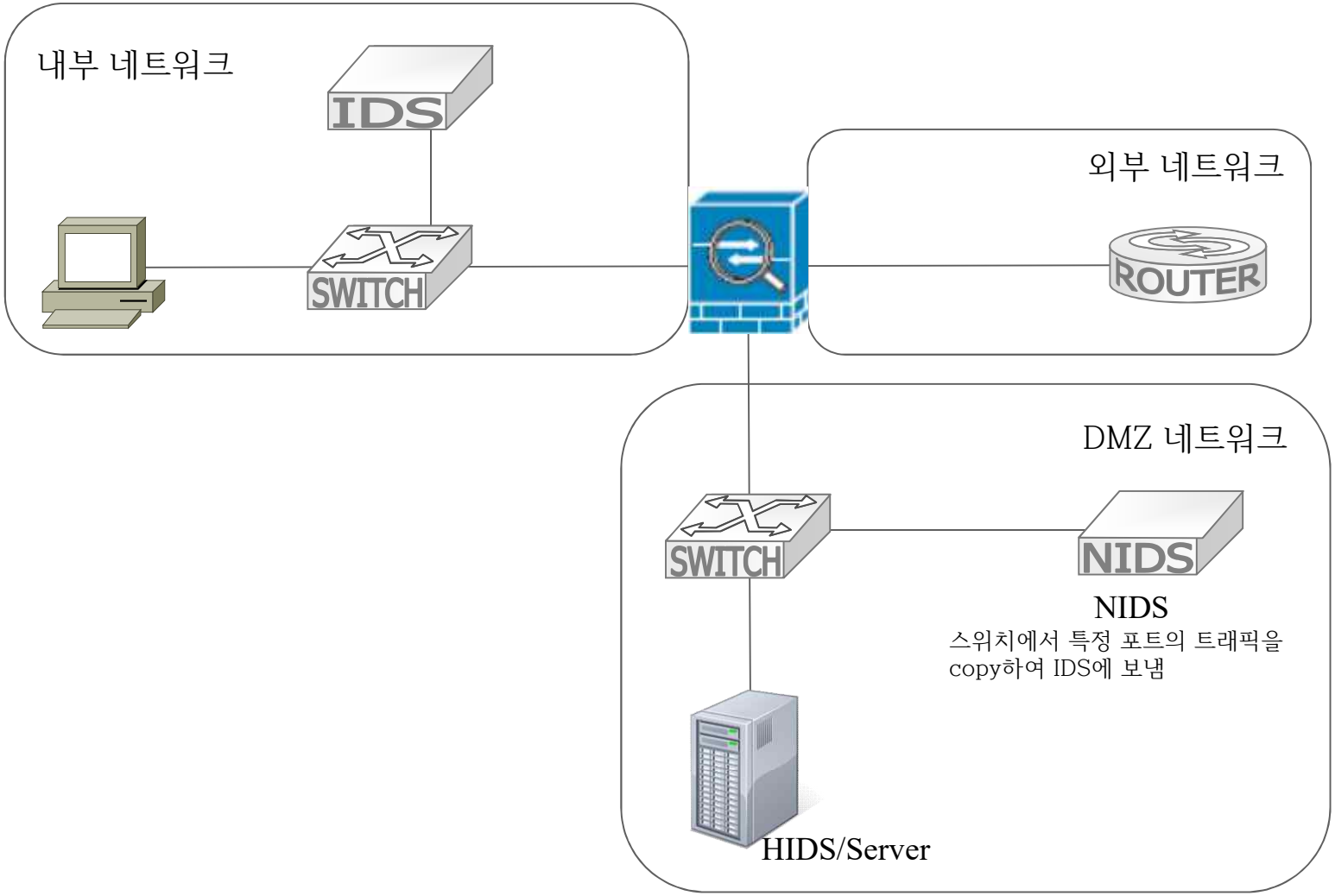
❷ 침입 탐지 시스템 (Intrusion Detection System)

- 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 데이타베이스에 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	• 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	• 행동 기반의 탐지 • 정상범위(normal)을 벗어나는 데이터를 탐지하는 방법 • 정량적인 분석, 통계적 분석을 사용 • 형태 관찰, 프로파일 생성, 프로파일 기반 으로 이상여부를 확인 • I/O 사용량, 로그인 횟수, 패킷양 등

IDS 탐지 방법

	오용탐지(Misuse Detection)	이상탐지(Anomaly Detection)
장점	• 오탐률(false positive)이 낮음 • 트로이 목마, 백도어 공격 탐지 가능	• 미탐률(false negative)이 낮음 • 인공지능 알고리즘 사용으로 스스로 판단하여 수작업의 패턴 업데이트 불필요 • 알려지지 않는 새로운 공격 탐지 가능
단점	• 미탐률(false negative)이 높음 • 새로운 공격 탐지를 위해 지속적인 공격 패턴 갱신 필요 • 패턴에 없는 새로운 공격에 대해서는 탐지 불가능	• 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

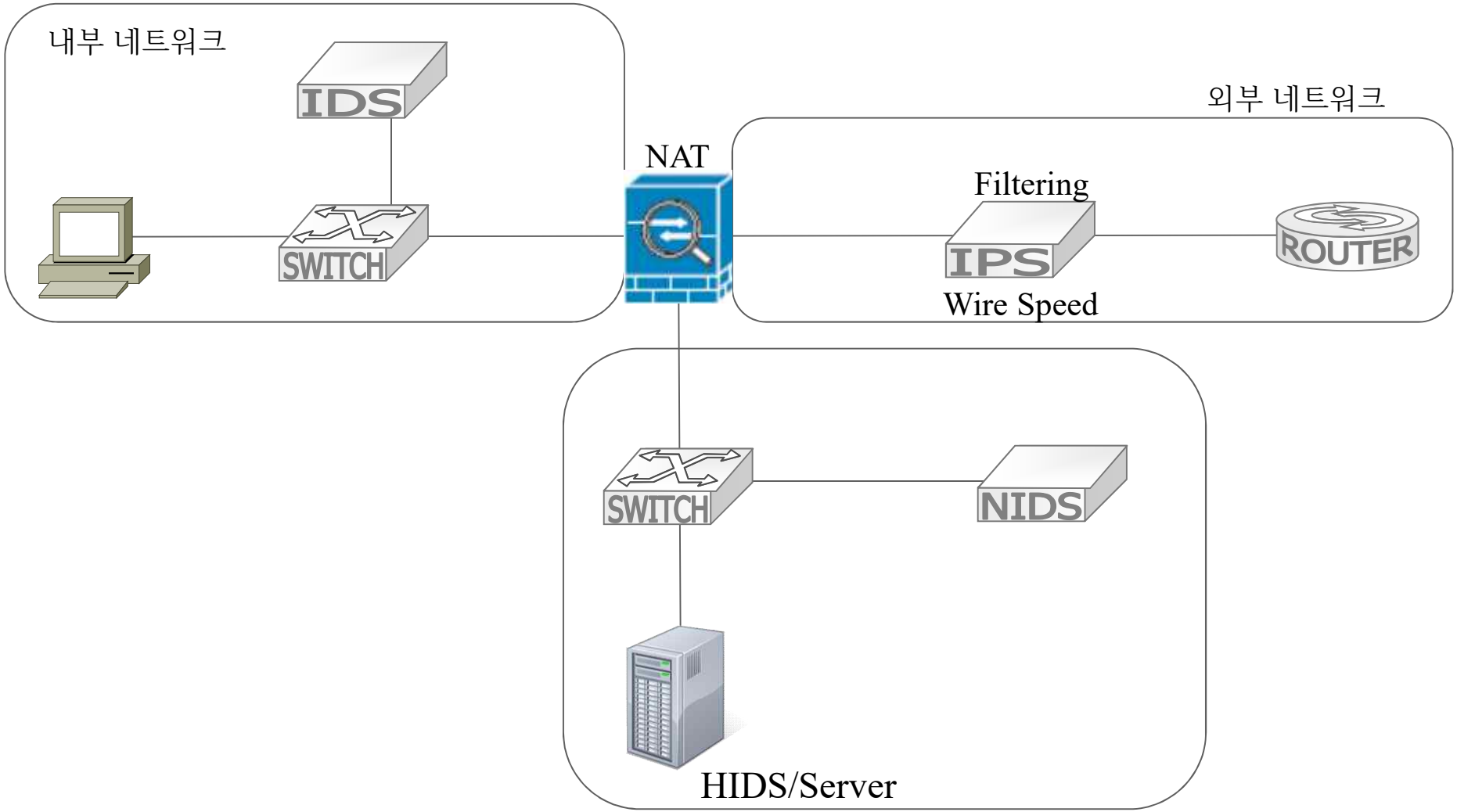
  - 공격에 대한 패턴을 모르다면 분석과 탐지가 어려움

- 실시간 공격을 막을 수 없음

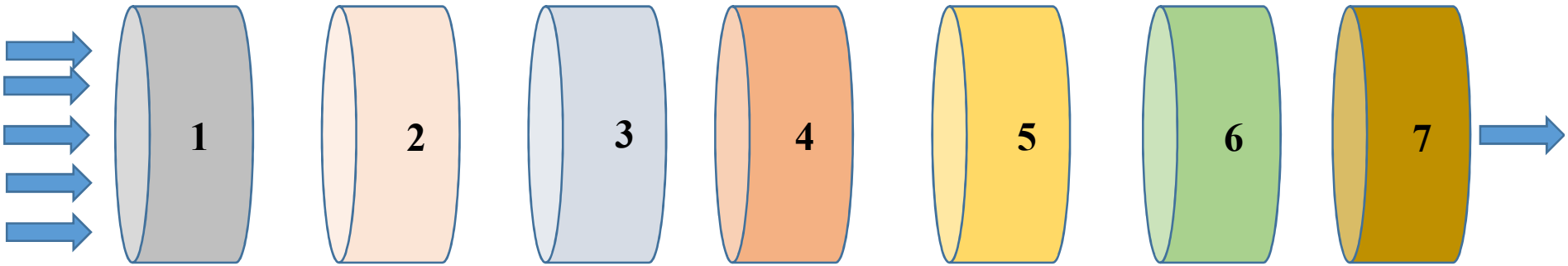
- 단편화(fragmentation), 난독화, 암호화와 같은 기술은 감지하지 어려움

❸침입 방지 시스템 (Intrusion Prevention System)

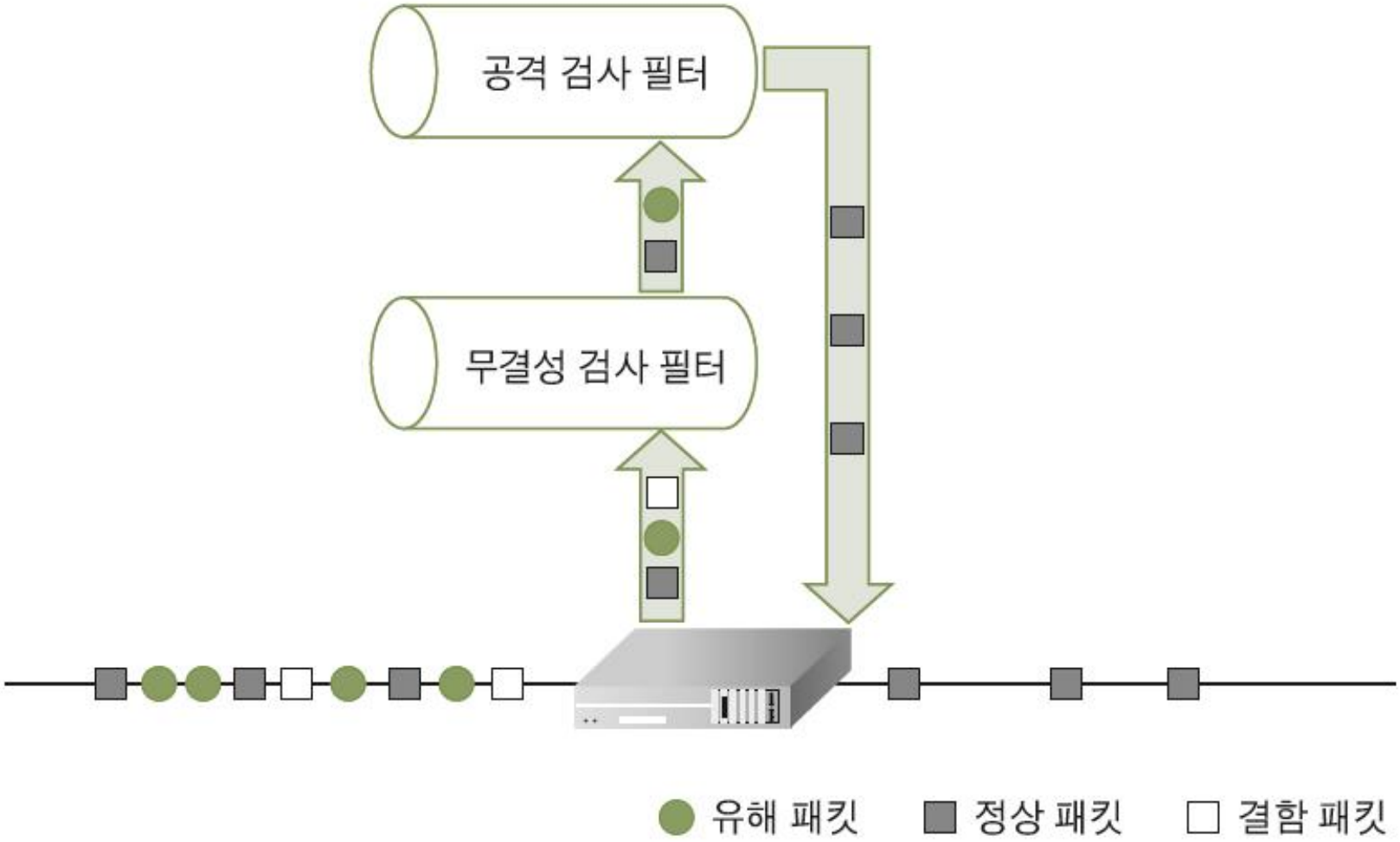
- 침입탐지시스템의 detection 기능과 방화벽의 차단(blocking) 기능 결합
- 이상 행위 탐지(anomaly detection)를 통해 알려지지 않은 공격 패턴에 대응
- 공격에 대한 사전 방지를 조치하는 것으로 in-line 방식으로 설치 및 운영
- 실시간 침입차단, 인터넷 웜, 악성 코드 및 해킹에 기인한 유해 트래픽 차단
- 능동형 보안 솔루션
  - IDS : 탐지 후 사후에 조치를 취하는 기술
  - IPS : 예방적이고 사전에 조치를 취하는 기술


내부 네트워크
IDS
SWITCH
NAT
외부 네트워크
Filtering
IPS
Wire Speed
ROUTER
SWITCH
NIDS
HIDS/Server

침입 차단 시스템 필터들

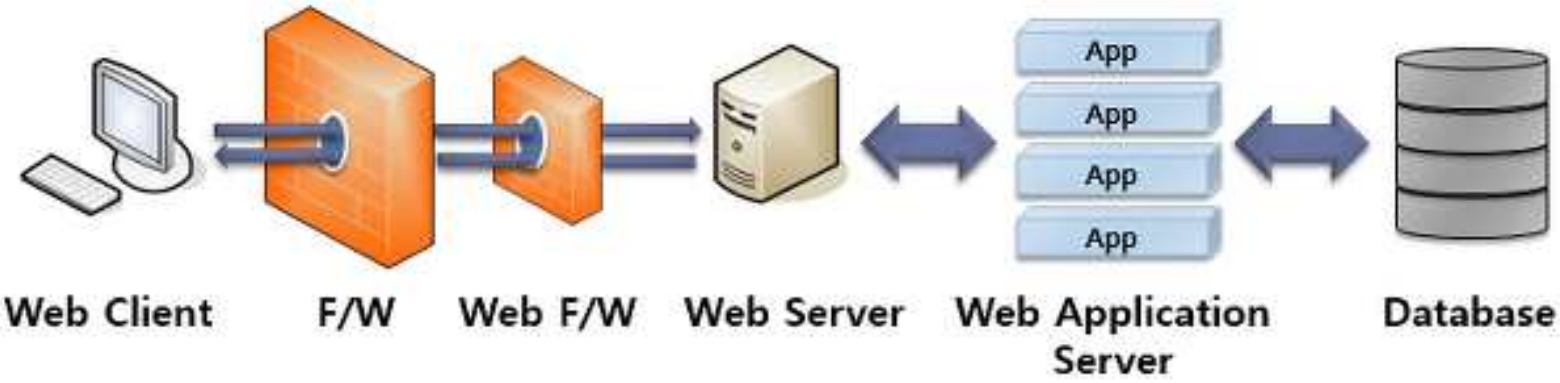


필터	기능
1	방화벽필터 - 액세스 제어 및 패킷 필터링 기능 (IP, 포트 등 패킷 필드별로 막을 패킷 정의)
2	트래픽 모니터링 및 QoS 필터 - 프로토콜별, 서비스별, IP 영역별 QoS 기능 제공
3	프로토콜 무결성 확인 필터 - FTP, DNS, 메일, 웹 등 TCP/IP 프로토콜 동작 표준에 위반하는 패킷 조사
4	Signature 이상 감시 필터 : 악성 코드, 취약성, 웜에 대한 탐지 및 차단
5	DoS/DDoS 스캔 필터
6	L7 필터 : TCP /IP 단편화, 웹 우회 공격 등 L7 프로토콜 디코딩을 통한 필터
7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


공격 검사 필터
무결성 검사 필터
유해 패킷
정상 패킷
결함 패킷

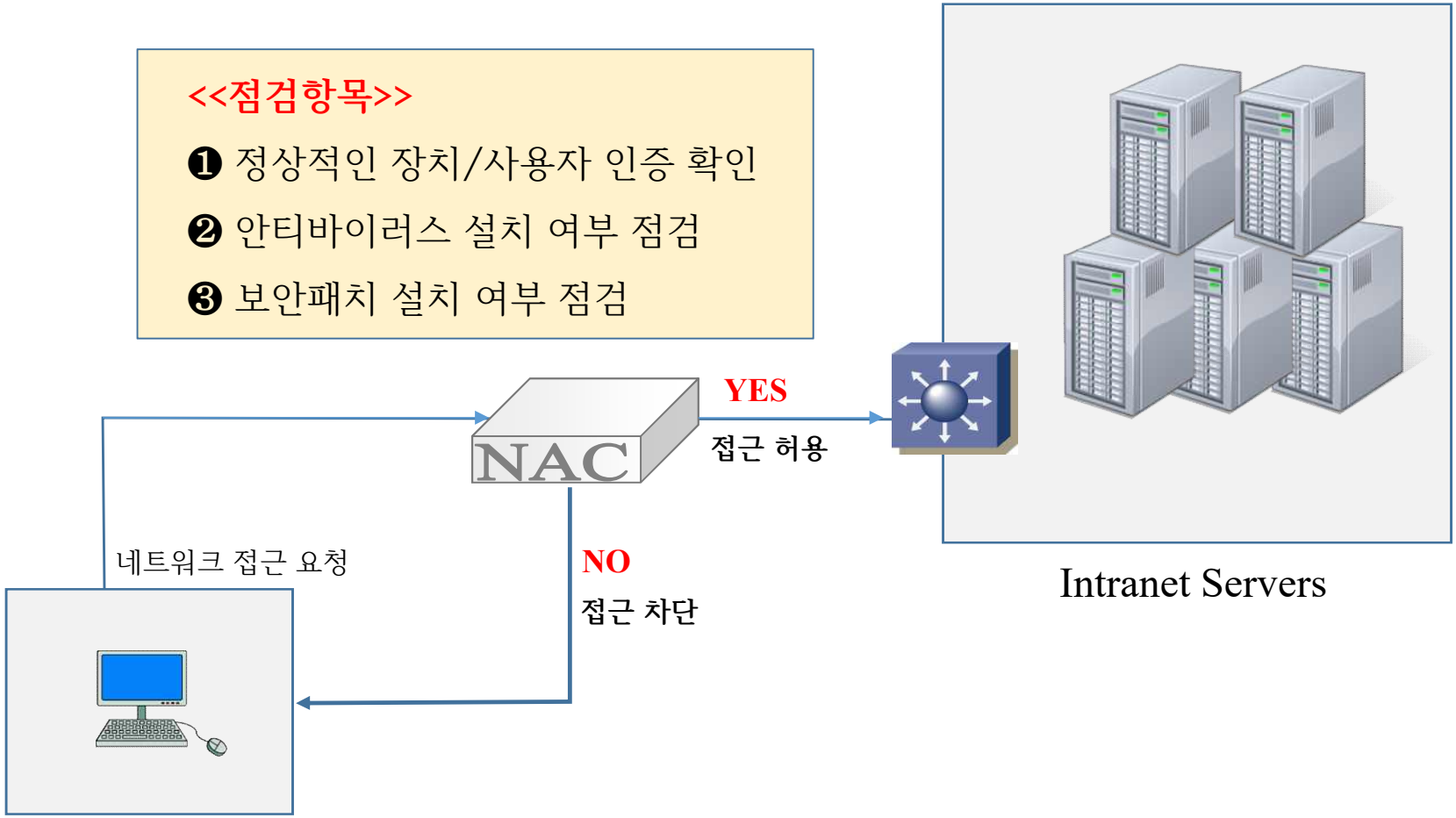
❹Web Application Firewall(WAF)

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

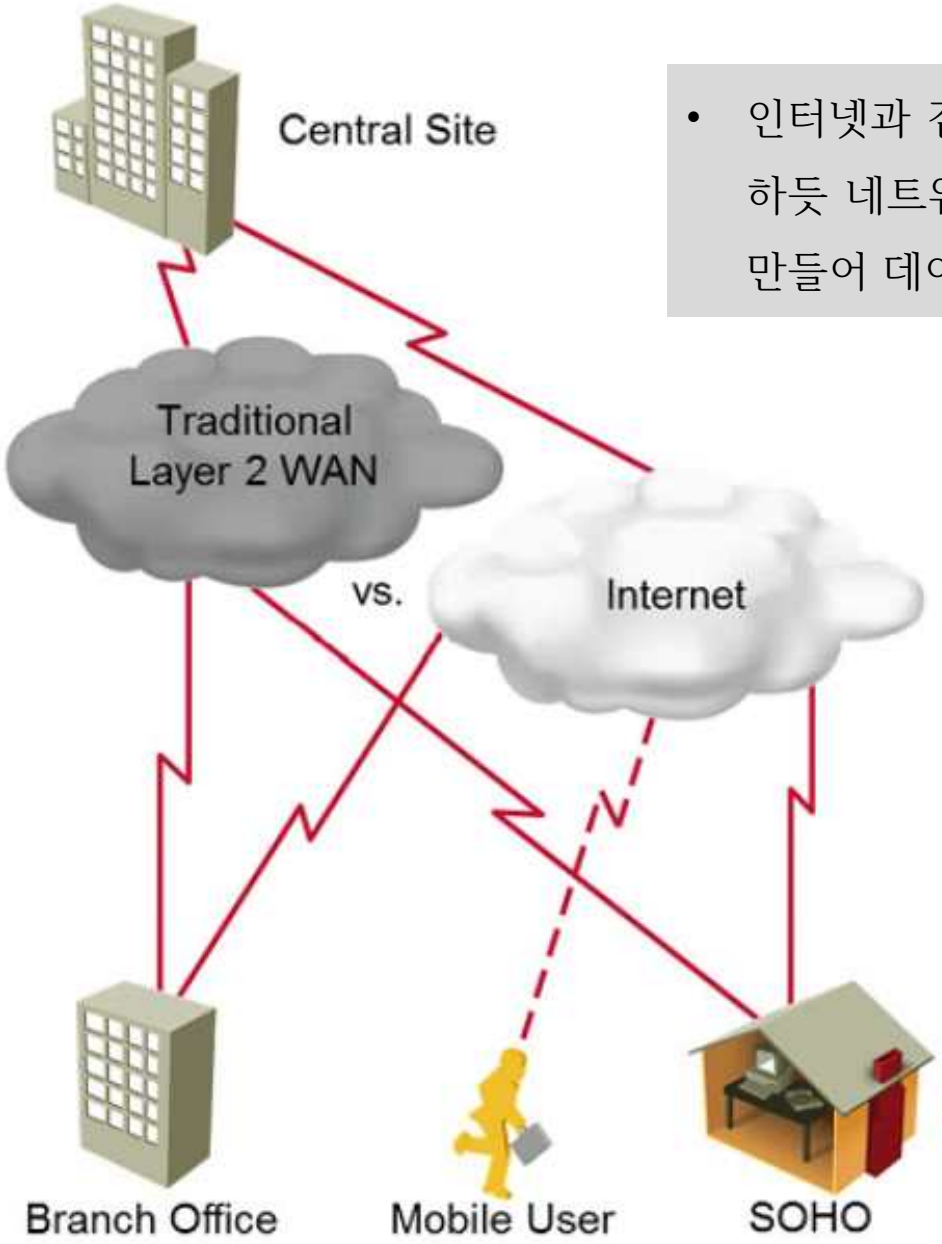


❺ NAC(Network Access Control)

* NAC 기반 구성도



❻VPN (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

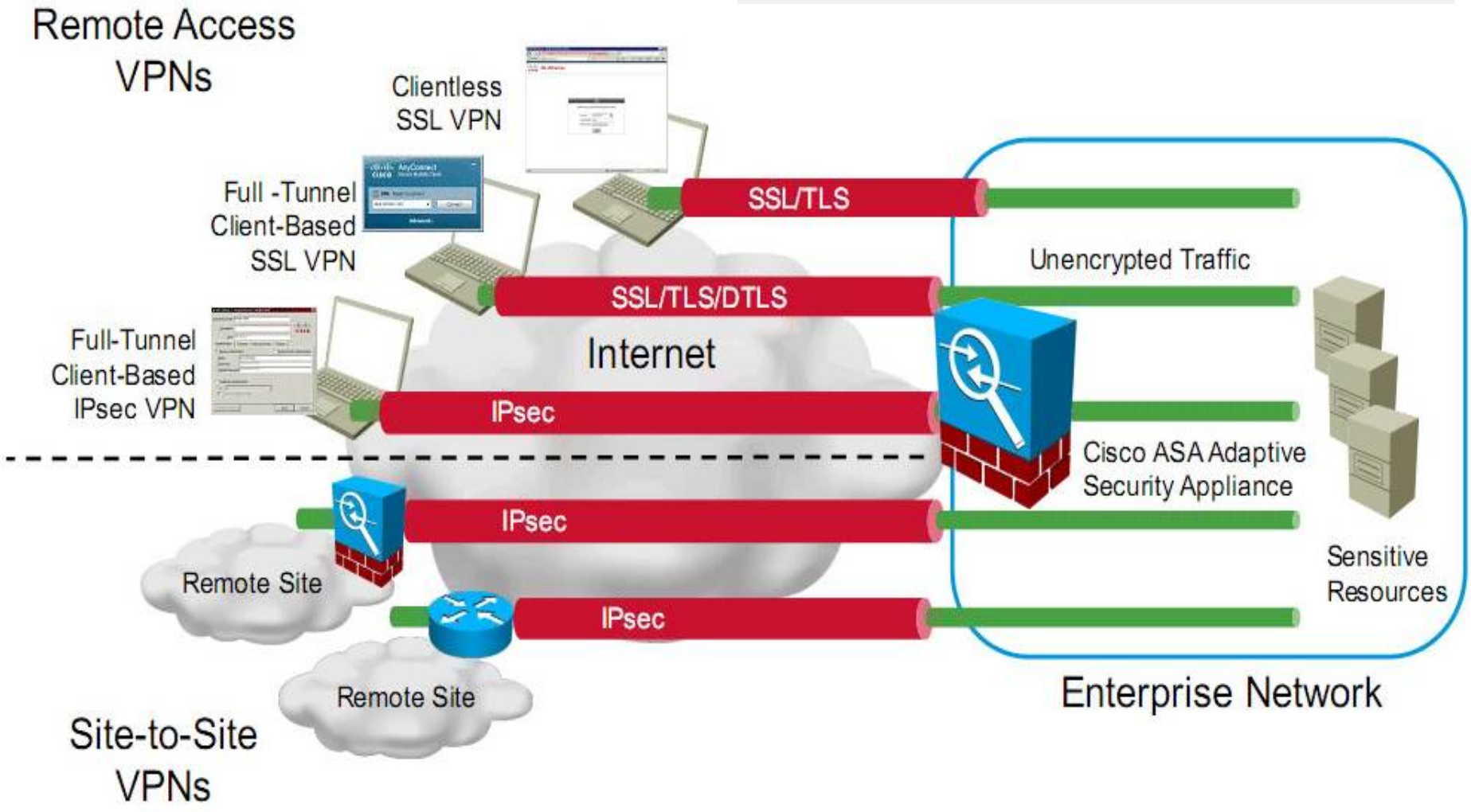
*VPN : 캡슐화 기술(암호화 header를 추가시킴)

- header : 제어 정보

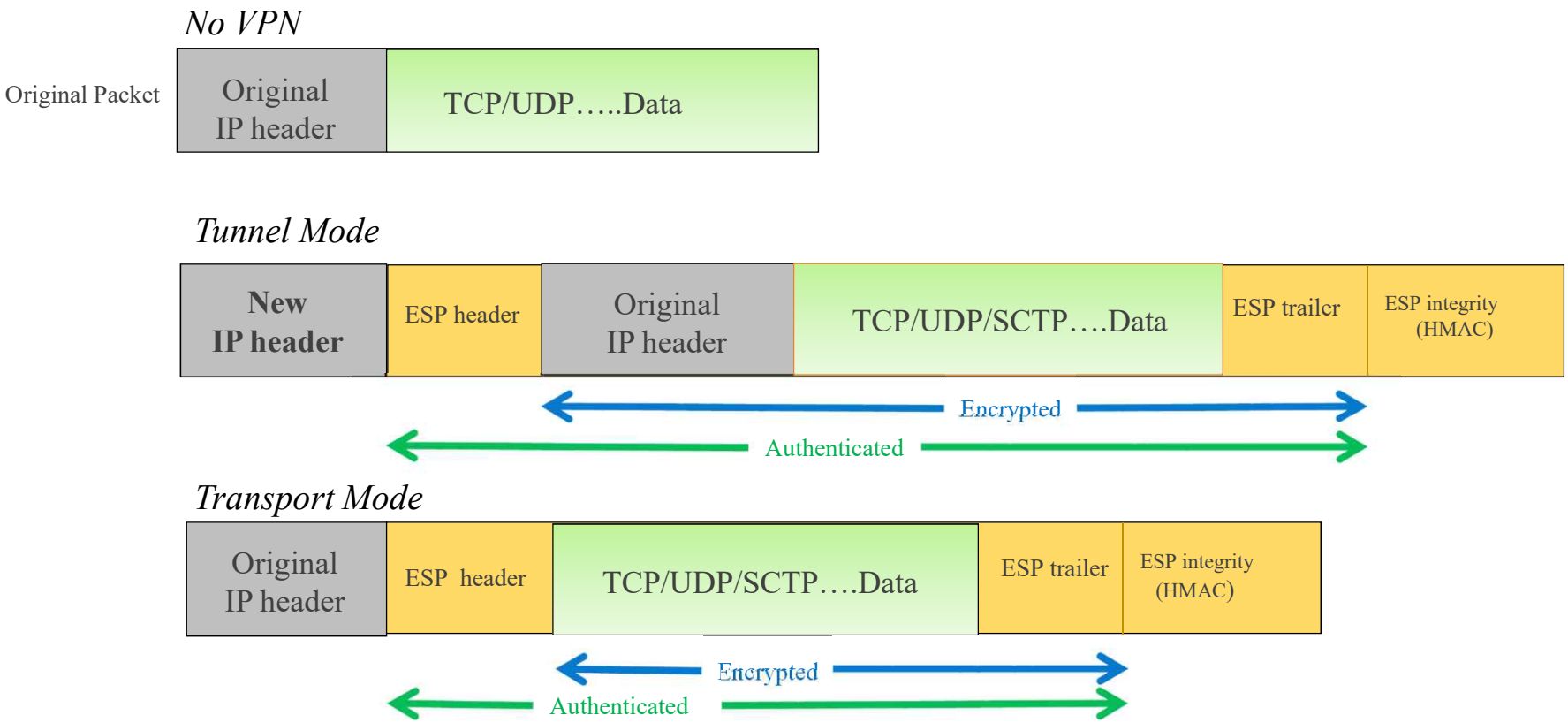
계층	암호화 프로토콜	VPN
2계층	L2TP, PPTP	L2TP VPN PPTP VPN
3계층	IPSec	IPSec VPN
4계층	TLS	SSL VPN
5계층	SSL	
7계층	HTTPS, SSH etc	

Cisco ASA VPN

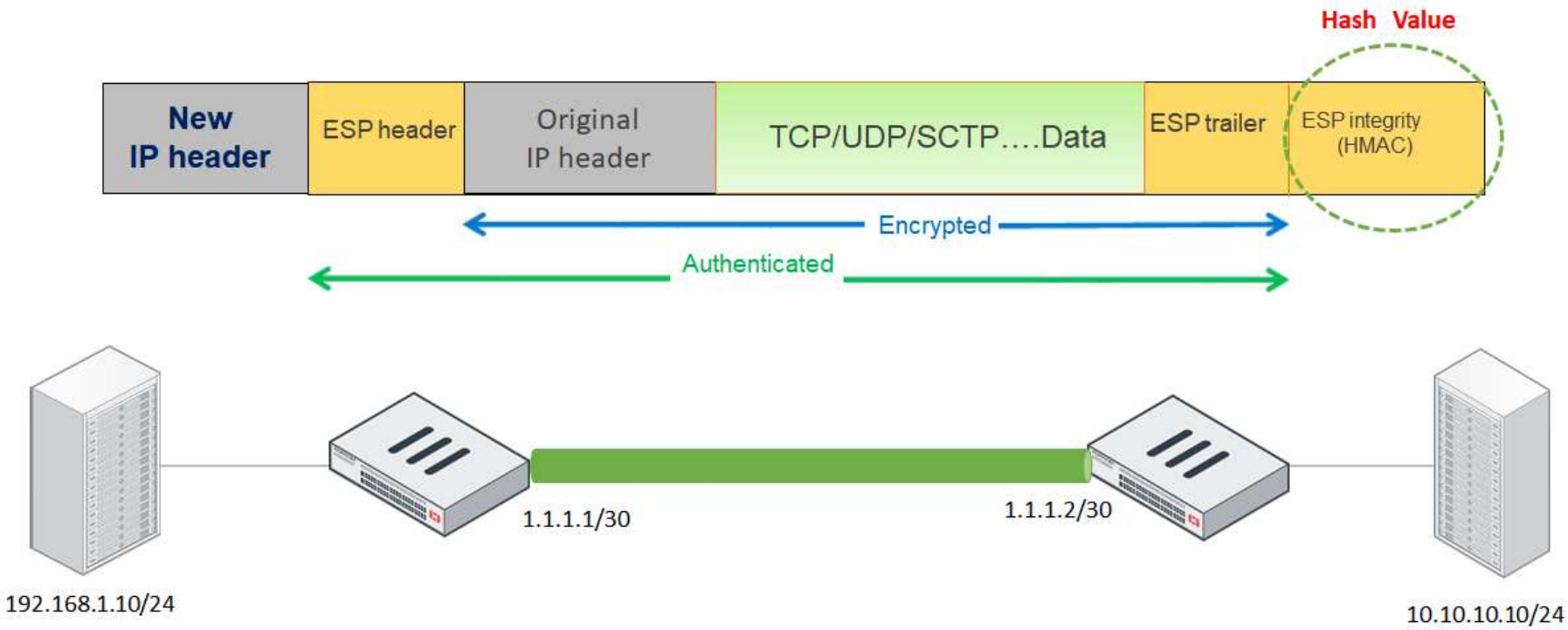
*VPN = 캡슐화 기술 = 터널 기술



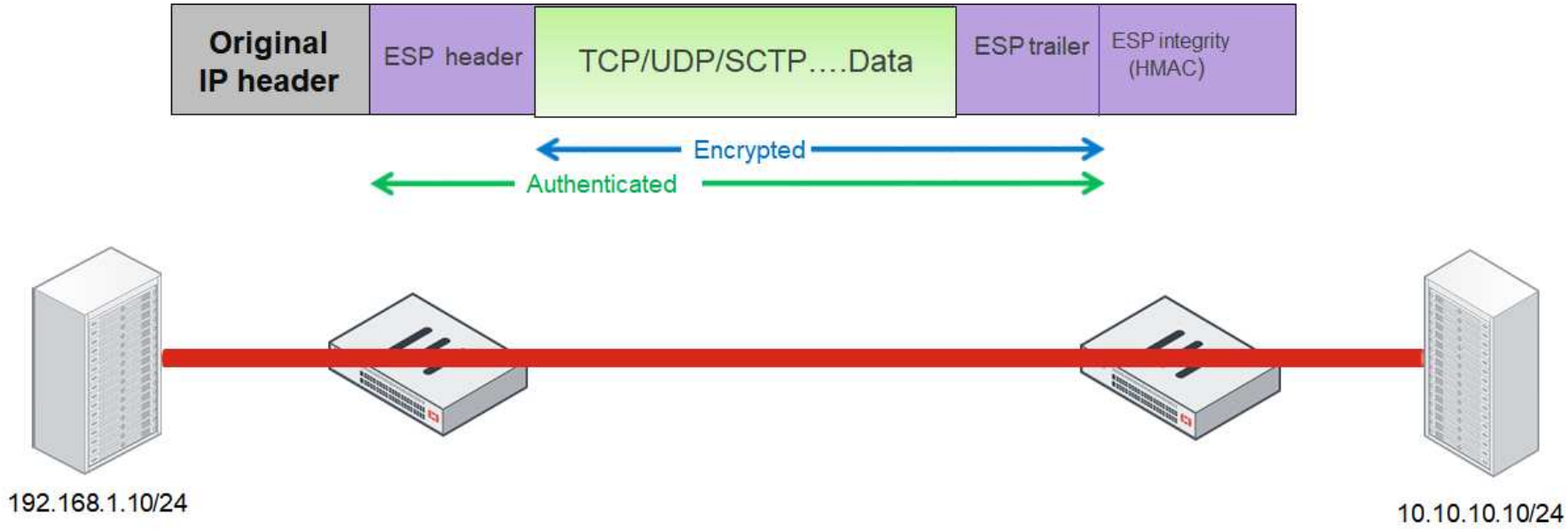
ESP Encapsulation—Tunnel or Transport Mode



Tunnel Mode


Hash Value
New IP header
ESP header
Original IP header
TCP/UDP/SCTP….Data
ESP trailer
ESP integrity (HMAC)
Encrypted
Authenticated
1.1.1.1/30
1.1.1.2/30
192.168.1.10/24
10.10.10.10/24

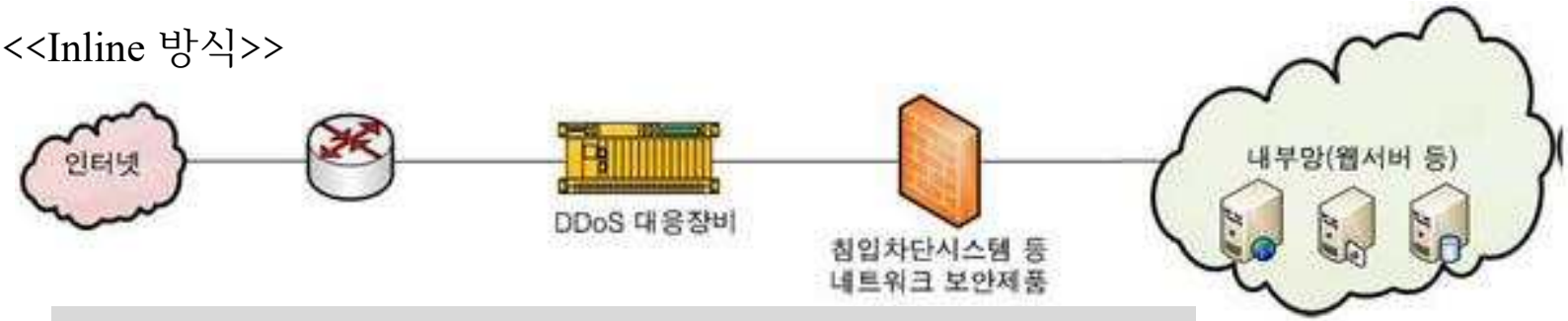
Transport Mode



❼ DDoS 대응 시스템

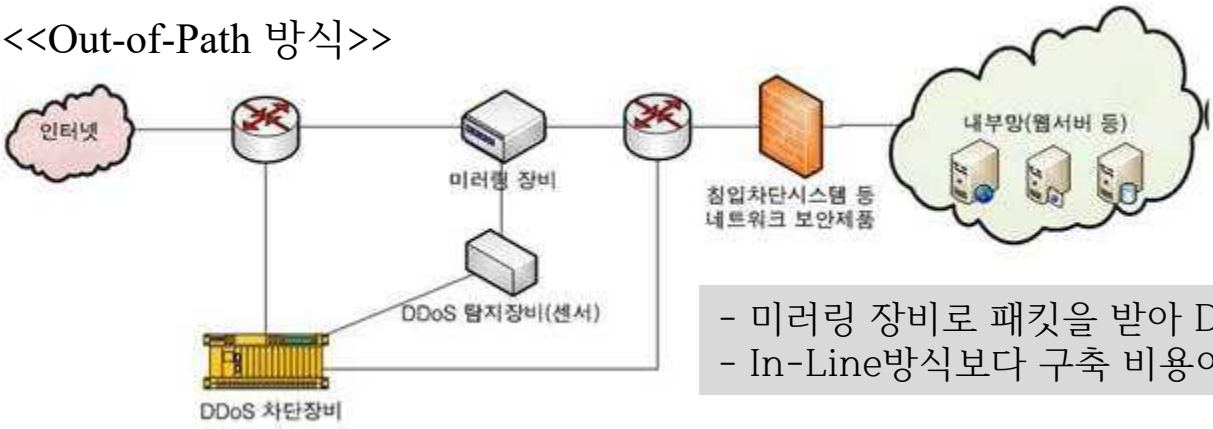
- DDoS 공격에 특화된 방어 네트워크 보안 장비
- 기존 방화벽와 IPS로 DDoS 공격이 일정 수준을 방어할 수 있었지만 대량의 DDoS 공격이 한계에 의해 생성된 장비

<<Inline 방식>>



- DDoS 대응 장비로 유입되는 트래픽을 모니터닝하여 공격을 차단
- 방화벽 앞에 위치

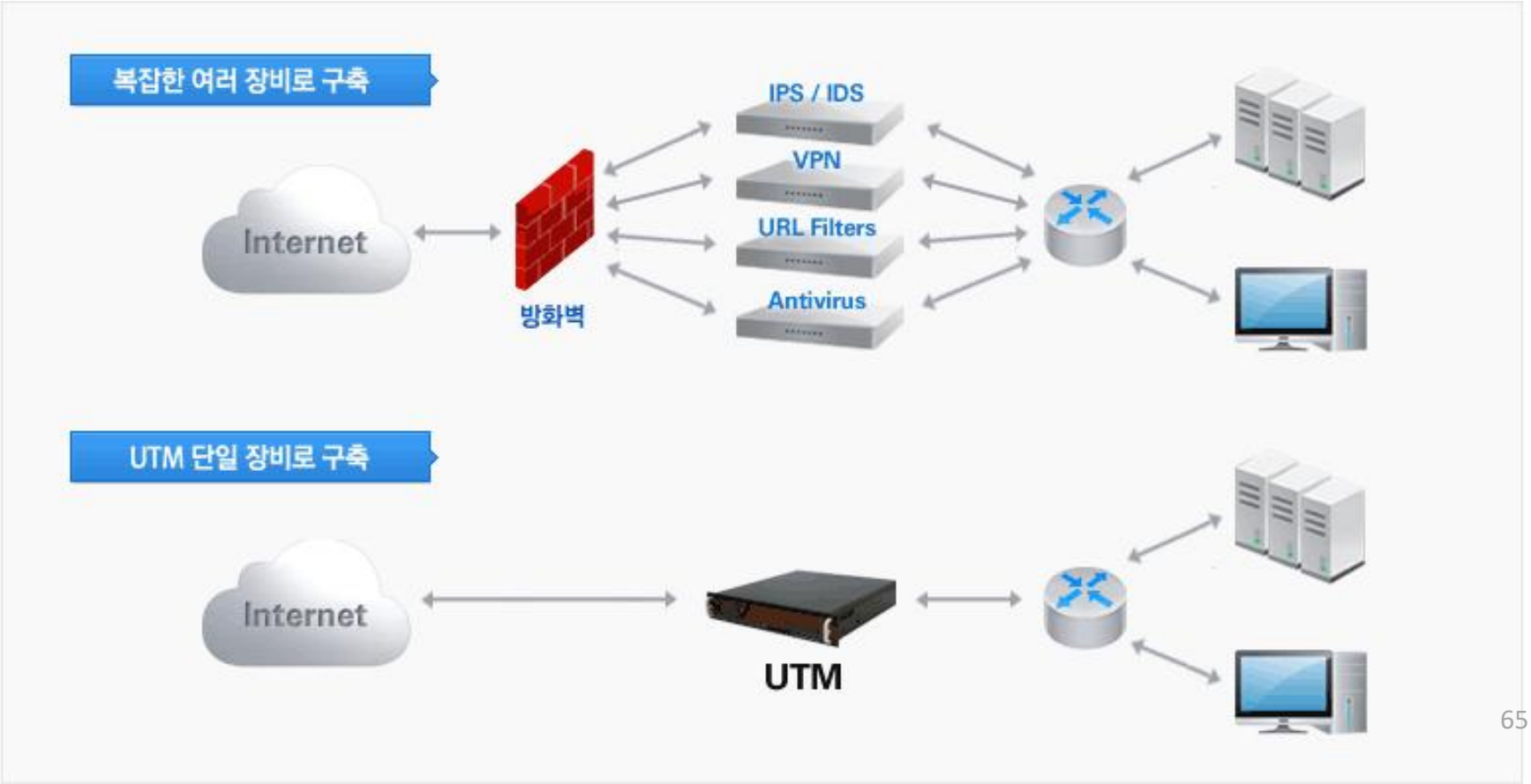
<<Out-of-Path 방식>>



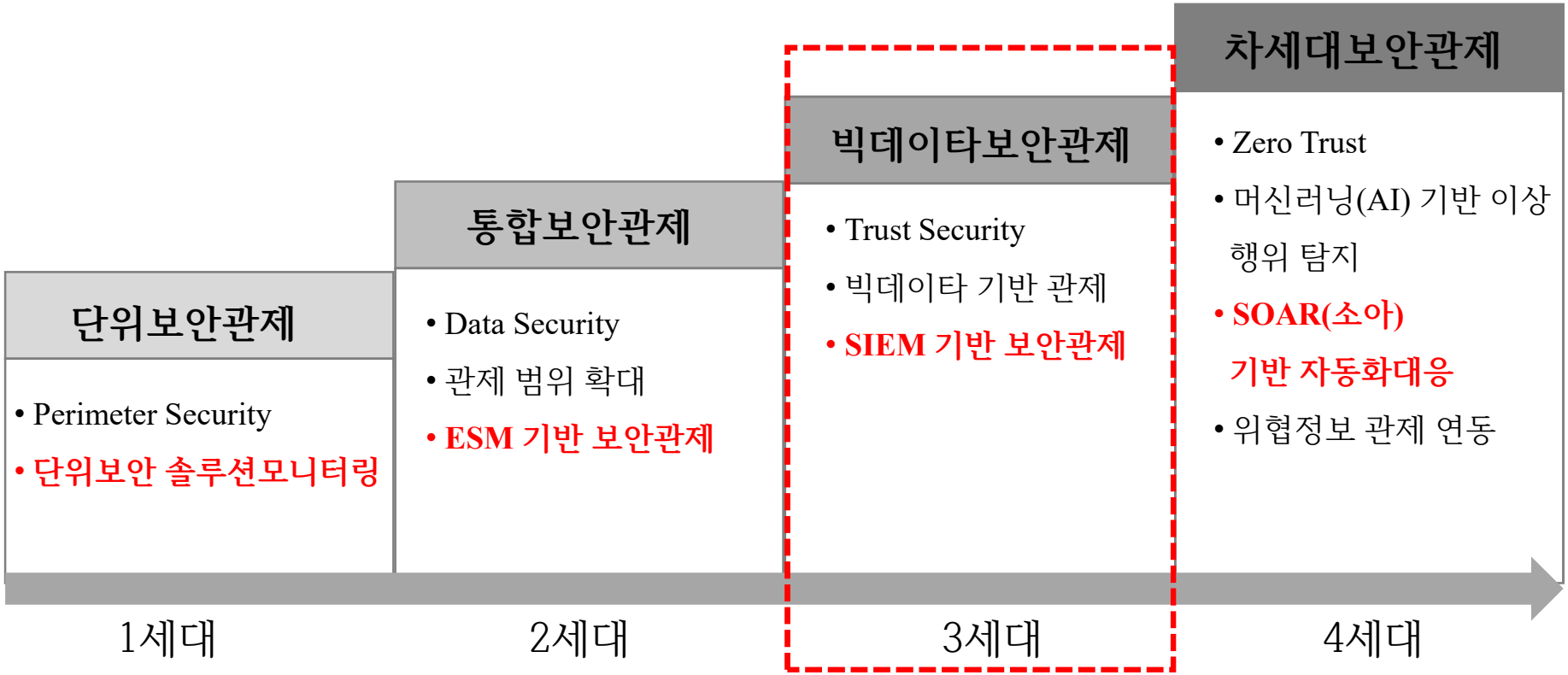
- 미러링 장비로 패킷을 받아 DDOS 장비로 분석/차단
- In-Line방식보다 구축 비용이 많이 듦

❽ UTM (Universal Threat Management)

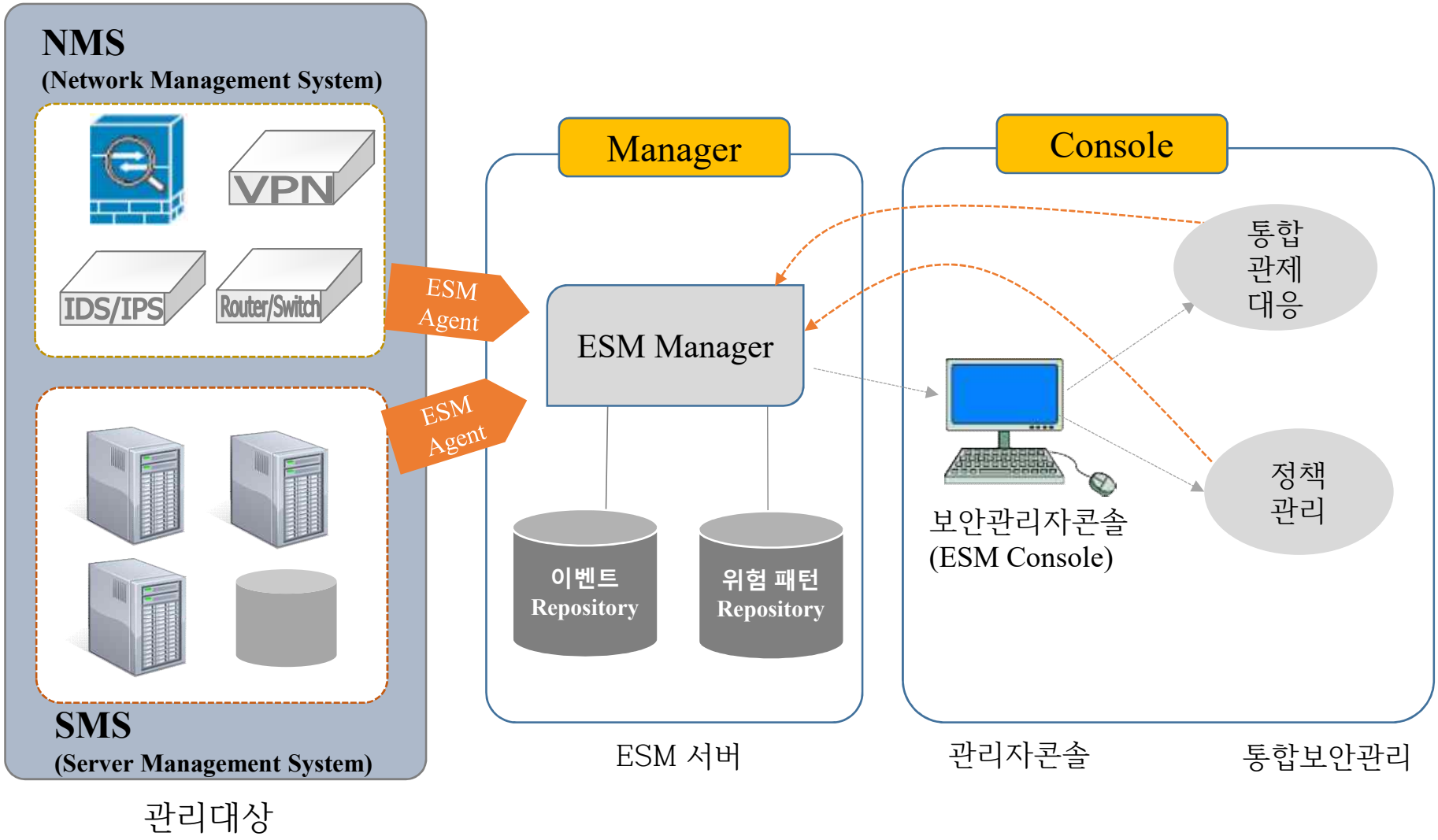
- 다양한 보안 기능을 하나의 장비로 통합하여 제공하는 보안 솔루션
- 네트워크는 간단해져서 투자 비용은 줄고 관리는 쉬워짐
- 중소 규모의 네트워크를 중심으로 많이 적용되고 있는 장비



보안 관제 솔루션


단위보안관제
• Perimeter Security
• 단위보안 솔루션모니터링
통합보안관제
• Data Security
• 관제 범위 확대
• ESM 기반 보안관제
빅데이타보안관제
• Trust Security
• 빅데이타 기반 관제
• SIEM 기반 보안관제
차세대보안관제
• Zero Trust
• 머신러닝(AI) 기반 이상 행위 탐지
• SOAR(소아) 기반 자동화대응
• 위협정보 관제 연동
1세대
2세대
3세대
4세대

❶ ESM(Enterprise Security Management)



ESM(Enterprise Security Management) 구조

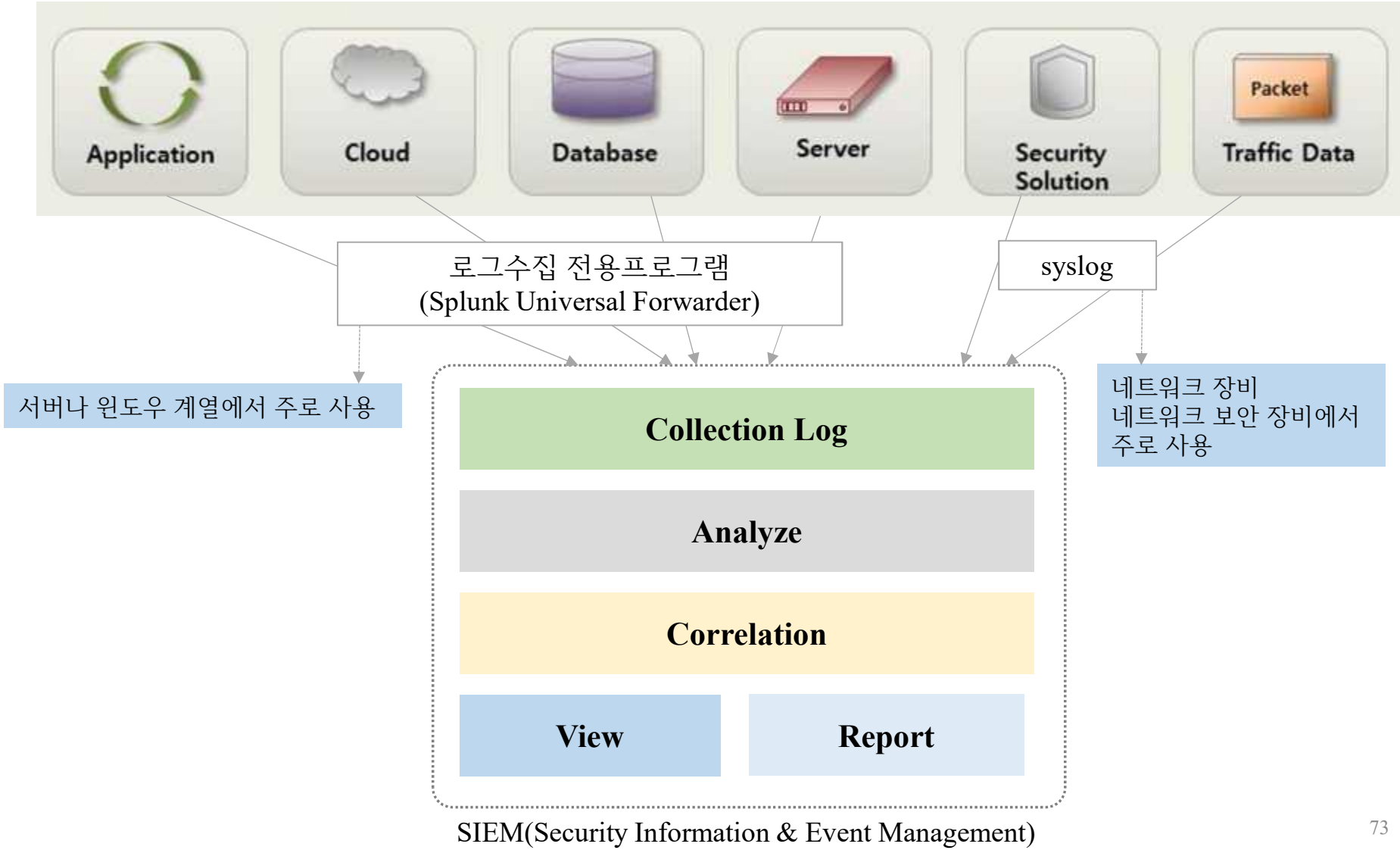
Agent	• 관리 대상 보안 장비(보안장비, 시스템장비, 네트워크 장비)에 설치 • 사전에 정의된 규칙에 의한 이벤트 수집 및 보안 정책 반영 • 정책에 따른 로그 및 이벤트 데이터를 수집하여 ESM manager에 전달
Manager (Engine)	• ESM agent에 의해 수집된 데이터 분석및 저장 • 분석 결과를 ESM Console에 전달
Console	• ESM Manager에 의해 전달된 정보의 시각적 전달, 상황 판단 및 리포팅 기능 제공 • ESM Manager/Agent에 대해 규칙을 제어/통제 수행

ESM 기능

❷ SIEM(Security Information & Event Management)

- ESM의 진화된 형태 (2015년 가트너에 의해 처음으로 도입된 개념)
- 기업 정보에 대한 종합 관제 솔루션
- HP 아크사이트(ArcSight), IBM 큐레이더(Qrader), Splunk 등이 널리 쓰임

SIEM 구성요소

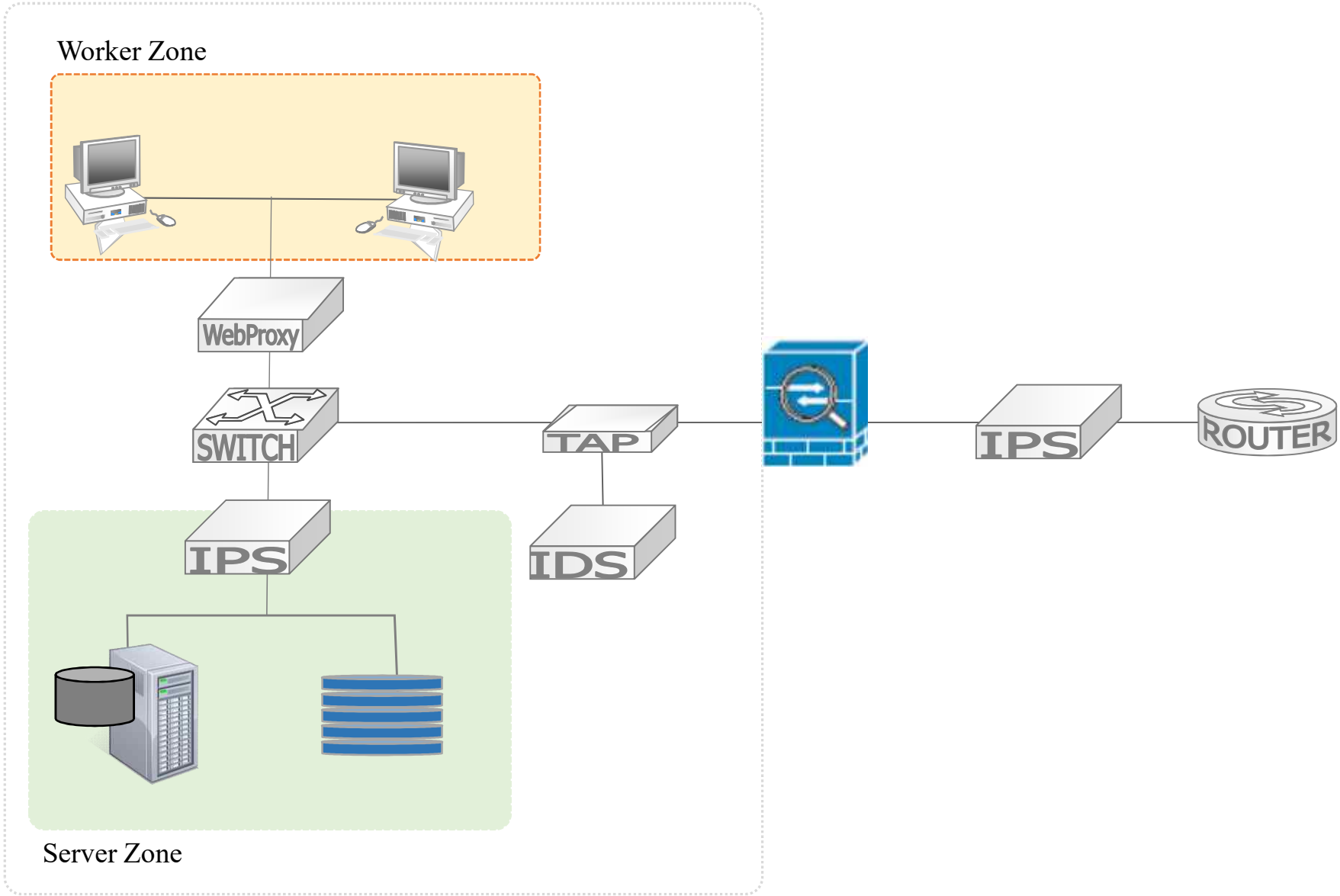

Application
Cloud
Database
Server
Security Solution
Packet
Traffic Data
로그수집 전용프로그램
(Splunk Universal Forwarder)
syslog
서버나 윈도우 계열에서 주로 사용
네트워크 장비
네트워크 보안 장비에서
주로 사용
Collection Log
Analyze
Correlation
View
Report
SIEM(Security Information & Event Management)

SIEM과 ESM 비교

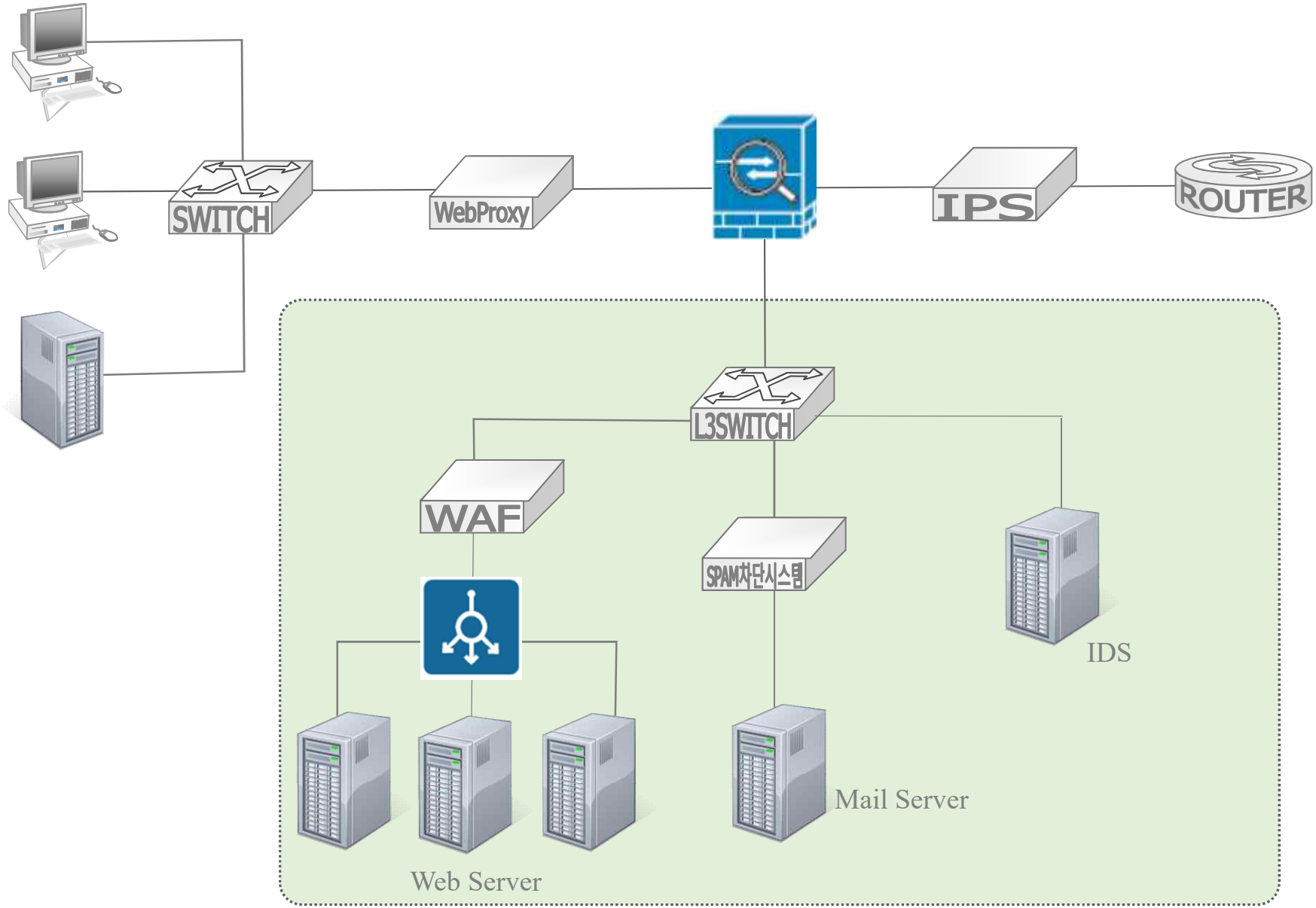
	ESM	SIEM
수집·분석	• **Event 위주의 단시간(최대1일) 위협분석** • RDBMS 기반 상관분석 및 리포트, 중앙 처리 구조 • 초당 3초건 내외 수집/분석 포함	• **빅데이타 수준의 장기간(수개월) 심층분석** • Indexing, MapReduce 등 빅데이타 처리 기반 상관분석 및 리포트 • 초당 3만~5만건 이상 수집/분석 ➔ ***RDBMS 기반의 처리 속도 지연 극복***
시각화	• 대시보드, 정형보고서 제공	• 대시보드, 정형보고서, 사용자 보고서, 시각화 보고서 제공 ➔ ***다양한 Report 제공***
사용자	• 보안관리자, 관제 요원 위주	• 보안관리자, 관제요원 • 각업무시스템 별 담당자 • 개인정보보호담당자 • 대외 서비스 담당자 ➔ ***사용자 관점의 다양한 view 지원***
하드웨어	• 고가의 유닉스 서버 스템	• 저가의 리눅스 x86 시스템

	ESM	SIEM
정의	• 기업 내 다양한 보안시스템을 관제/운영/관리하여 중앙에서 통합적으로 보안 현황을 모니터링 하는 시스템	• 기업 내에서 발생하는 모든 자원의 정보 및 보안 이벤트를 통합 관리 ➔ *장애처리 관점에서 운영 및 심층분석, 규제 준수 관점으로 확대*
수집·저장	• 정형데이타 기준, 원본로그 보관안함 • 수집 데이터 보존기간 :1~2개월	• 정형/비정형데이타 수용, 원본로그 보관 • 수집 데이터 보존기간 :1년 이상 ➔ *광범위 데이터 처리 및 장기간 보관*
위협탐지	• IP, Port 등 시그니처 중심의 네트워크 계층 탐지 • 단순 패턴 기반 탐지 • 알려진 공격 위주 분석 • 단시간(최대1일) 범위 분석	• IP, Port 외 애플리케이션, 프로토콜 등 연관성 분석 및 탐지 • APT 등 알려지지 않은 공격 및 공격간의 연관성 분석, 정상상태에서의 정보위협분석 • 장시간(수개월) 범위 분석 ➔ *심층분석, 연관분석 지원*

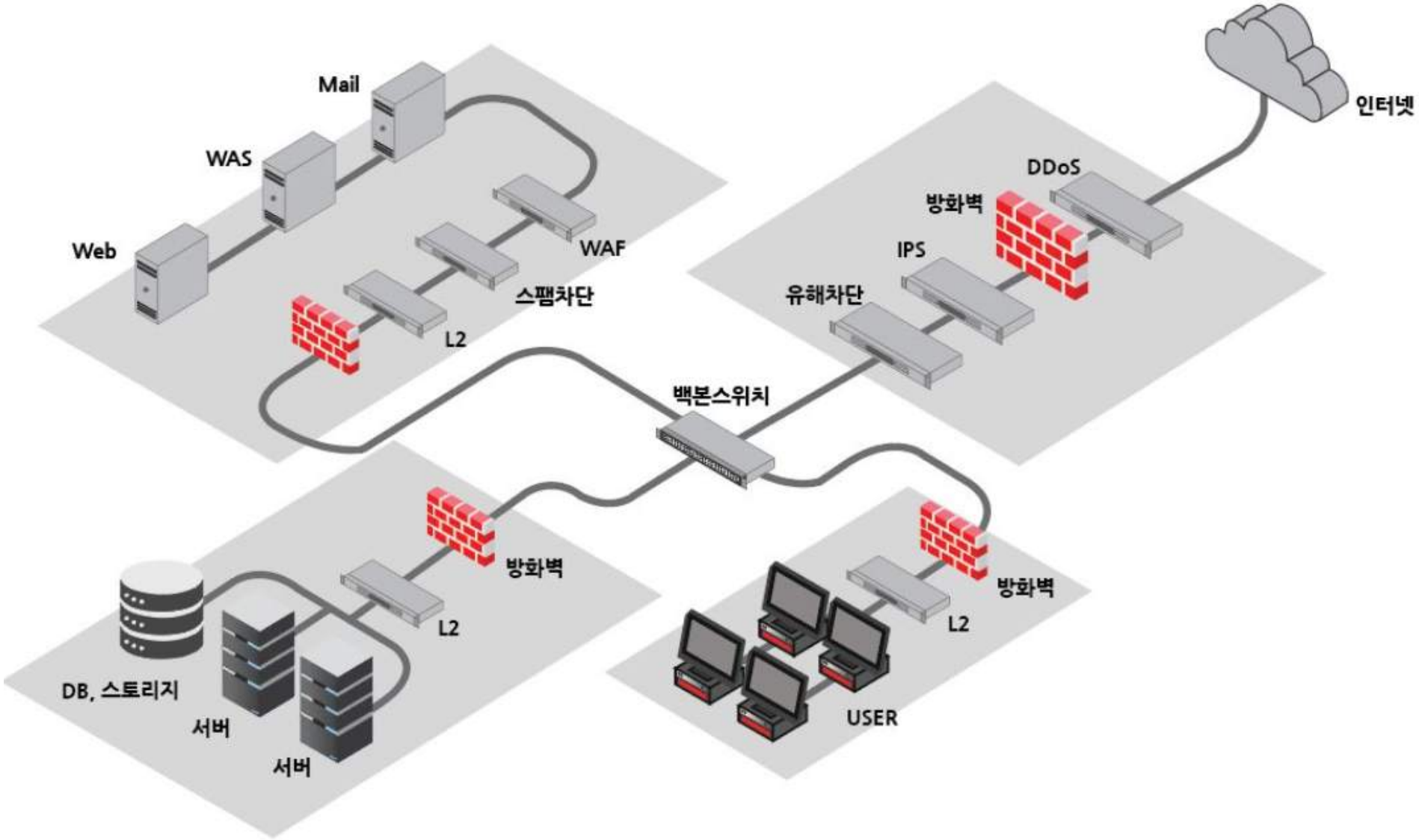
보안망 구성(2)

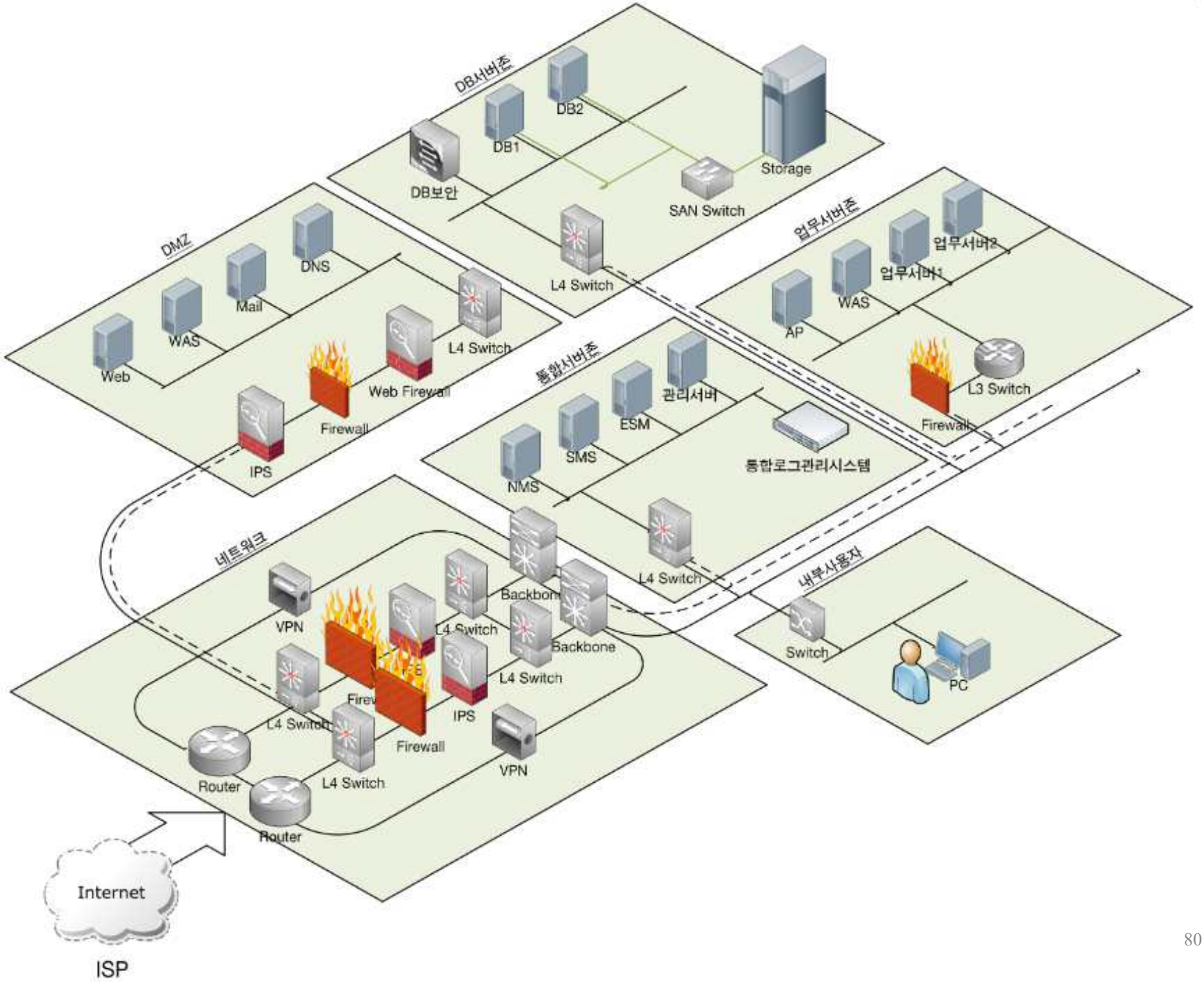


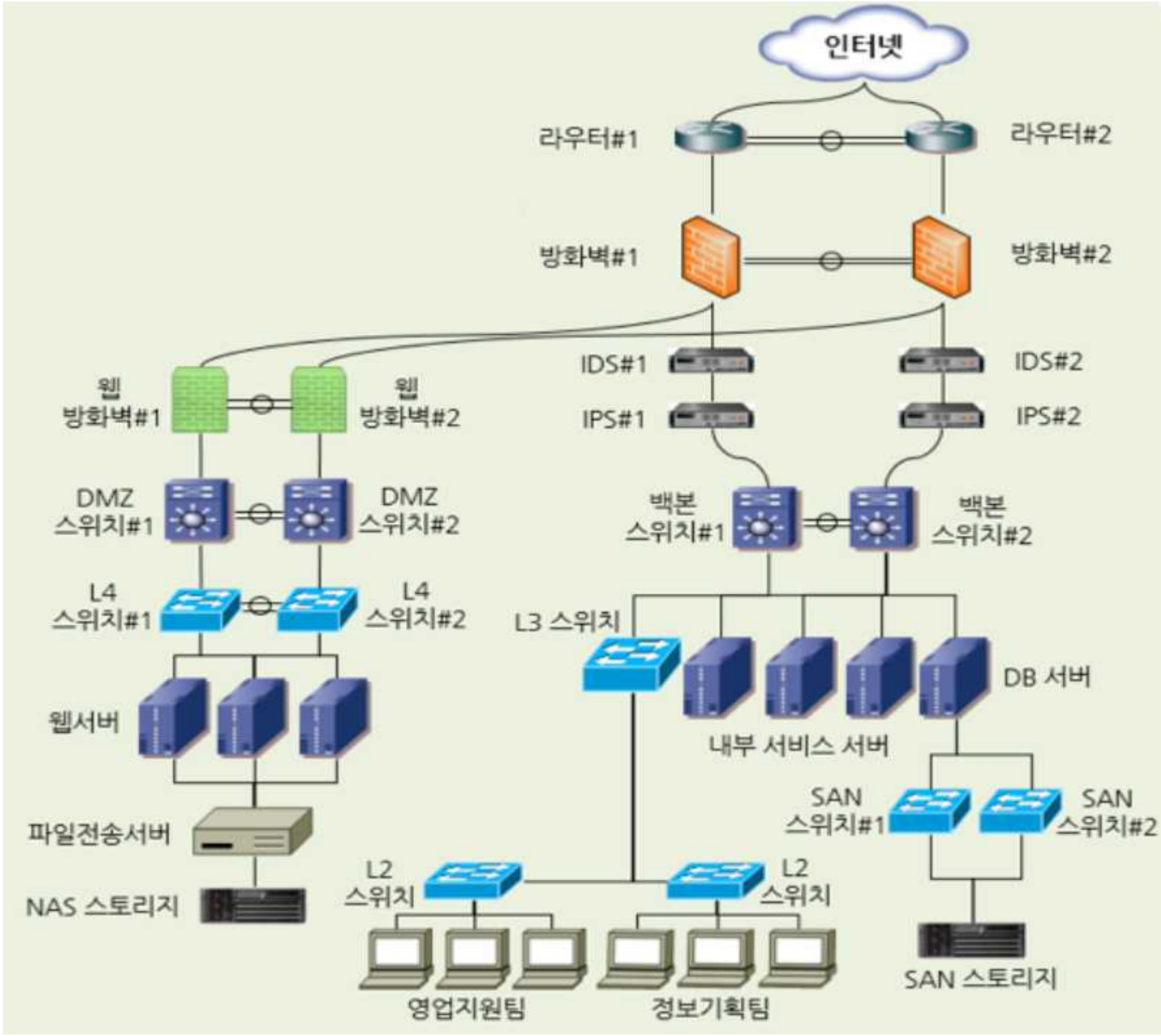
Intranet Zone(Private/Trust)



DMZ Zone(Service/Public)


Mail
WAS
Web
WAF
스팸차단
L2
인터넷
DDoS
방화벽
IPS
유해차단
백본스위치
방화벽
L2
DB, 스토리지
서버
서버
방화벽
L2
USER


DB서버존
DB2
DB1
DB보안
Storage
SAN Switch
L4 Switch
업무서버존
업무서버2
업무서버1
WAS
AP
L3 Switch
Firewall
DMZ
DNS
Mail
WAS
Web
L4 Switch
Web Firewall
Firewall
IPS
통합서버존
관리서버
ESM
SMS
NMS
통합로그관리시스템
L4 Switch
네트워크
VPN
Backbone
L4 Switch
Backbone
L4 Switch
IPS
Firewall
L4 Switch
VPN
Router
Router
내부사용자
Switch
PC
Internet
ISP


인터넷
라우터#1
라우터#2
방화벽#1
방화벽#2
IDS#1
IDS#2
IPS#1
IPS#2
웹
방화벽#1
웹
방화벽#2
DMZ
스위치#1
DMZ
스위치#2
백본
스위치#1
백본
스위치#2
L4
스위치#1
L4
스위치#2
L3 스위치
웹서버
DB 서버
내부 서비스 서버
SAN
스위치#1
SAN
스위치#2
파일전송서버
NAS 스토리지
L2
스위치
L2
스위치
SAN 스토리지
영업지원팀
정보기획팀