

Network

For Presentation

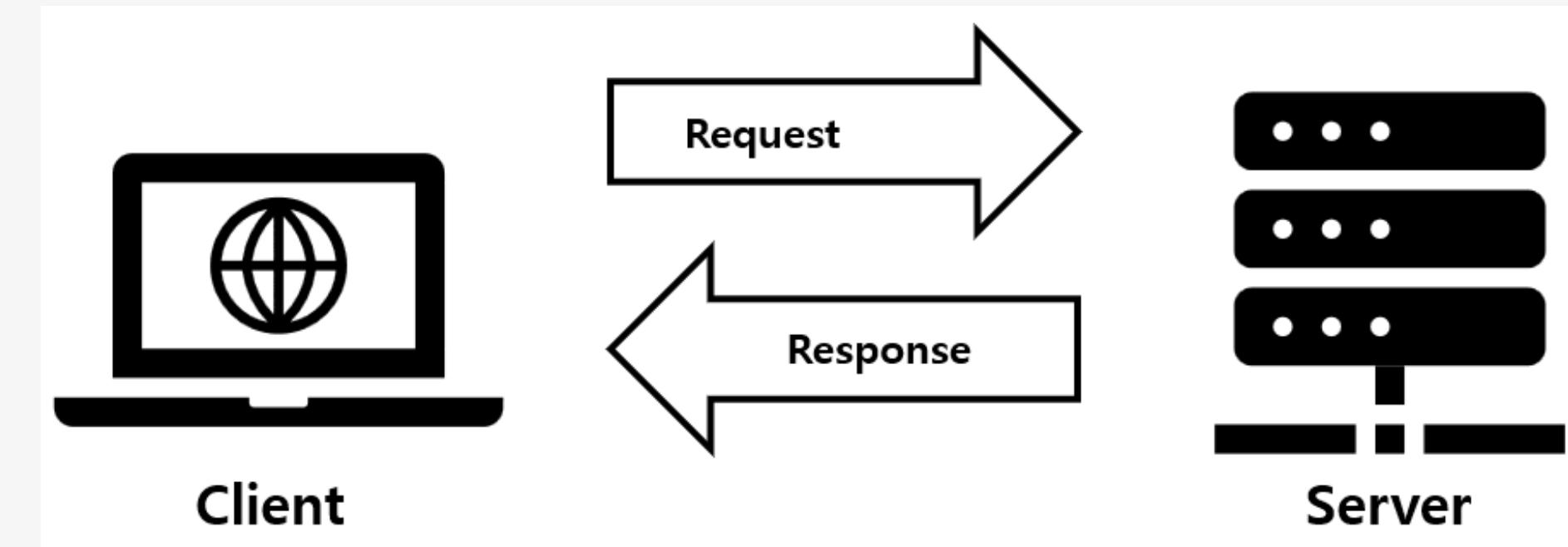
2023 June 23
Lim taehee



Index

- 1. Server, Client
- 2. Packet tracer
- 3. Ethernet, Bluetooth, Access point
- 4. Port number, Protocol
- 5. NAT
- 6. Port Forwarding
- 7. DHCP
- 8. Port scanning
- 9. OSI 7 layer, Internet 4 layer
- 10. TCP, UDP
- 11. Firewall
- 12. IPS, IDS
- 13. UTM
- 14. NAC
- 15. Sniffing
- 16. MITM
- 17. Spoofing
- 18. DOS, DDOS, DRDOS (zombiePC, RAT, C&C)
- 19. Network Traffic management & distribution
- 20. Network Infrastructure configuration example
- 21. Cloud
- 22. Network Certification

Server - Client



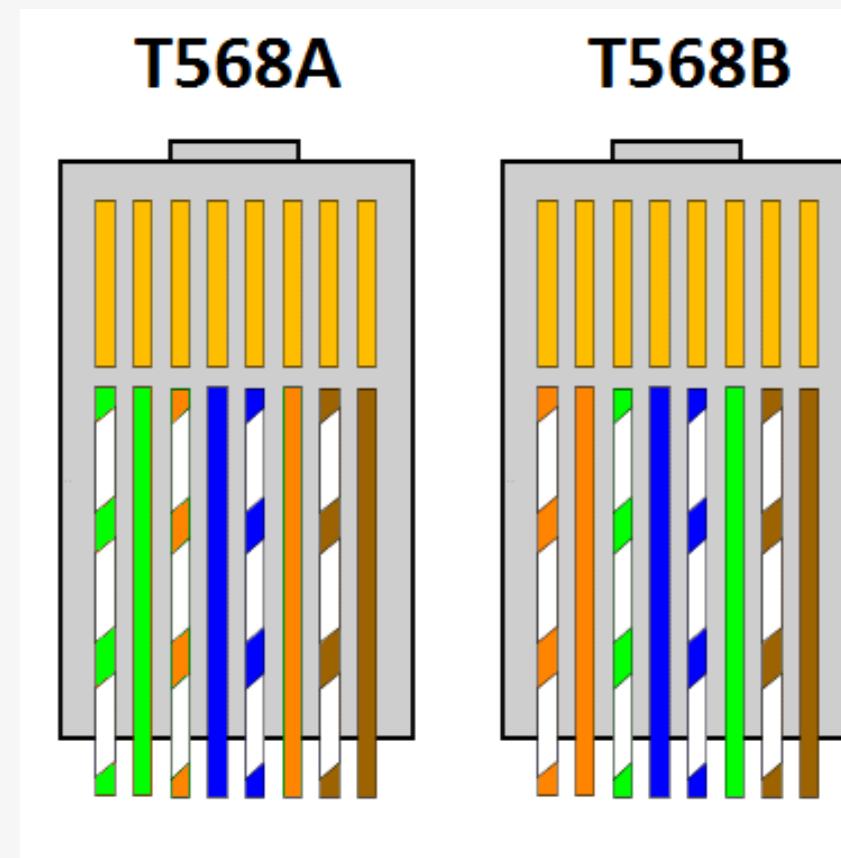
서버 : 다수의 클라이언트에게 서비스를 제공하기 위한 장치

클라이언트 : 서비스를 받으려고 하는 장치

Packet Tracer



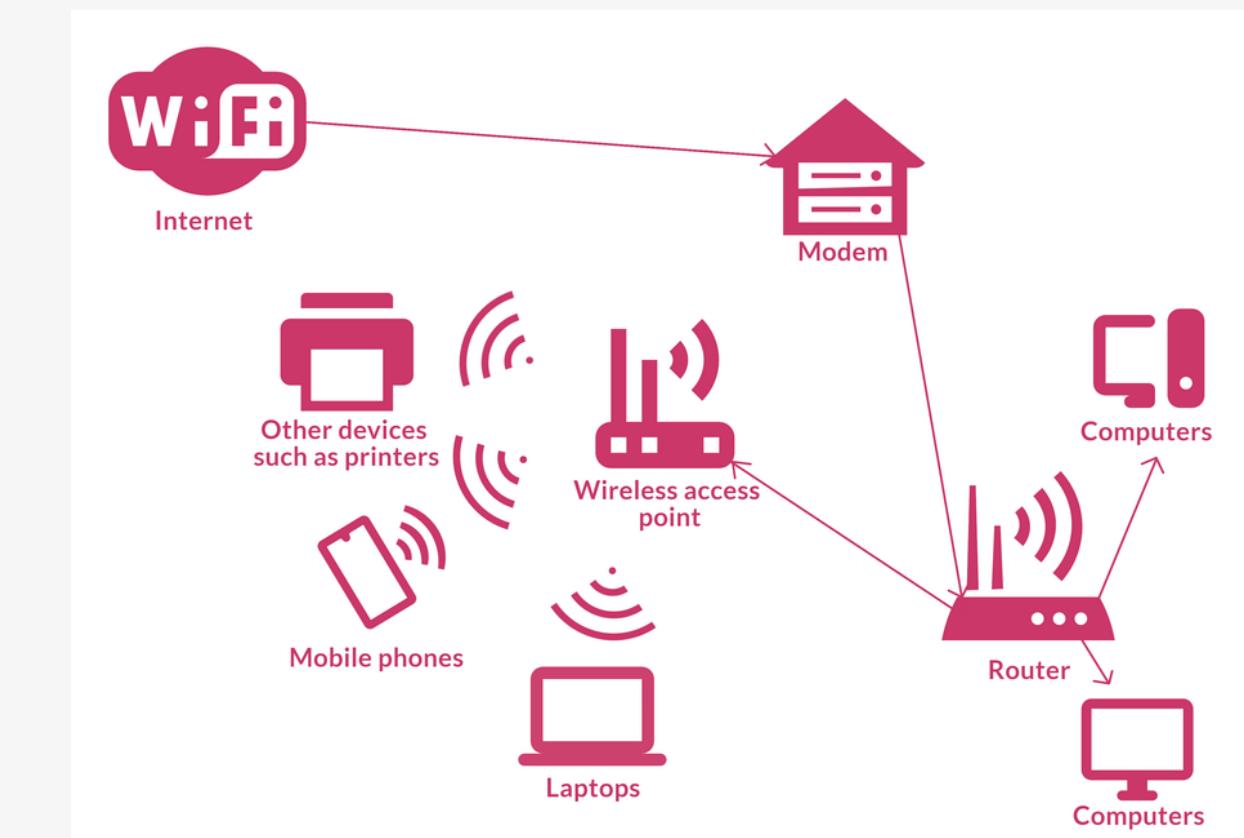
Ethernet, Bluetooth, Access point



Ethernet
IEEE 802.3



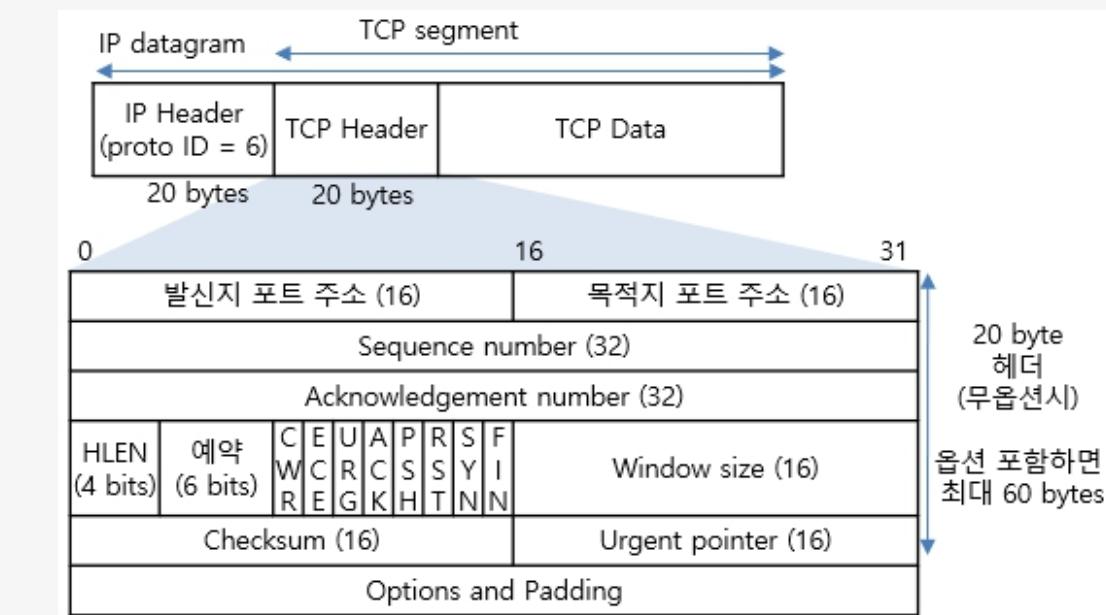
Bluetooth(10m)
IEEE 802.15.1



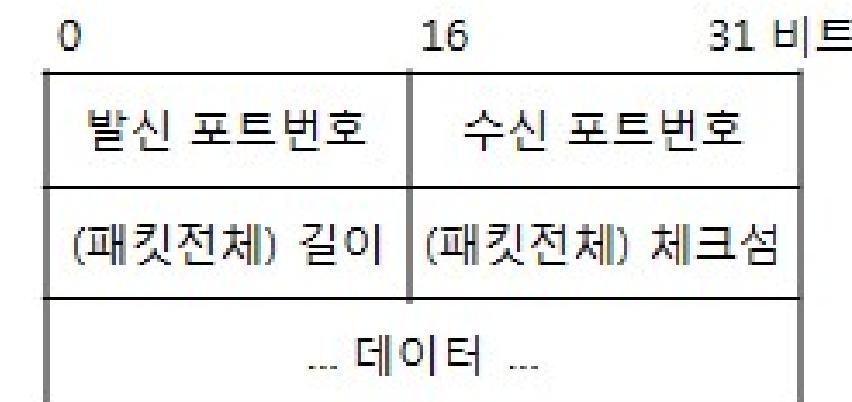
Access Point
wireless access point

Port number, Protocol

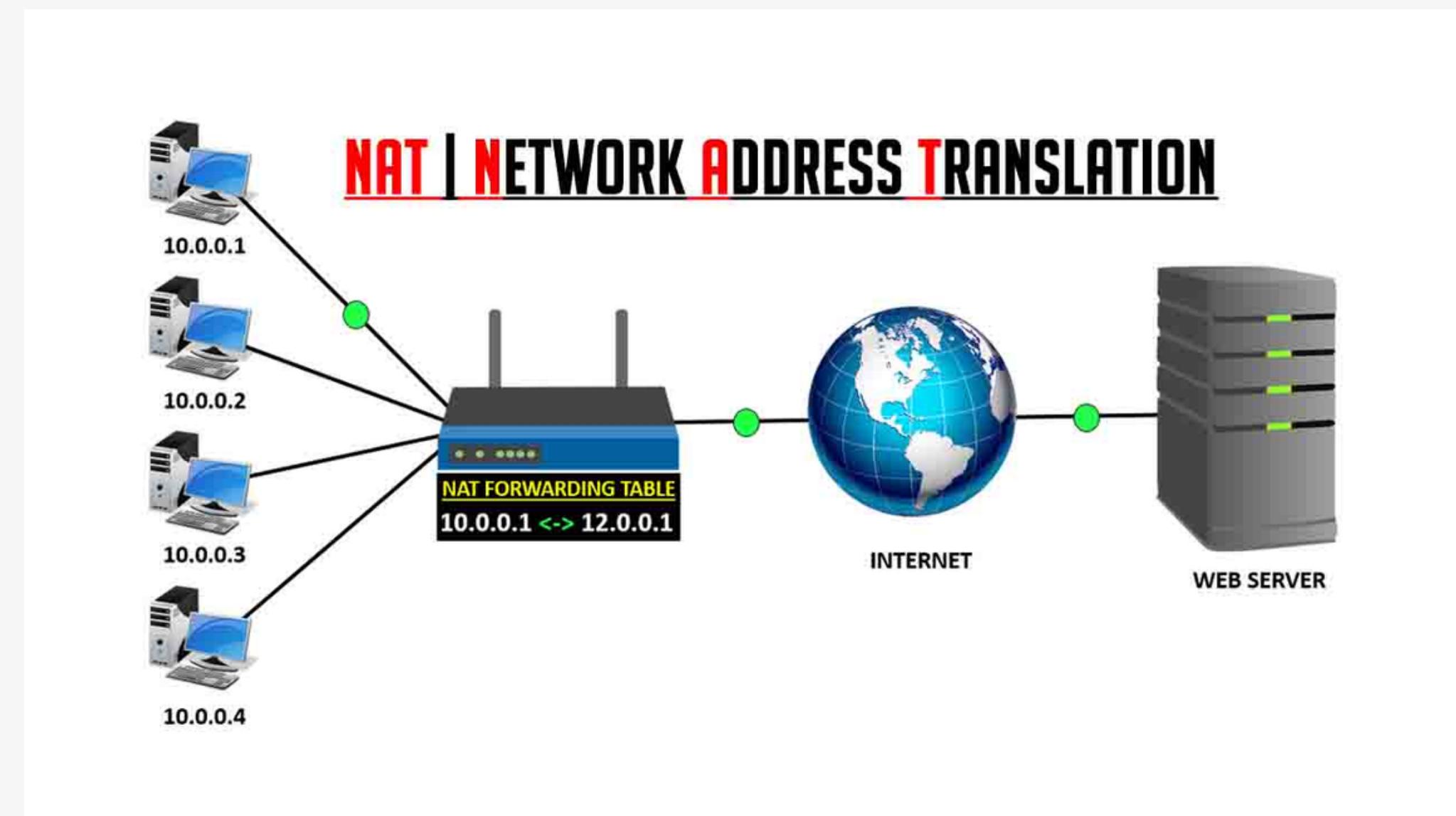
- 20 : FTP(File Transfer Protocol) data transfer
- 21 : FTP(File Transfer Protocol) command
- 22 : SSH(Secure Shell)
- 23 : Telnet(Telecommunication Networking)
- 25 : SMTP(Simple Message Transfer Protocol)
- 53 : DNS(Domain Name Service)
- 80 : HTTP(HyperText Transfer Protocol)
- 110 : POP3(Post Office Protocol)
- 123 : NTP(Network Time Protocol)
- 143 : IMAP(Internet Messaging access protocol)
- 443 : HTTPS(HTTP over SSL(Secure Socket Layer))
- 445 : SMB(Server Message Block)
- 3306 : MySQL



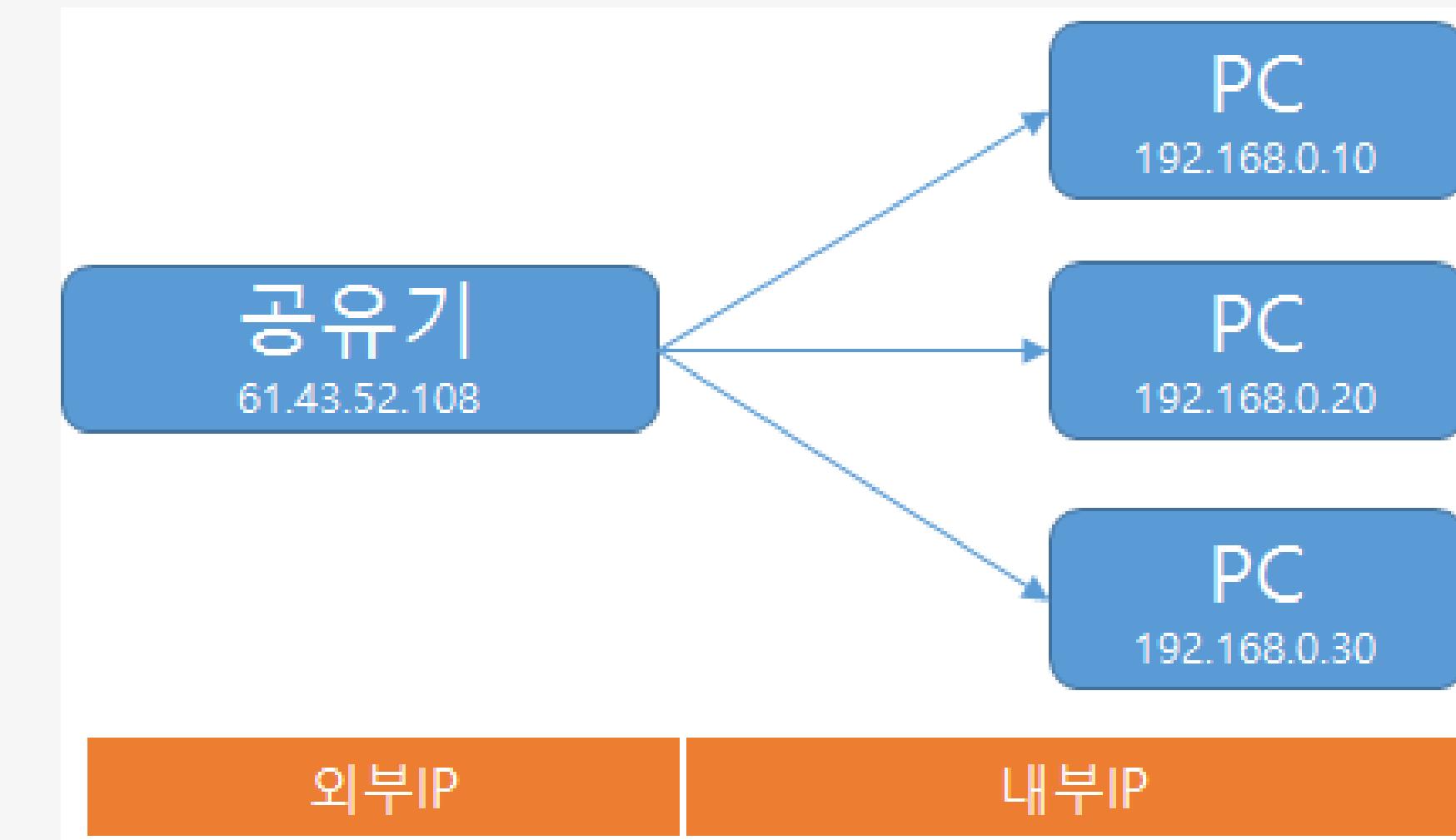
o UDP 패킷 헤더 구조



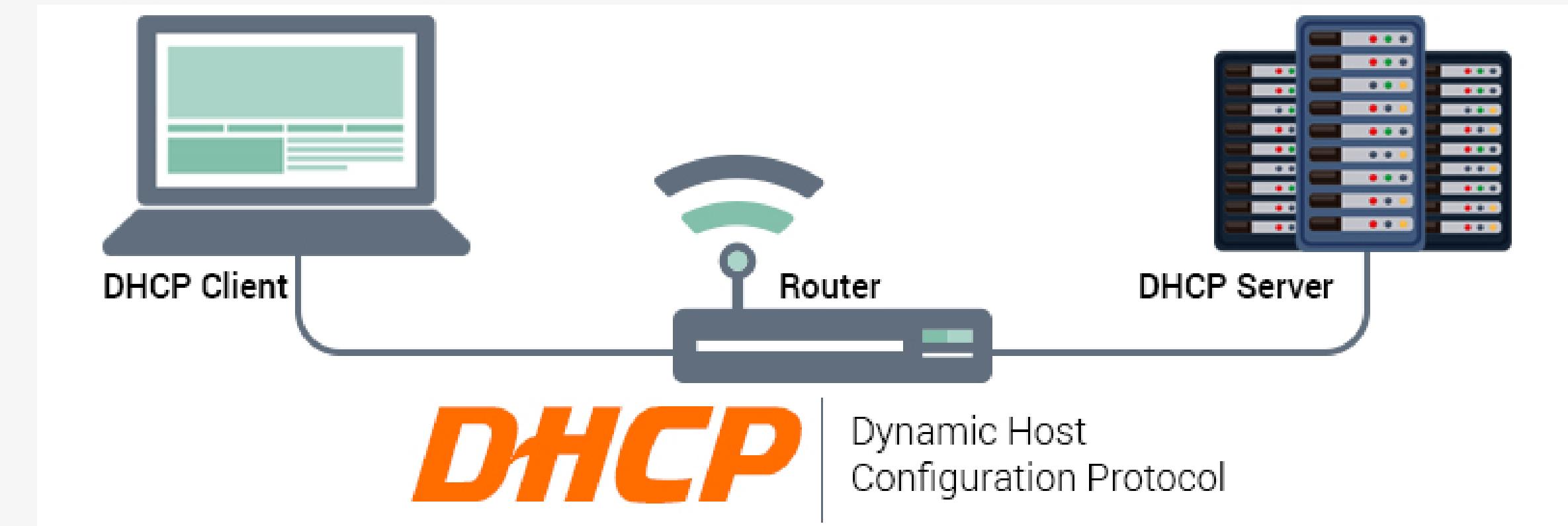
NAT

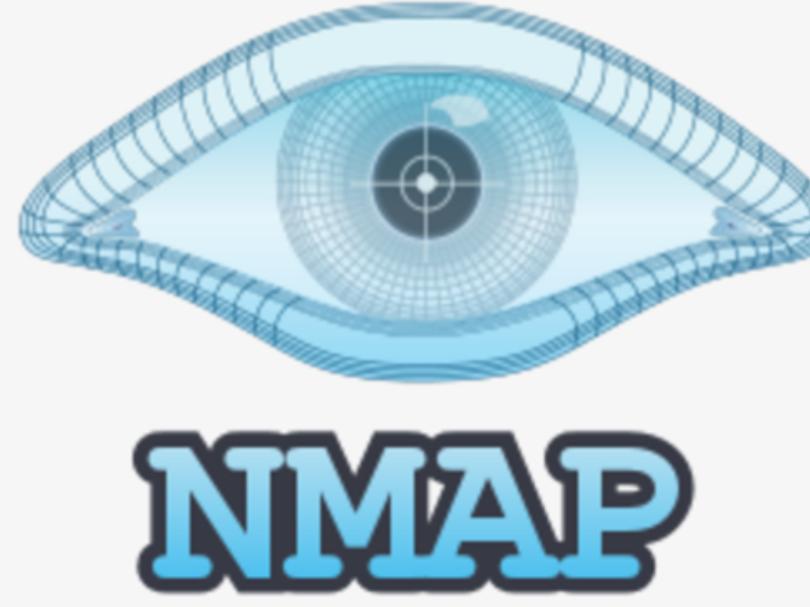


Port Forwarding



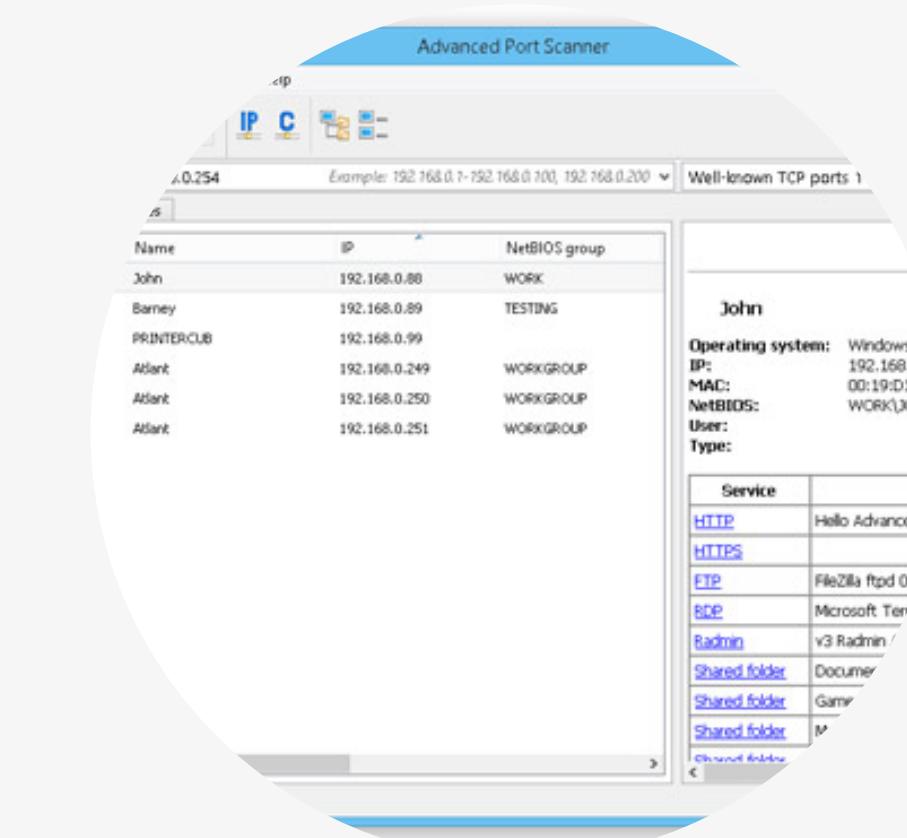
DHCP





NMAP

Port Scanning

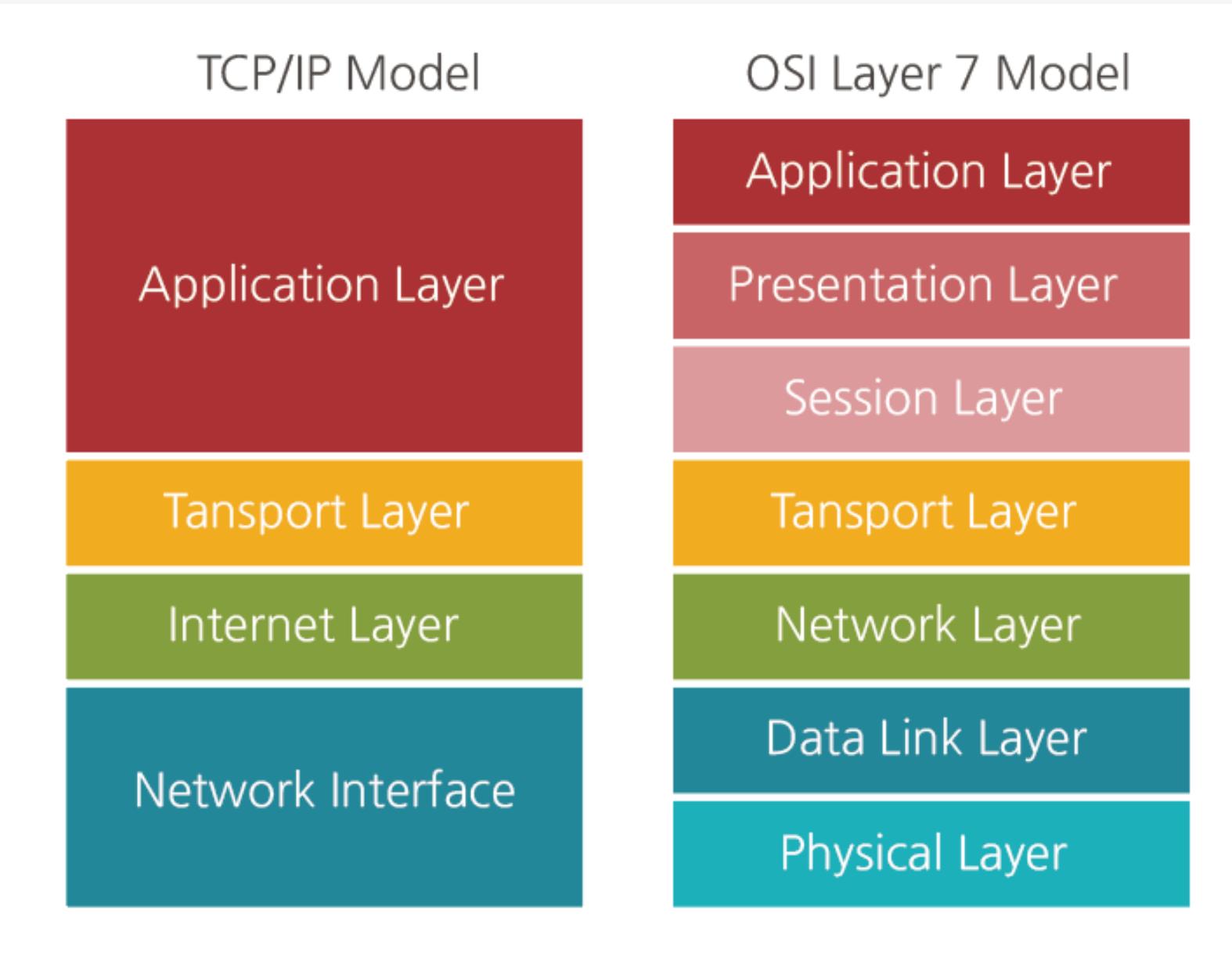


Advanced port scanner

```
1 import nmap
2 DATA_DICT = {}
3 nmScan = nmap.PortScanner()
4 hostName="google.com"
5 for a in range(80,100): #80 to 443
6     print("Checking port no:",a)
7     portNumber=str(a)
8     # print('checking port no:',portNumber)
9     d=nmScan.scan(hostName, portNumber)
10    print(d)
```

python NMAP

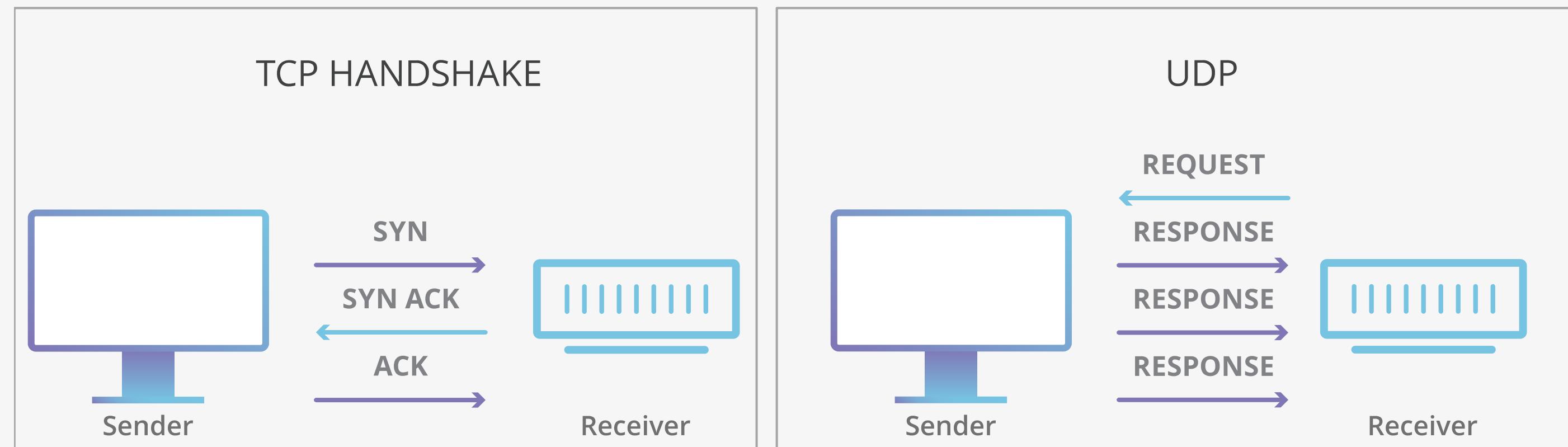
OSI 7 layer, Internet 4 layer



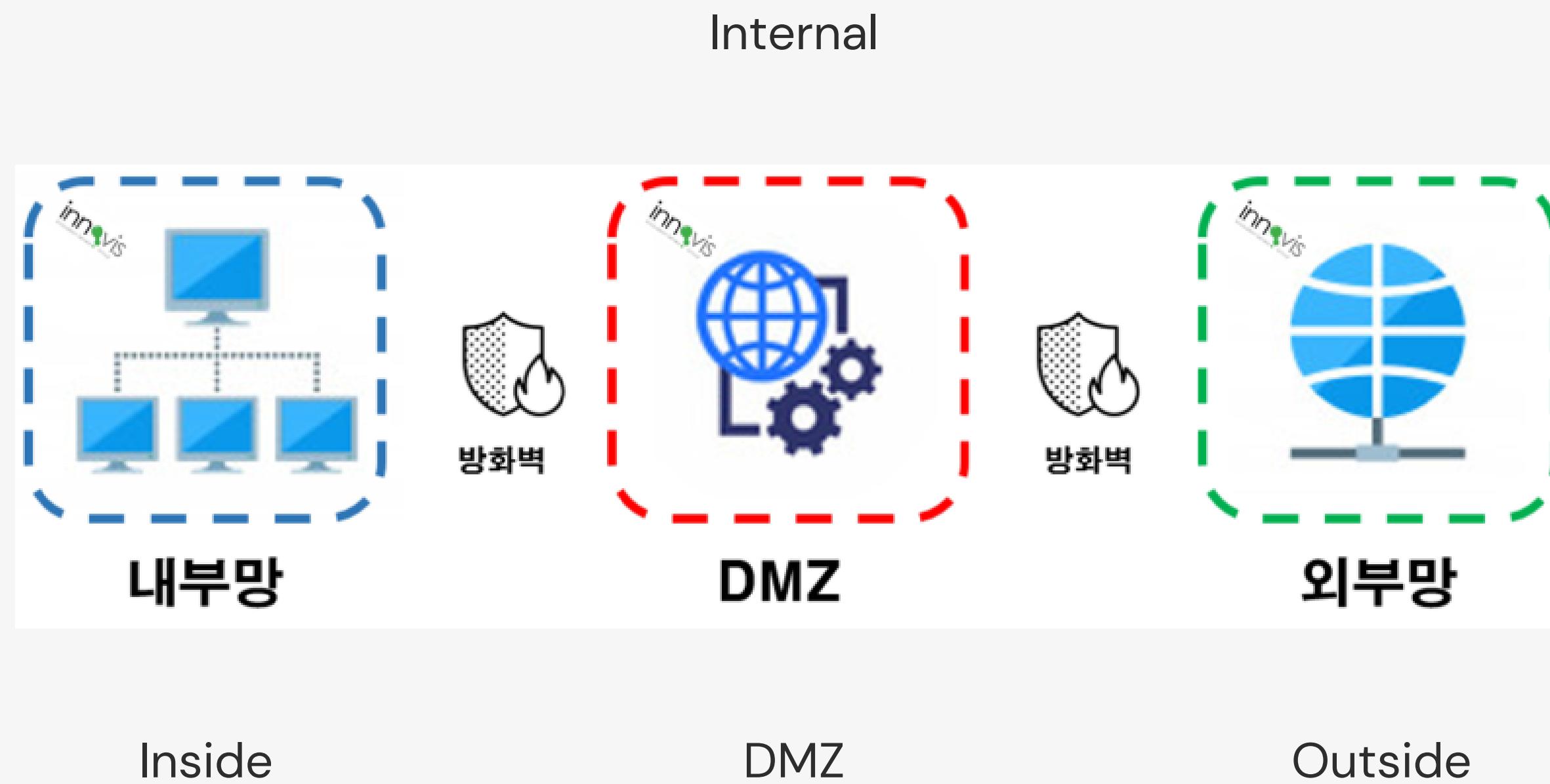
- DNS, FTP, HTTP, NTP, SMTP
- 압축, 암호화, 복호화, 데이터변환
- NetBIOS, 인증 및 허가
- TCP, UDP
- IP, ICMP, IPsec
- ARP, MAC
- 블루투스, USB, RS-232

TCP, UDP

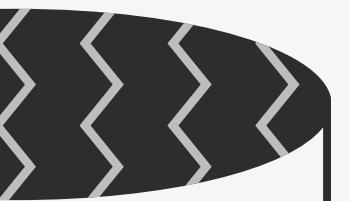
TCP vs UDP Communication



Firewall



IDS, IPS



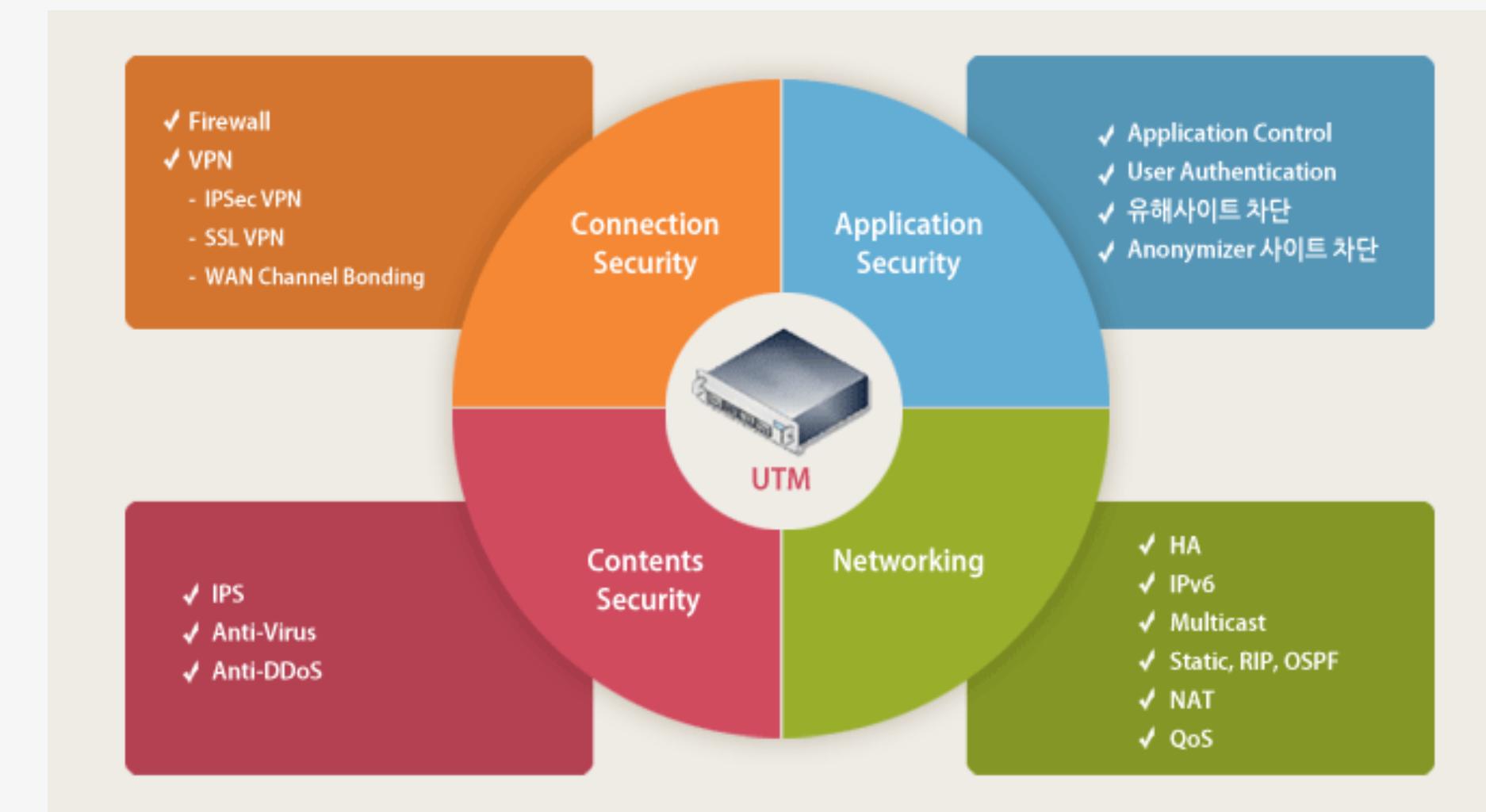
IDS (Intrusion Detection System)

침입 탐지 시스템의 약자로서
패킷 차단이나 행위 방지보다는
탐지만 하는 장비
장점 : 싸다, 패킷에 대한 분석을 세
밀하게 모니터링 할 수 있다.
단점 : 행위 방지나 차단기능이 없음

IPS (Intrusion Detection System)

침입 차단 시스템의 약자로서
패킷 차단이나 행위 방지 기능도
제공하는 장비
장점 : 행위 방지나 차단이 가능하
다.
단점 : 비싸다

UTM

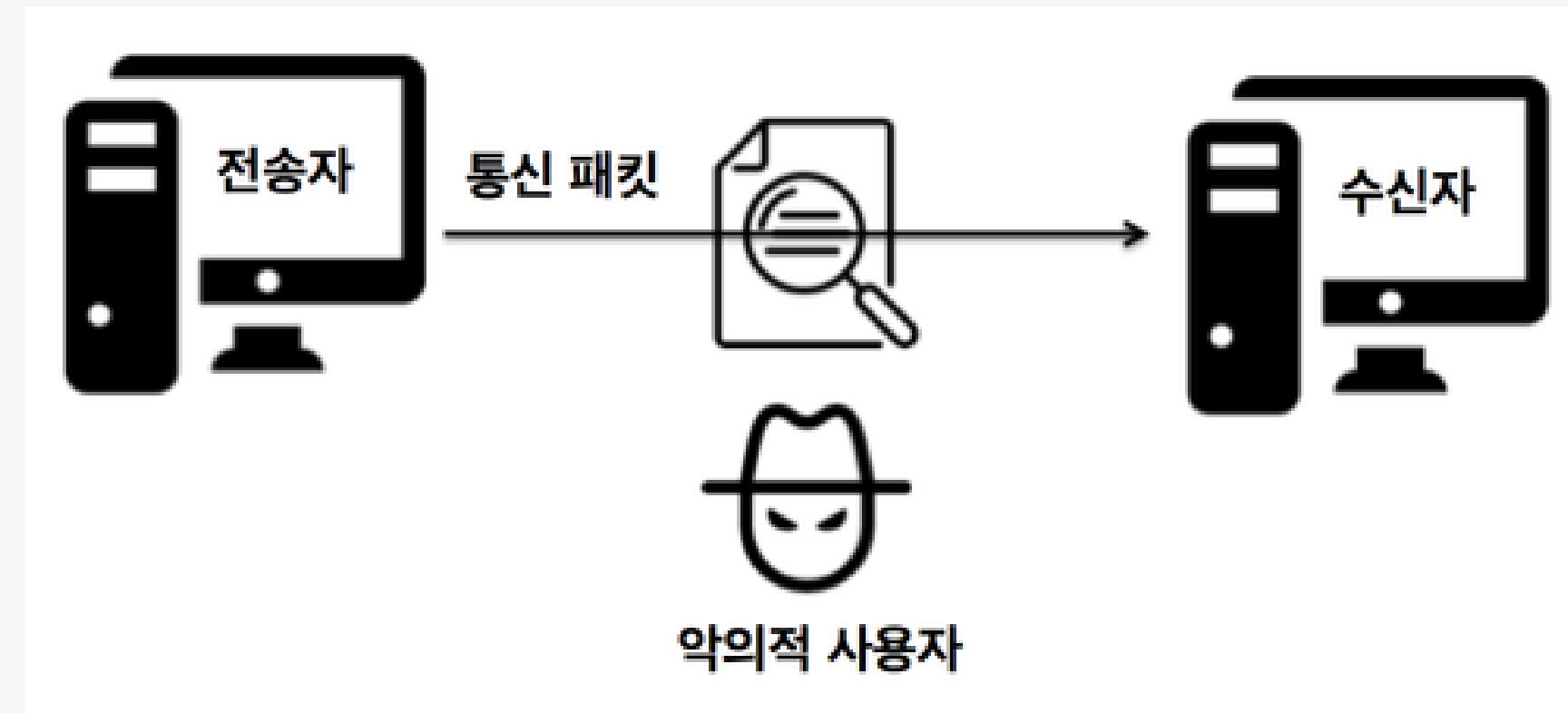


Unified Threat Management

NAC

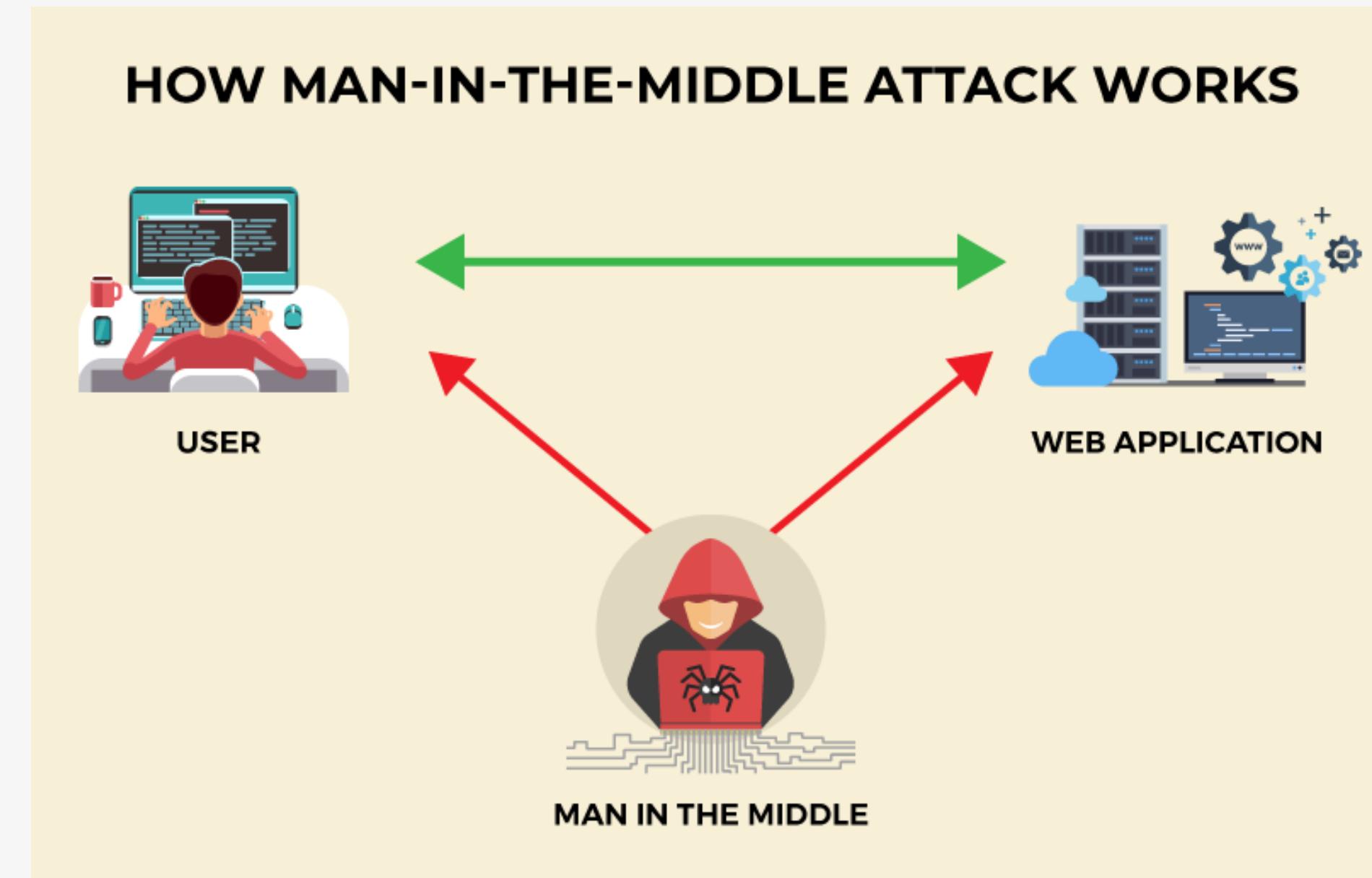


Sniffing

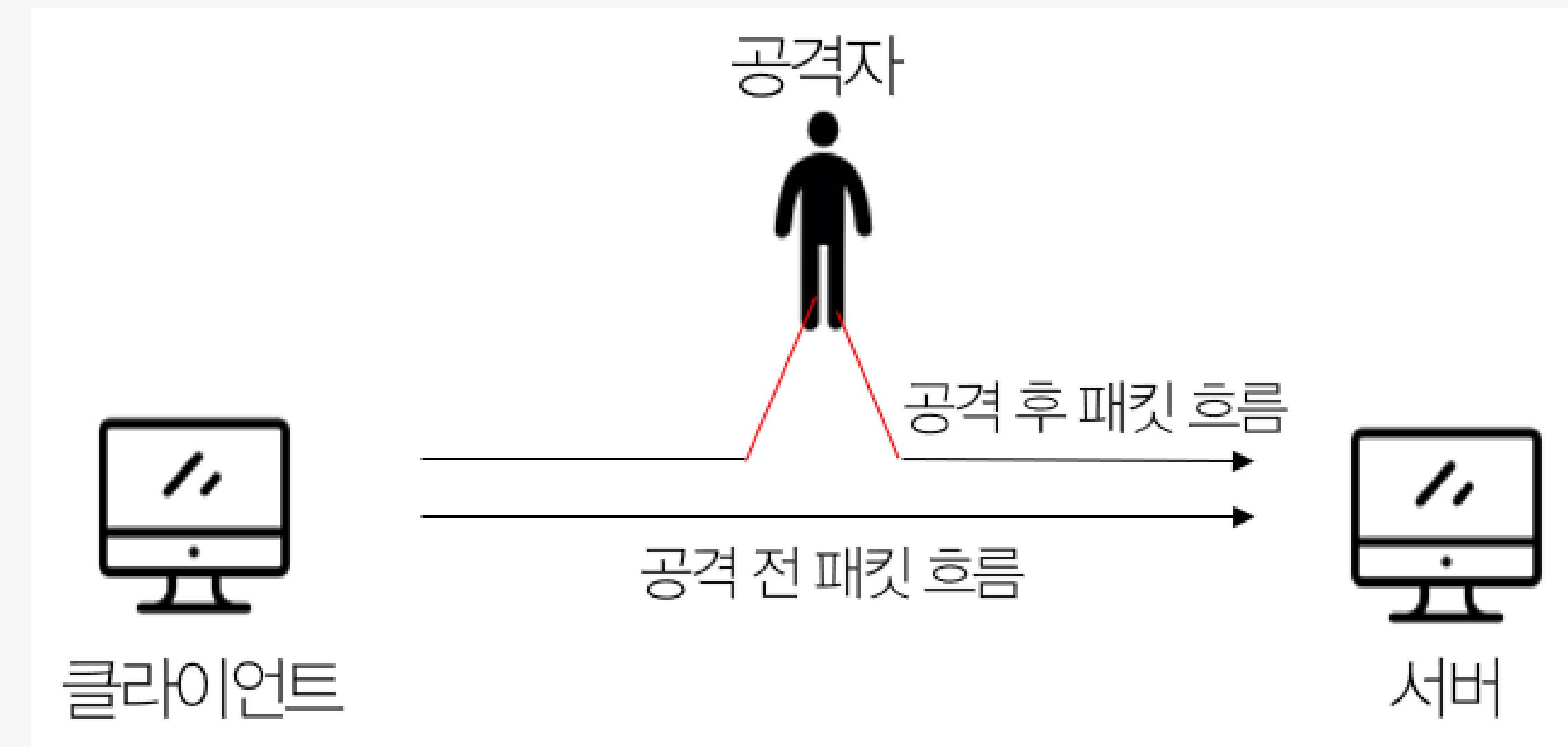


from scapy import *

MITM



Spoofing



ip

DNS

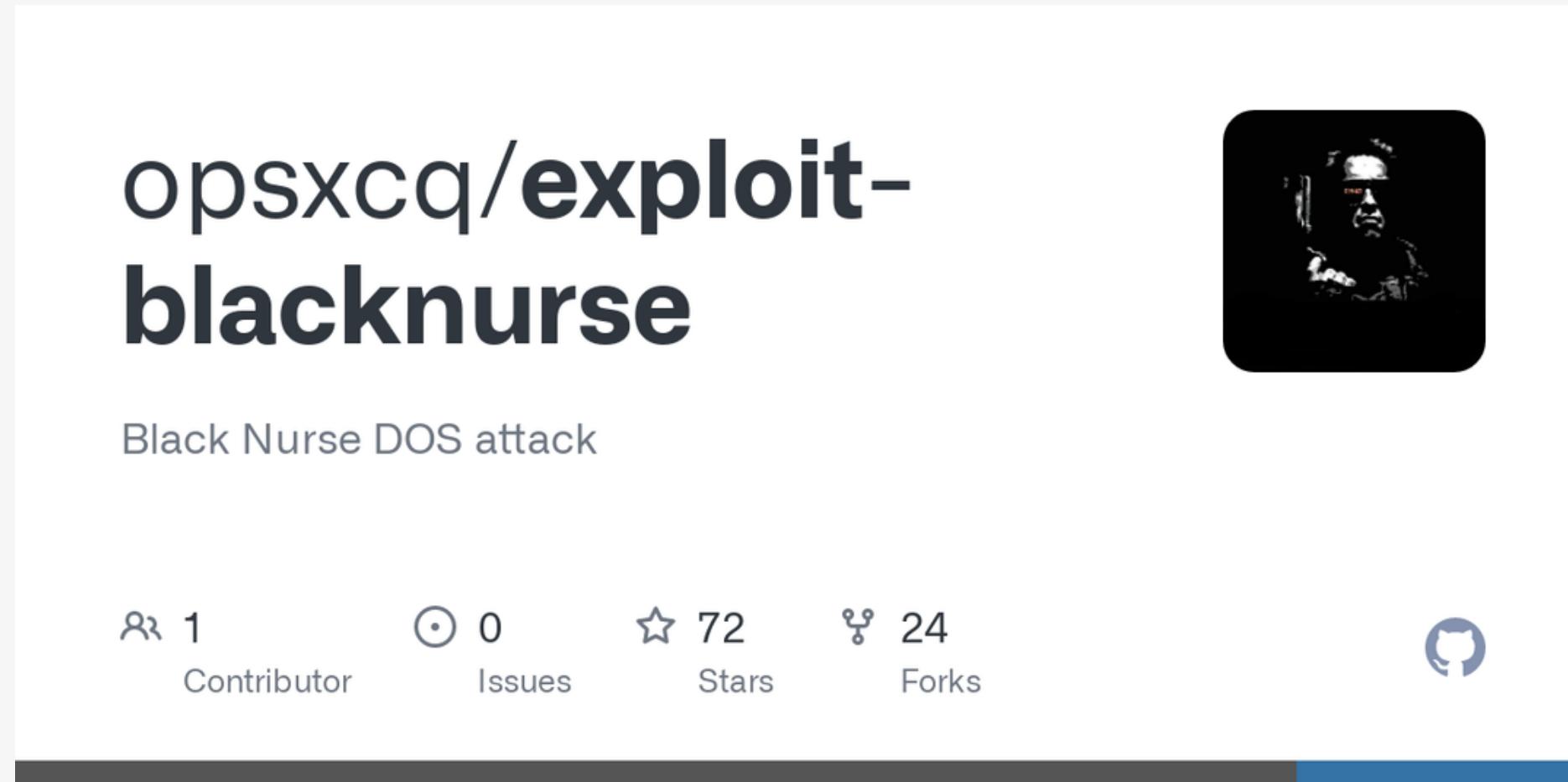
ARP

DOS, DDOS, DRDOS

[opsxcq/exploit-blacknurse](#)

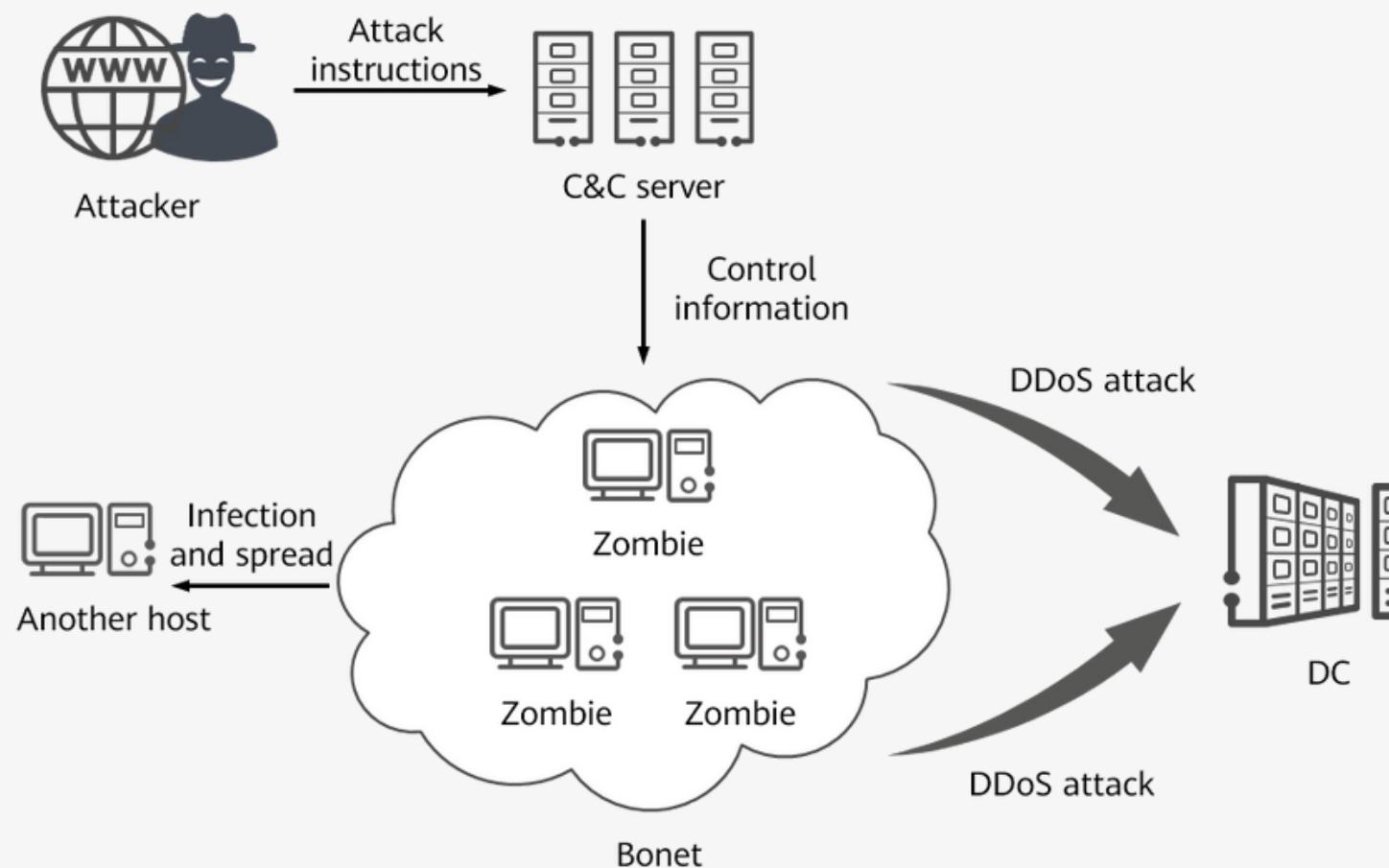
Black Nurse DOS attack

1 Contributor 0 Issues 72 Stars 24 Forks



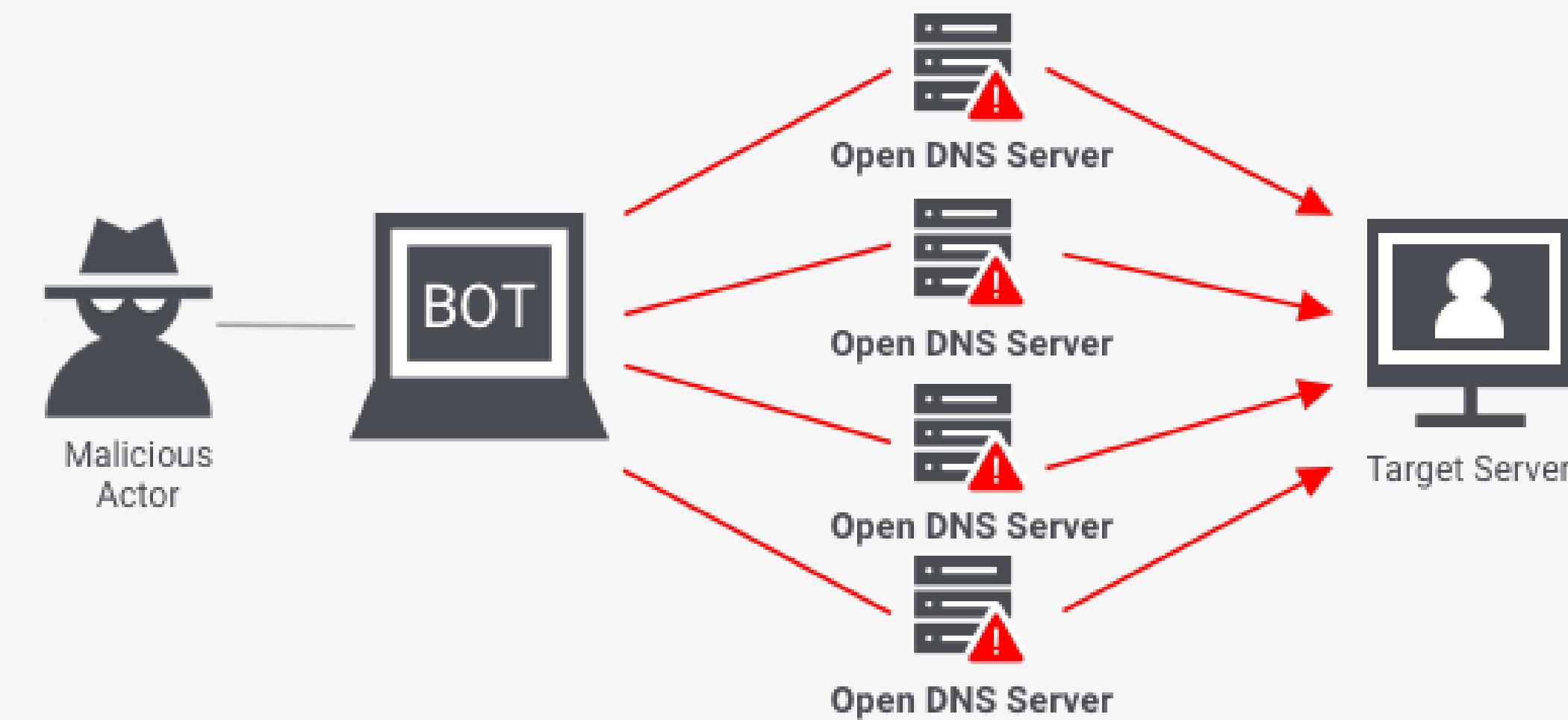
1. 전산 자원을 소진
2. 구성 정보를 교란
3. 상태 정보를 교란
4. 물리적 전산망 요소를 교란
5. 원래 사용자와 희생물 사이의 통신 매체 차단

DOS, DDOS, DRDOS

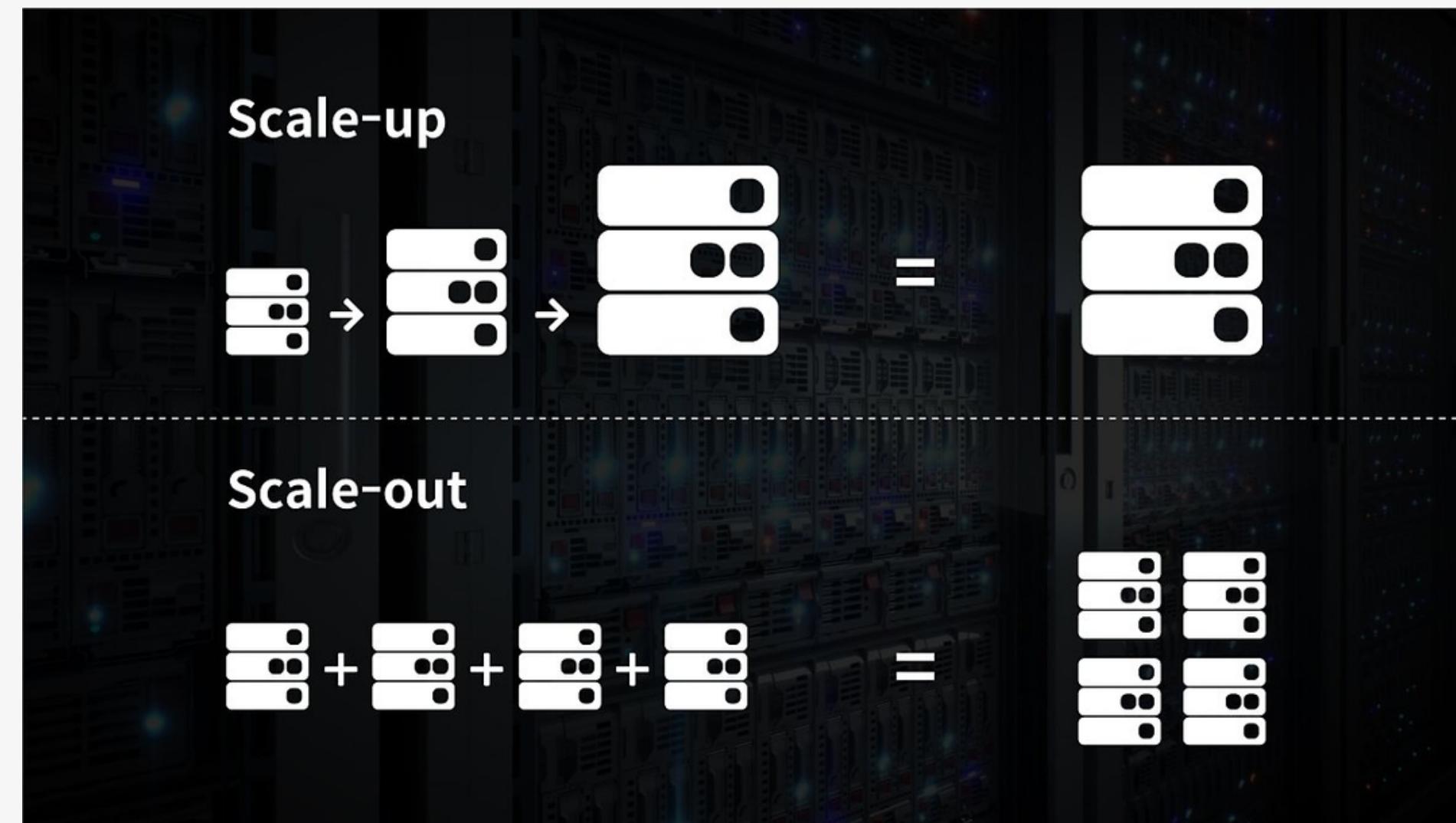


구분	대역폭 공격	자원 소진 공격	Web/DB 부하공격
사용 Protocol	UDP, ICMP, TCP, GRE 등	TCP	HTTP, HTTPS
공격 유형	ICMP/UDP Flooding, Fragmentation 공격, UDP 기반 반사공격 (DNS, NTP, CLDAP, SSDP 등)	SYN Flooding, Flag Flooding, TCP Open Flooding 등	비정상적인 HTTP request, HTTP Get Flooding 등
공격효과	동일 네트워크에서 사용중인 모든 시스템	대상서버, 보안장비, 네트워크 장비 등	대상 Web/DB 서버 과부하 발생
IP 위/변조 여부	위/변조 가능	위/변조 가능	위/변조 가능
비고	일시적으로 대량의 트래픽을 발생	대역폭 공격에 비해 적은 트래픽으로도 서버 과부하 발생	정상 세션을 맺은 후 과도한 HTTP 요청으로 Web/DB서버의 과부하를 유도함

DOS, DDOS, DRDOS



Network Traffic management & distribution



Network Traffic management & distribution

Round Robin

서버에 들어온 순서대로
분배

Weighted RR

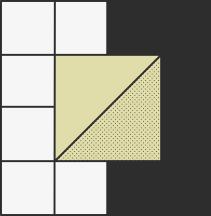
서버마다 가중치를 정
하고 그에 따라 분배

Least conn, response time

요청이 들어온 시점에 가장 적은 연결
상태, 서버와 연결 상태와 응답 시간 순
으로 분배

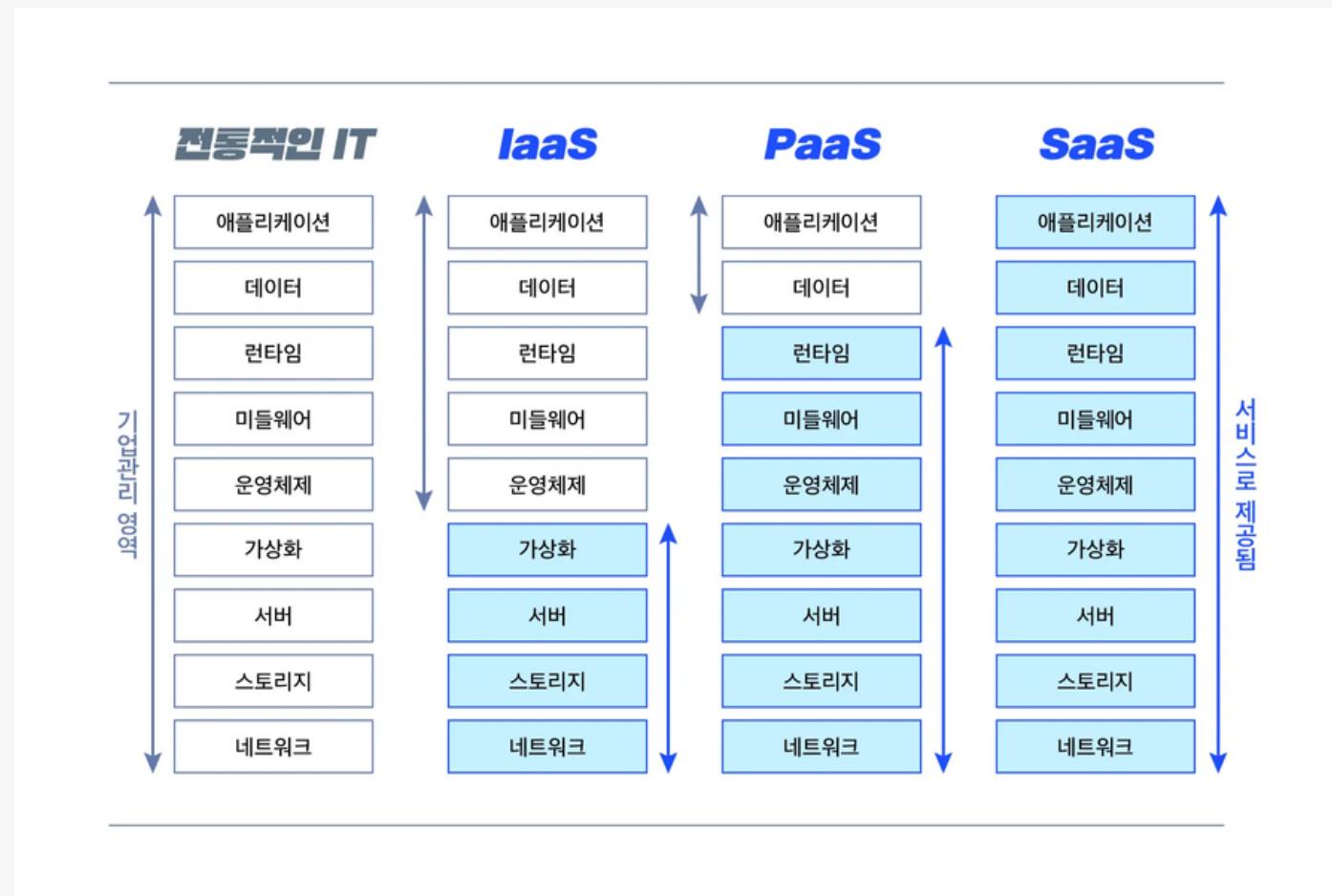
Network Traffic management & distribution

	L4 로드밸런서	L7 로드밸런서
네트워크 계층	Layer 4 전송계층(Transport layer)	Layer 7 응용계층(Application layer)
특징	> TCP/UDP 포트 정보를 바탕으로 함	> TCP/UDP 정보는 물론 HTTP의 URI, FTP의 파일명, 쿠키 정보 등을 바탕으로 함
장점	> 데이터 안을 들여다보지 않고 패킷 레벨에서만 로드를 분산하기 때문에 속도가 빠르고 효율이 높음 > 데이터의 내용을 복호화할 필요가 없기에 안전함 > L7 로드밸런서보다 가격이 저렴함	> 상위 계층에서 로드를 분산하기 때문에 훨씬 더 섬세한 라우팅이 가능함 > 캐싱 기능을 제공함 > 비정상적인 트래픽을 사전에 필터링할 수 있어 서비스 안정성이 높음
단점	> 패킷의 내용을 살펴볼 수 없기 때문에 섬세한 라우팅이 불가능함 > 사용자의 IP가 수시로 바뀌는 경우라면 연속적인 서비스를 제공하기 어려움	> 패킷의 내용을 복호화해야 하기에 더 높은 비용을 지불해야 함 > 클라이언트가 로드밸런서와 인증서를 공유해야하기 때문에 공격자가 로드밸런서를 통해서 클라이언트에 데이터에 접근할 보안 상의 위험성이 존재함



Network Infrastructure configuration example

CLOUD



IaaS

Amazon AWS, MS Azure

PaaS

AWS Elastic Beanstalk, Heroku,
Red Hat OpenShift

SaaS

Dropbox, Salesforce, Google
Drive, Naver MYBOX

Network Certification

\$900 == 102만원->

\$300 == 36만원->

