‘외워서’ 끝내는 네트워크 핵심이론 – 응용

당장 네트워크를 전공할 수 없다면

그냥 외워라!

널널한 개발자 최호성 (cx8537@naver.com)

YouTube: 널널한 개발자 TV

수강에 앞서

1. 외워서 끝내는 **네트워크 핵심이론 기초를 완강**한 것으로 가정.
2. 인터넷 **공유기**를 사용해본 경험이 있으며 내용을 이해하지 못하더라도 관련 설정을 찾아보고 변경할 수 있음.

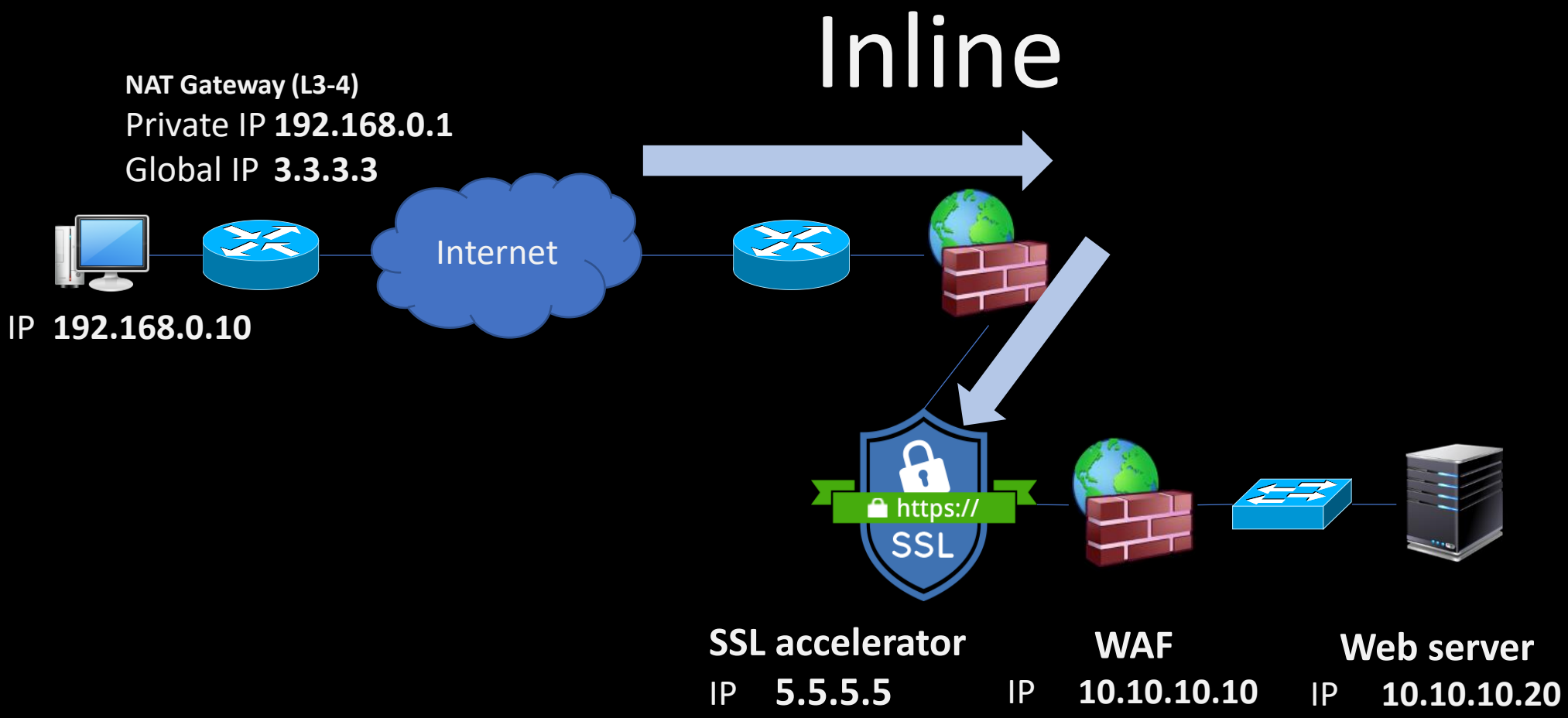
학습목표

- **네트워크 장치의 3대 구조**를 이해한다.
- **NAT**기술 기반 인터넷 **공유기** 작동원리를 이해한다.
- **부하분산 장치**의 원리를 이해한다.
- **VPN**의 구조와 원리를 이해한다.
- 주요 **네트워크 보안 장치**의 특징을 이해한다.

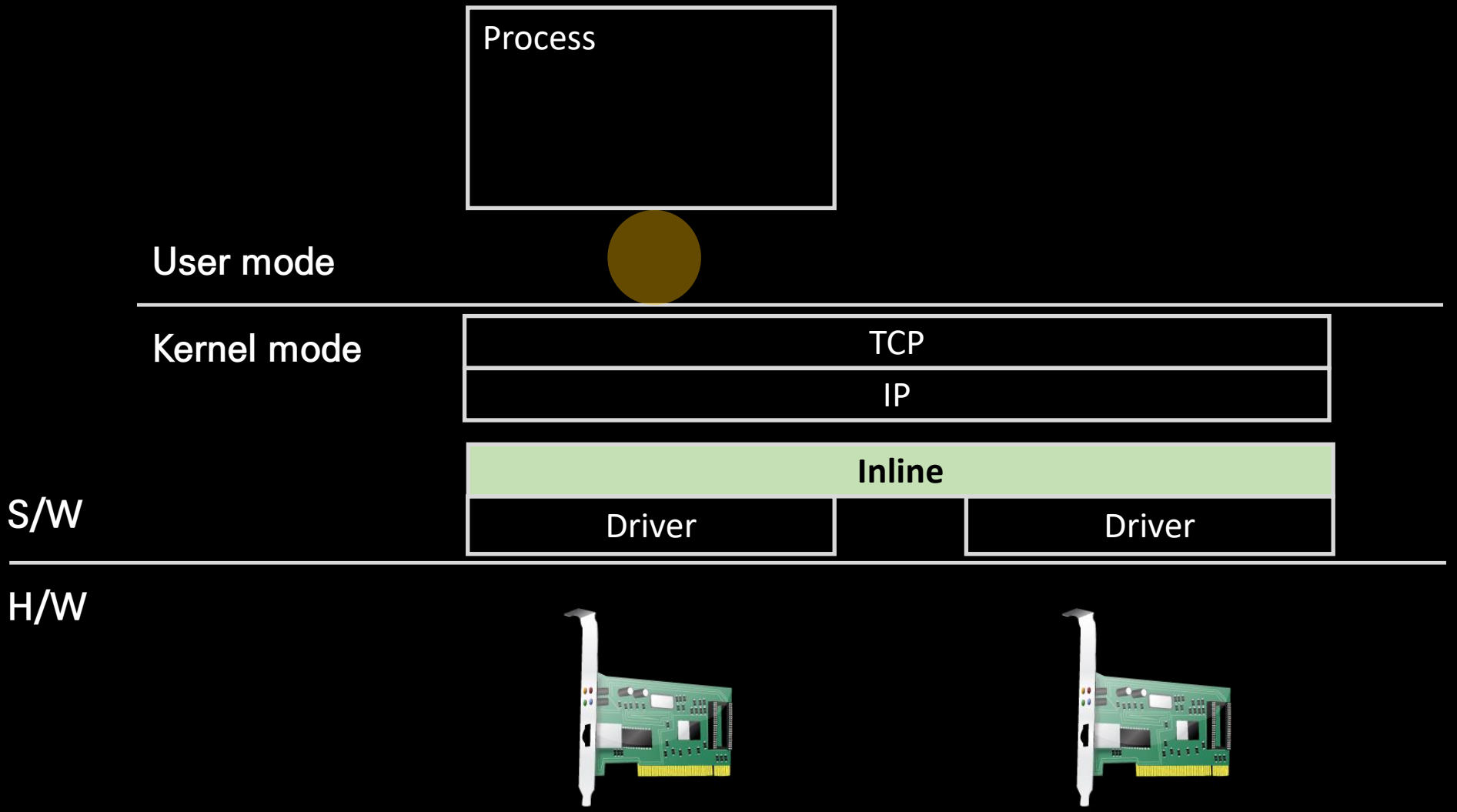
세 가지 네트워크 장치 구조

- Inline
  - Packet + Drop/Bypass + Filtering
- Out of path
  - Packet + Read only, Sensor
- Proxy
  - Socket stream + Filtering

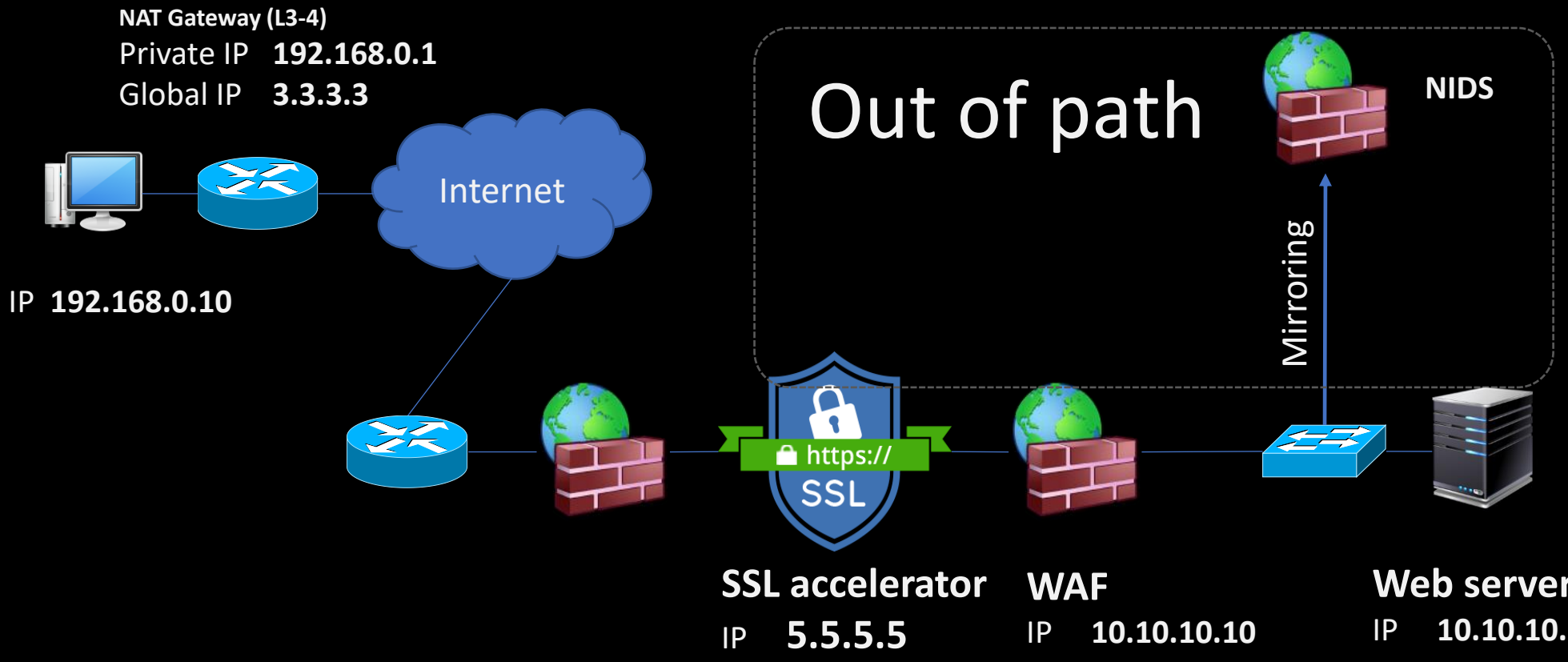
Inline 구조


Inline
NAT Gateway (L3-4)
Private IP 192.168.0.1
Global IP 3.3.3.3
Internet
IP 192.168.0.10
https://
SSL
SSL accelerator
IP 5.5.5.5
WAF
IP 10.10.10.10
Web server
IP 10.10.10.20

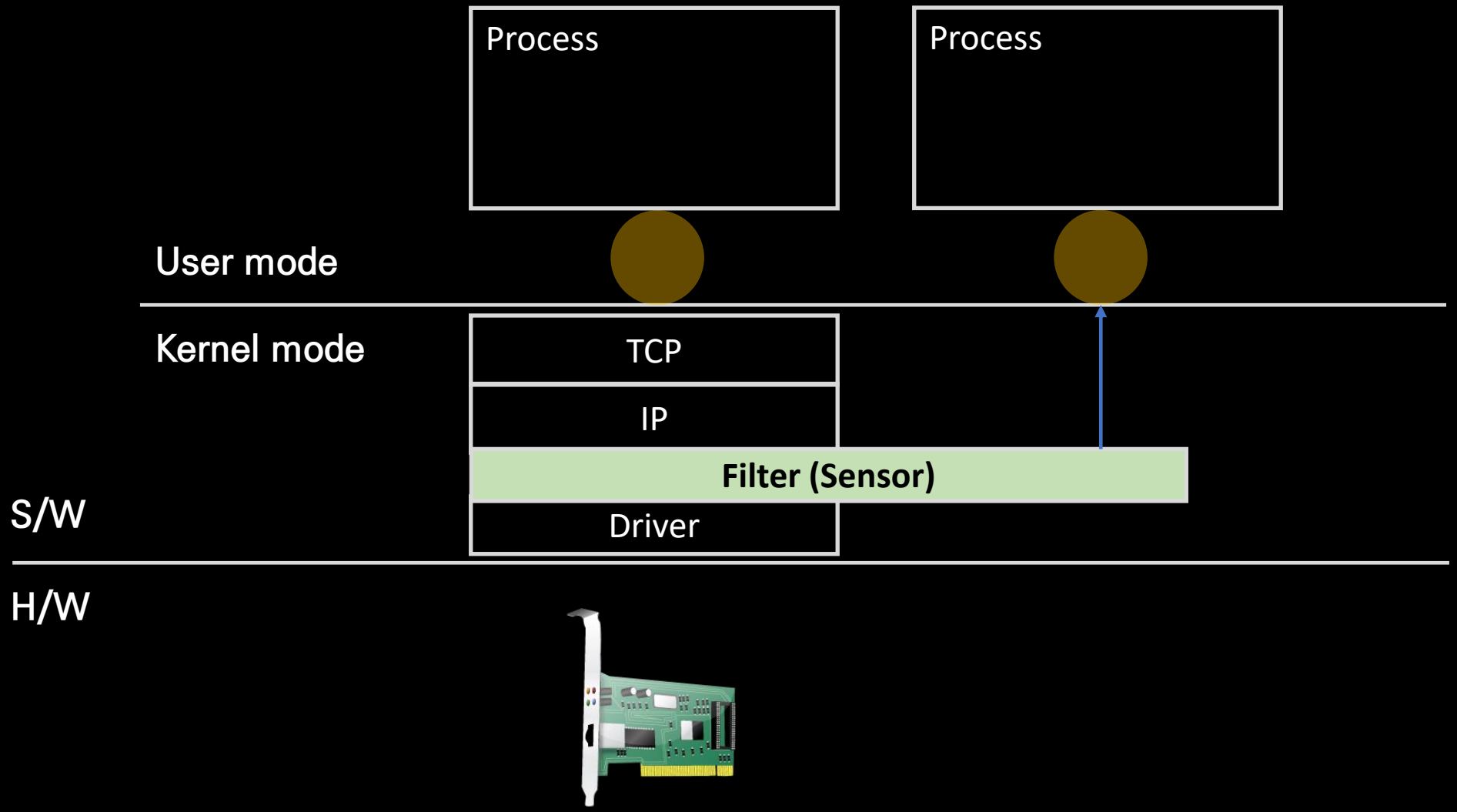
Inline 구조


Process
User mode
Kernel mode
TCP
IP
Inline
S/W
Driver
Driver
H/W

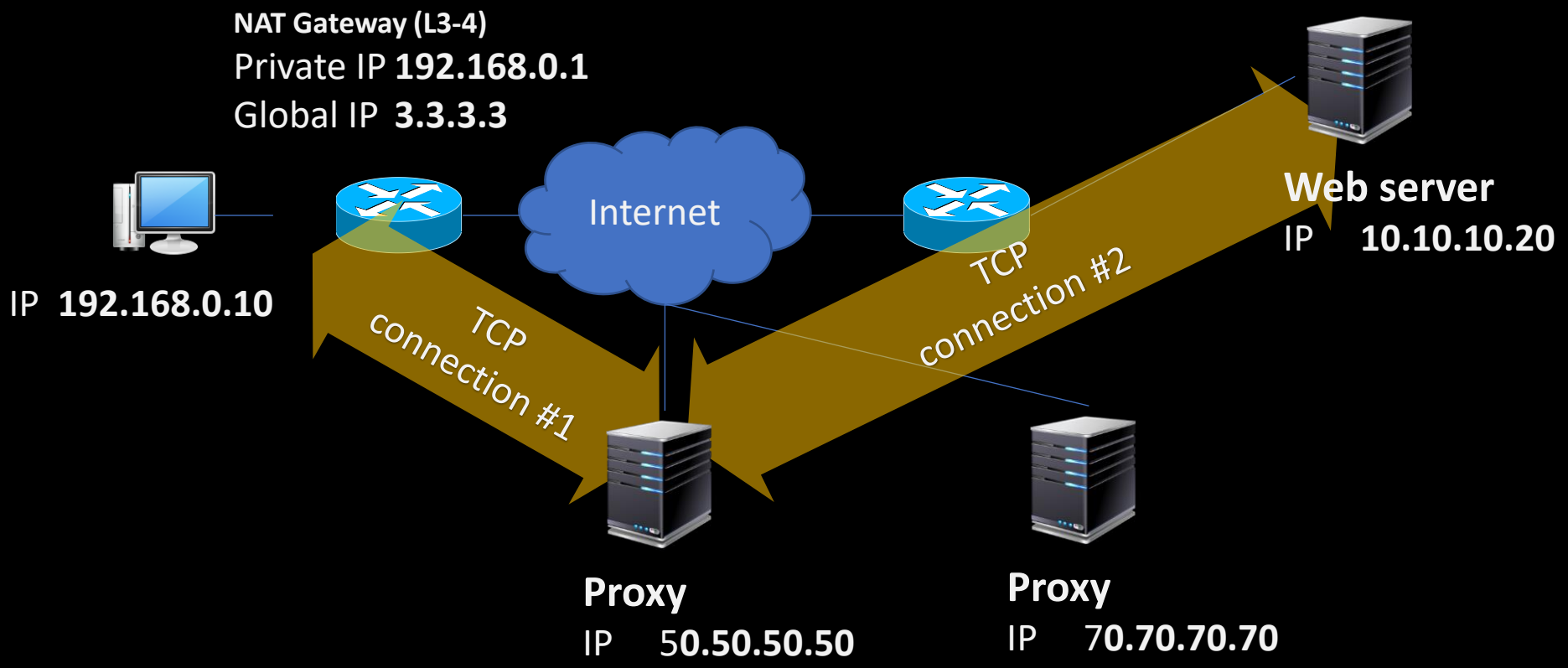
Out of path 구조



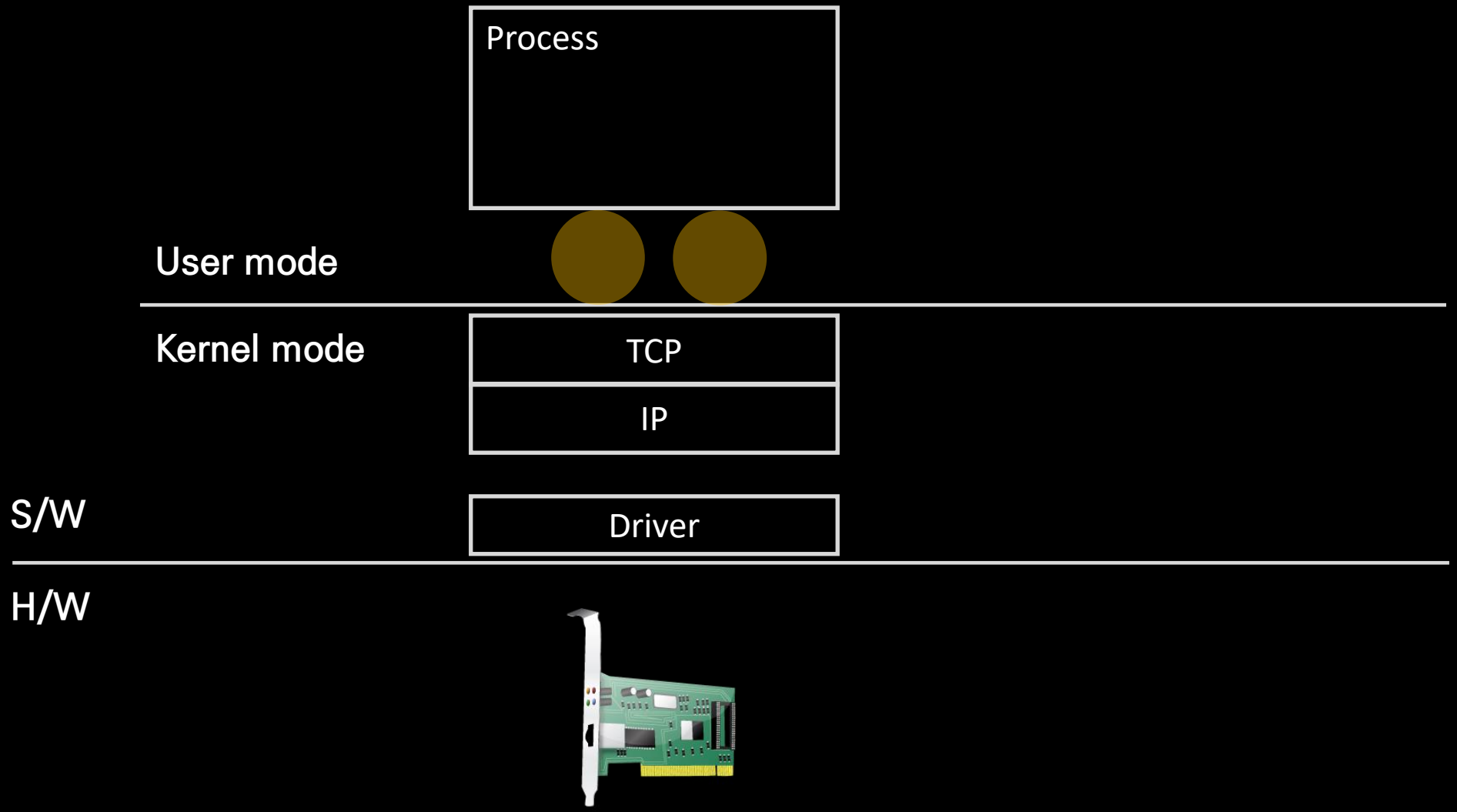
Out of path 구조



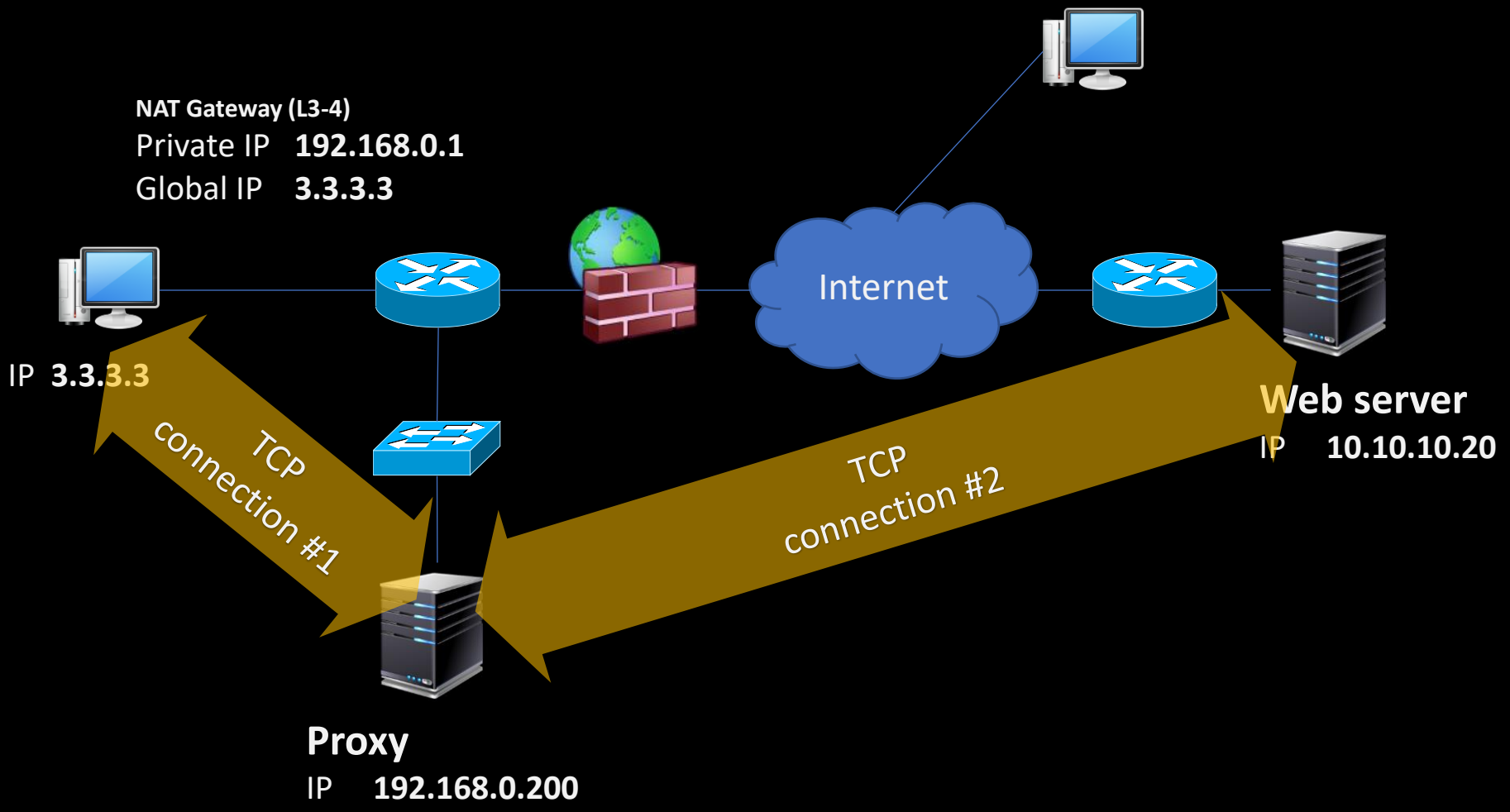
Proxy 구조 (우회)


NAT Gateway (L3-4)
Private IP 192.168.0.1
Global IP 3.3.3.3
Internet
IP 192.168.0.10
TCP connection #1
TCP connection #2
Web server
IP 10.10.10.20
Proxy
IP 50.50.50.50
Proxy
IP 70.70.70.70

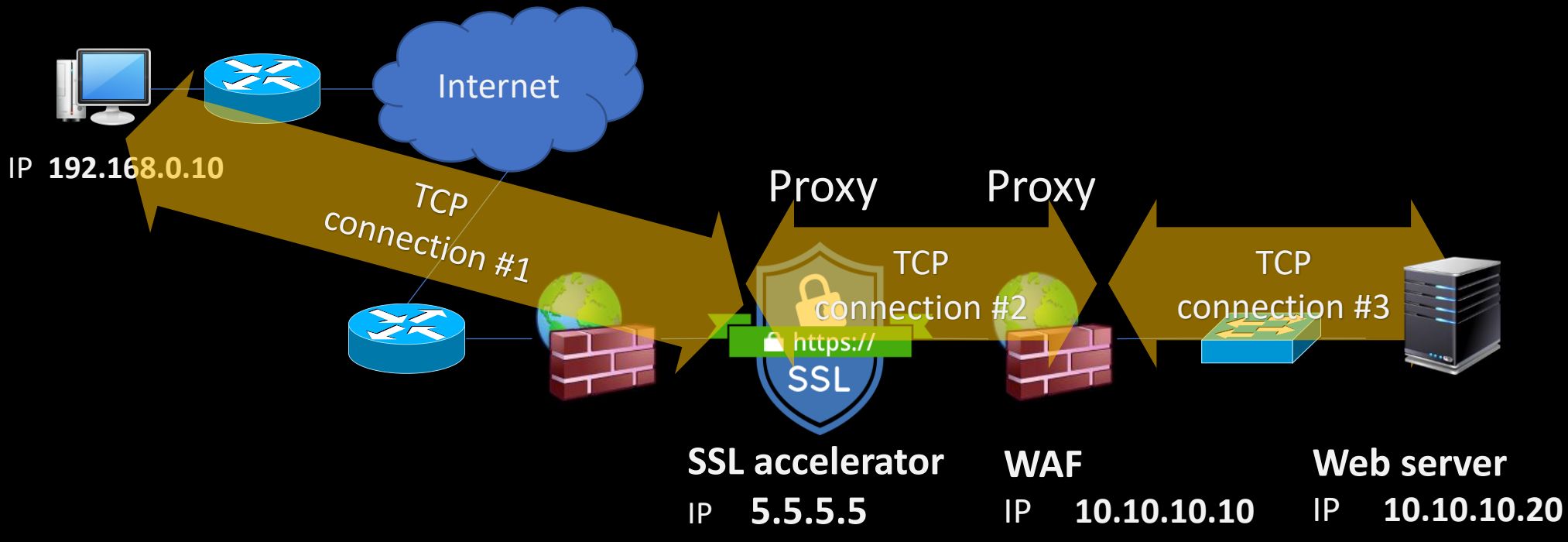
Proxy 구조



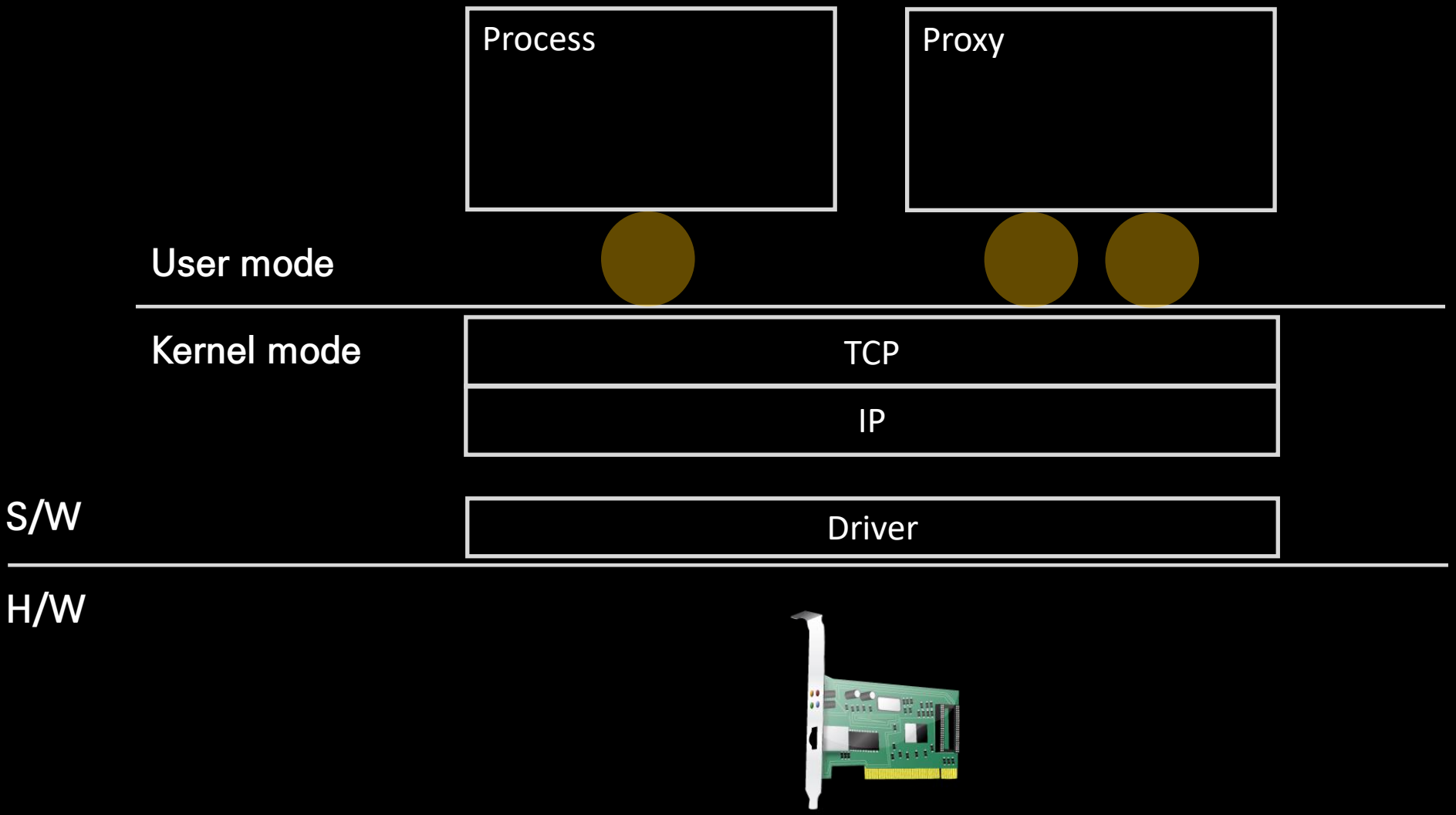
Proxy 구조 (보호와 감시)



Proxy 구조 (서버 보호)



Proxy 구조 (Fiddler)



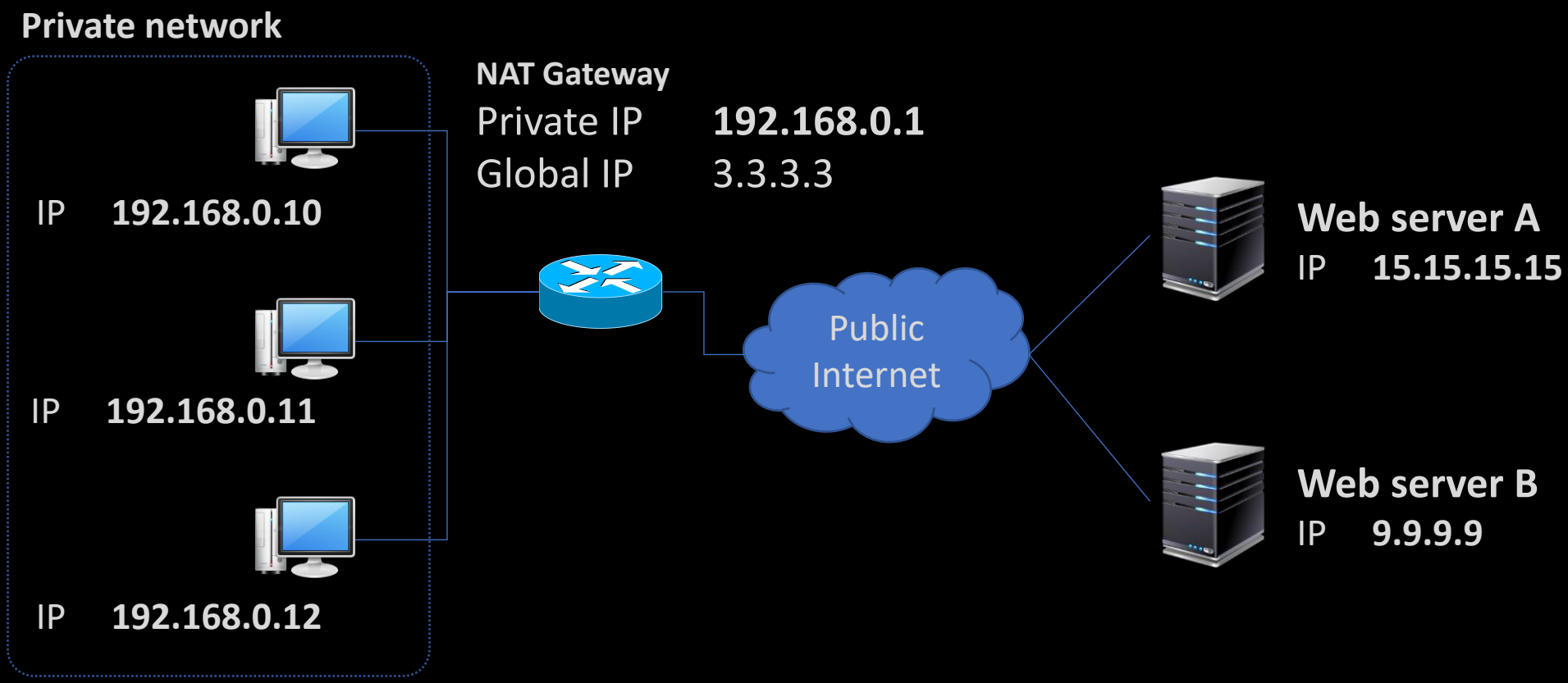
공유기 작동원리

- 일반적인 인터넷 공유기는 NAT(Network Address Translation) 기술이 적용된 장치이다.
- 보통 주소와 포트번호를 모두 제어한다.
- 인터넷 IP주소 부족 문제를 해결해준다.
- 패킷 필터링 방화벽과 비슷한 **보안성**을 제공한다.

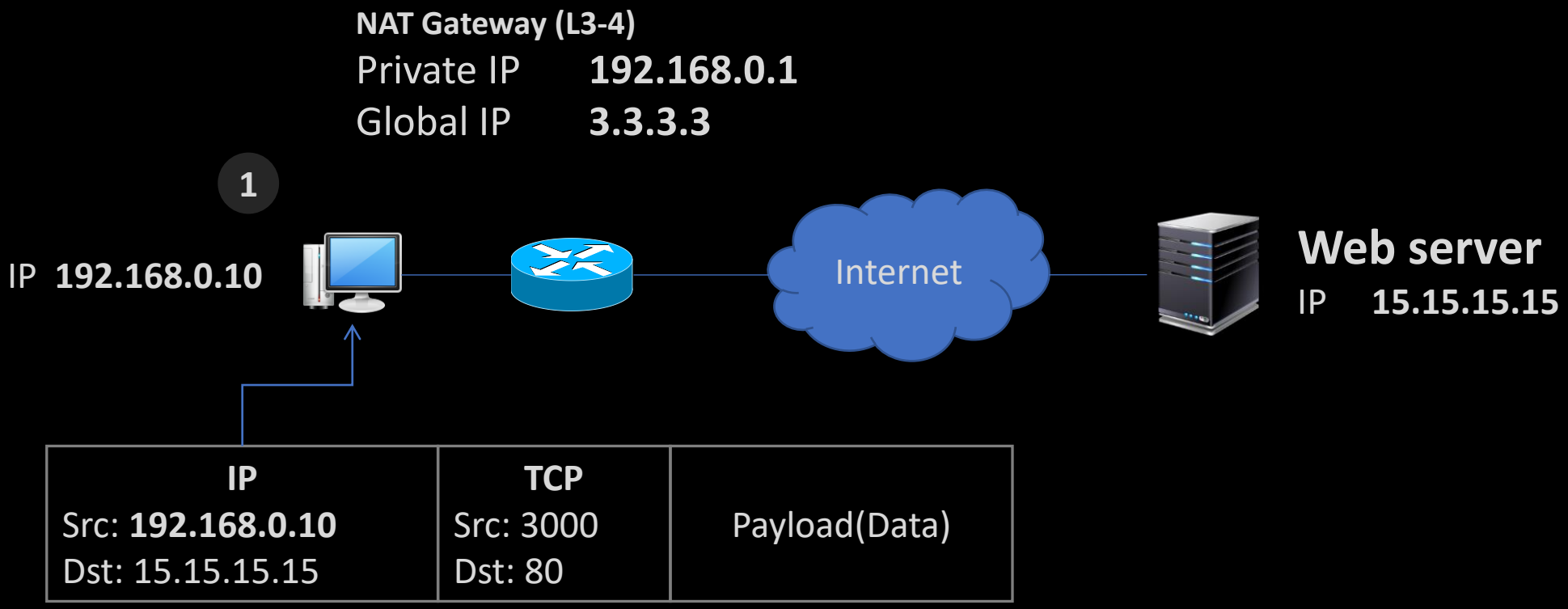
공유기 구조에 따른 분류

- **Cone NAT**
  - Host 단위로 외부포트 지정
  - Full Cone
  - Restricted Con
    - IP Address restricted
    - Port restricted
- **Symmetric NAT**
  - TCP 세션마다 외부 포트 지정

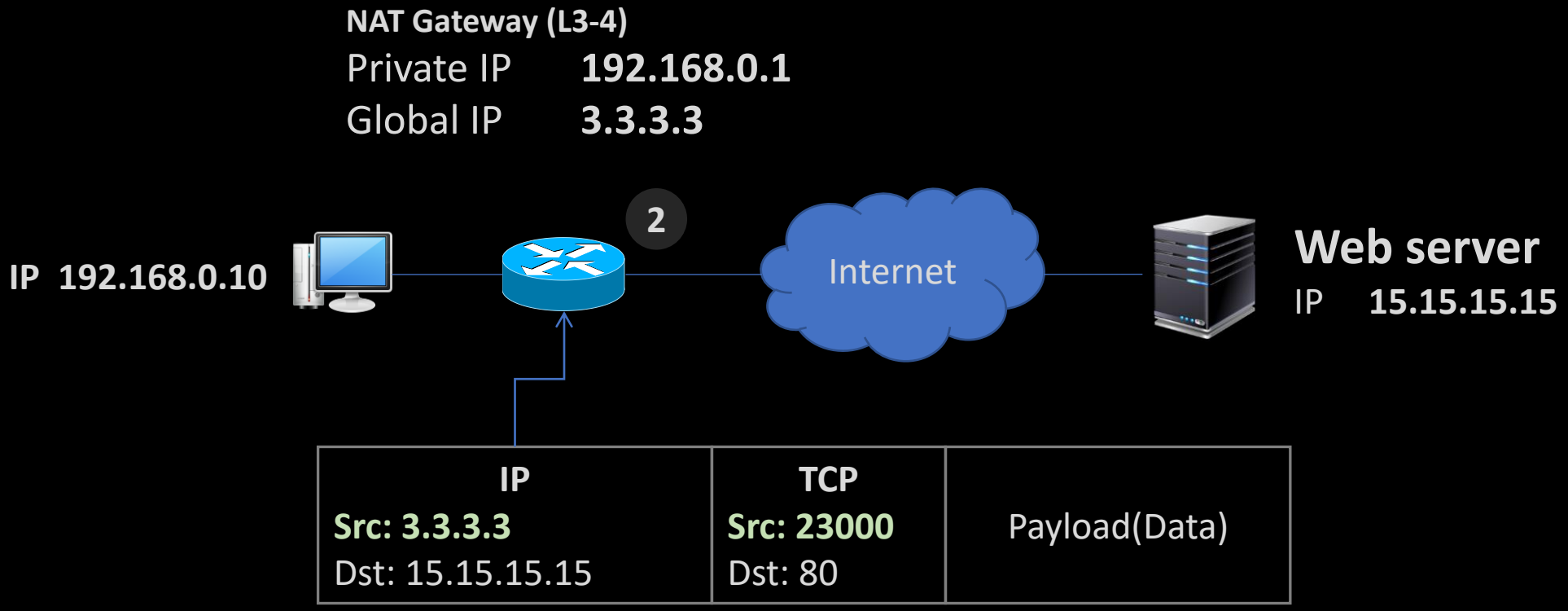
공유기 네트워크 구성 예


Private network
NAT Gateway
Private IP 192.168.0.1
Global IP 3.3.3.3
IP 192.168.0.10
IP 192.168.0.11
IP 192.168.0.12
Public Internet
Web server A
IP 15.15.15.15
Web server B
IP 9.9.9.9

Symmetric NAT #1

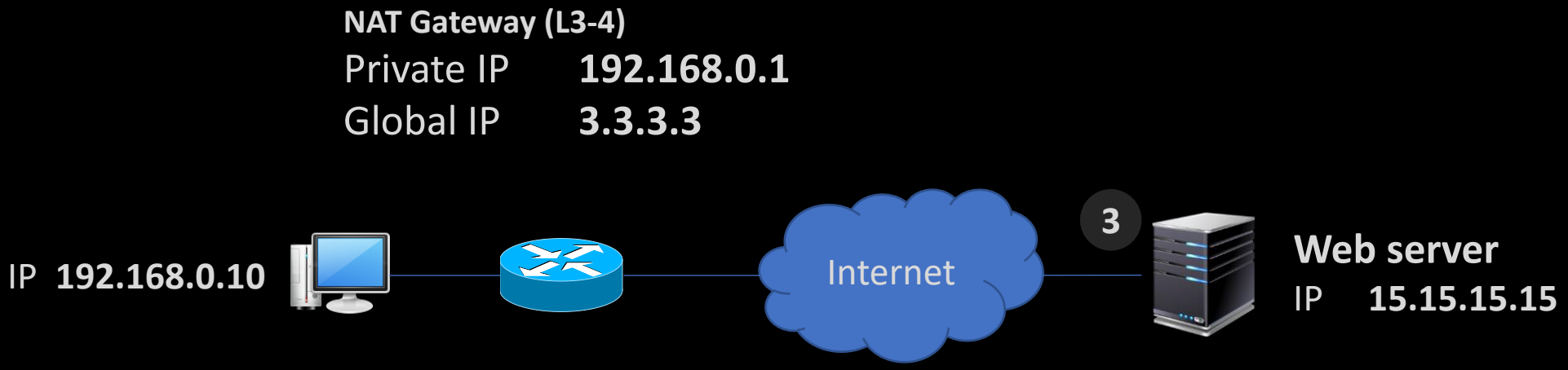


Symmetric NAT #2



출발지 IP주소가 **192.168.0.10에서 3.3.3.3**으로 변경.
출발지 포트가 **3000번에서 23000번**으로 변경.

Symmetric NAT #3

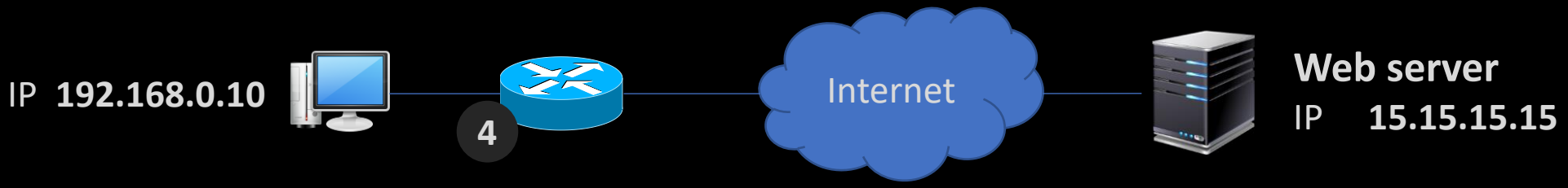


NAT table

Local IP	Local Port	External Port	Remote IP	Remote Port	Protocol
192.168.0.10	3000	23000	15.15.15.15	80	TCP
192.168.0.12	2500	23001	15.15.15.15	80	TCP
192.168.0.11	4000	23002	15.15.15.15	80	TCP

Symmetric NAT #4

NAT Gateway (L3-4)
Private IP **192.168.0.1**
Global IP **3.3.3.3**

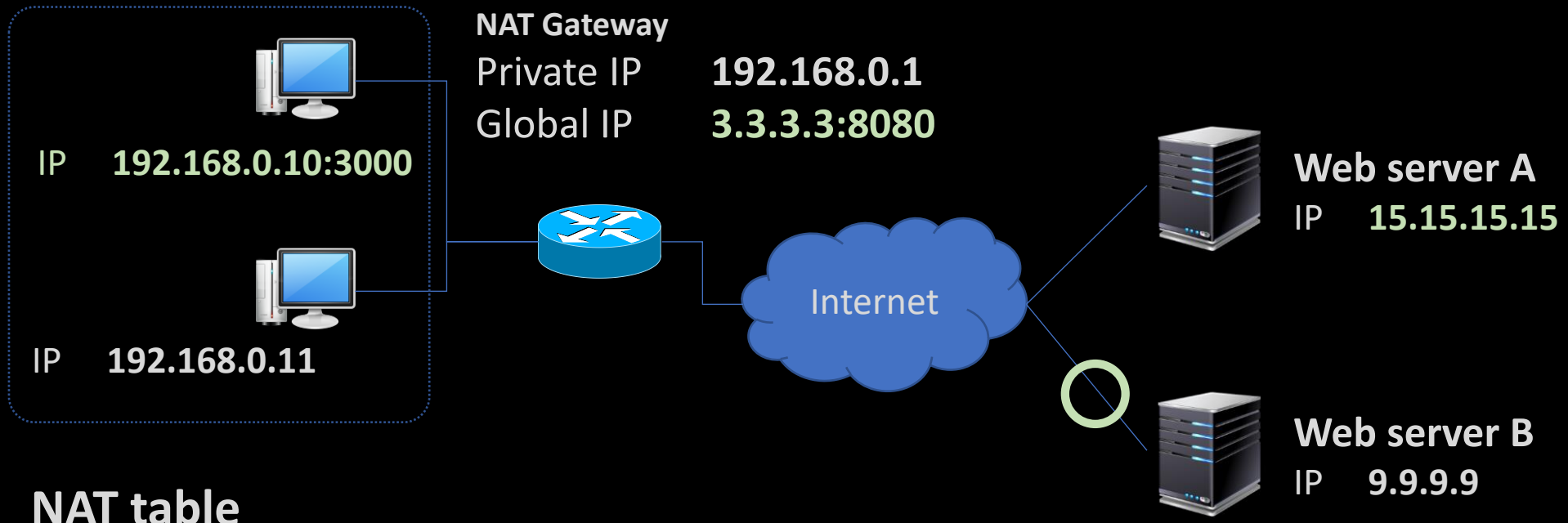


NAT table

Local IP	Local Port	External Port	Remote IP	Remote Port	Protocol
192.168.0.10	3000	23000	15.15.15.15	80	TCP
192.168.0.12	2500	23001	15.15.15.15	80	TCP
192.168.0.11	4000	23002	15.15.15.15	80	TCP

IP	TCP	
Src: 15.15.15.15 **Dst: 192.168.0.10**	Src: 80 **Dst: 3000**	Payload(Data)

Full Cone NAT

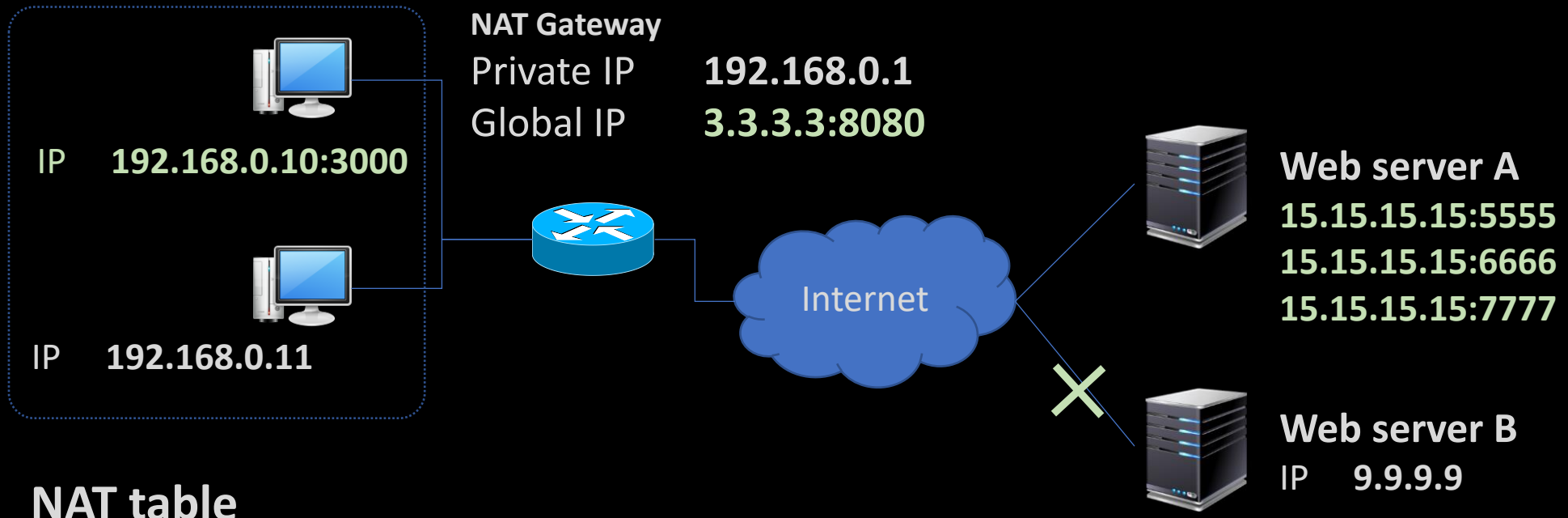


NAT table

Local IP	Local Port	External Port	Remote IP	Remote Port	Protocol
192.168.0.10	3000	8080	Any	Any	TCP

192.168.0.10 호스트를 3.3.3.3:8080번에 매핑하므로 3.3.3.3:8080으로 유입되는 모든 것을 192.168.0.10:3000으로 보낸다.

(IP) Restricted Cone NAT

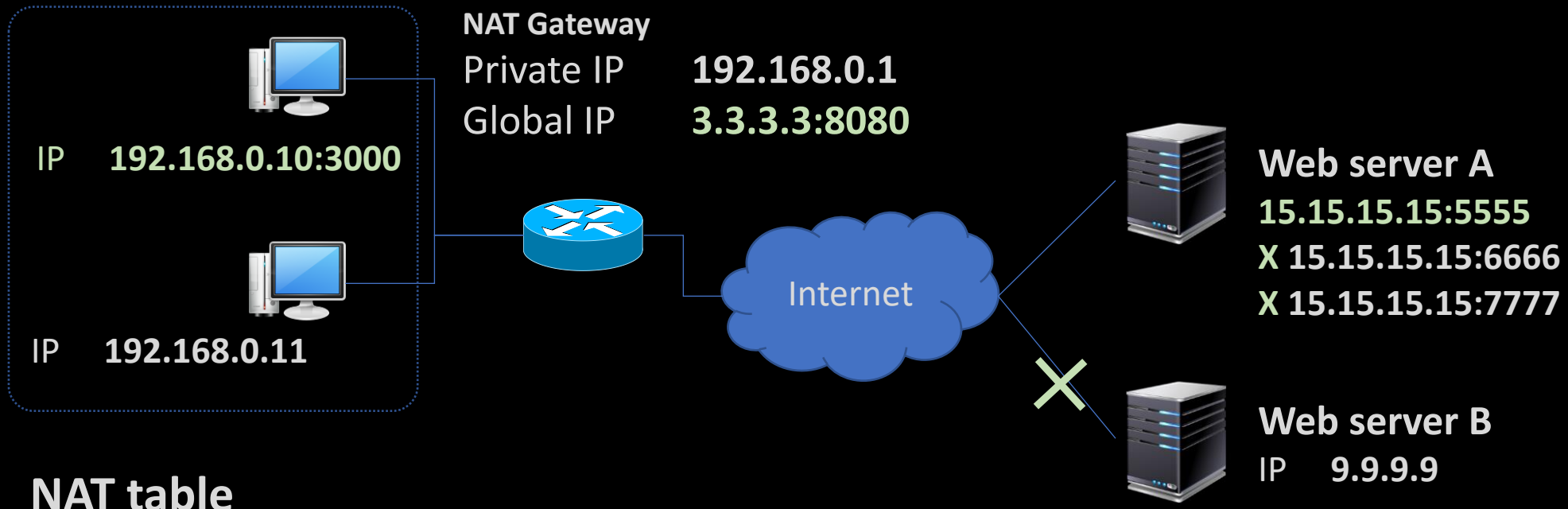


NAT table

Local IP	Local Port	External Port	Remote IP	Remote Port	Protocol
192.168.0.10	3000	8080	15.15.15.15	Any	TCP

192.168.0.10:8080과 15.15.15.15간의 통신으로 말미암아 15.15.15.15의 패킷 유입만 허용되고 나머지는 차단한다.

Port Restricted Cone NAT

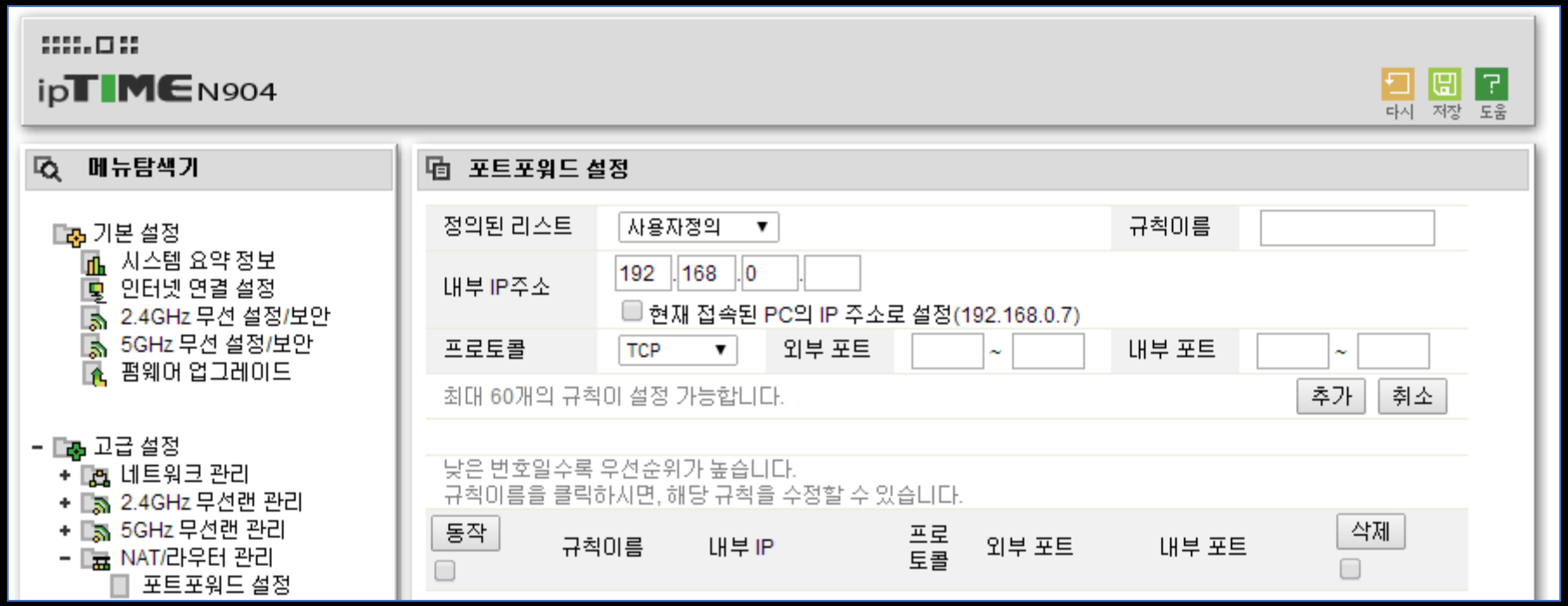


NAT table

Local IP	Local Port	External Port	Remote IP	Remote Port	Protocol
192.168.0.10	3000	8080	15.15.15.15	5555	TCP

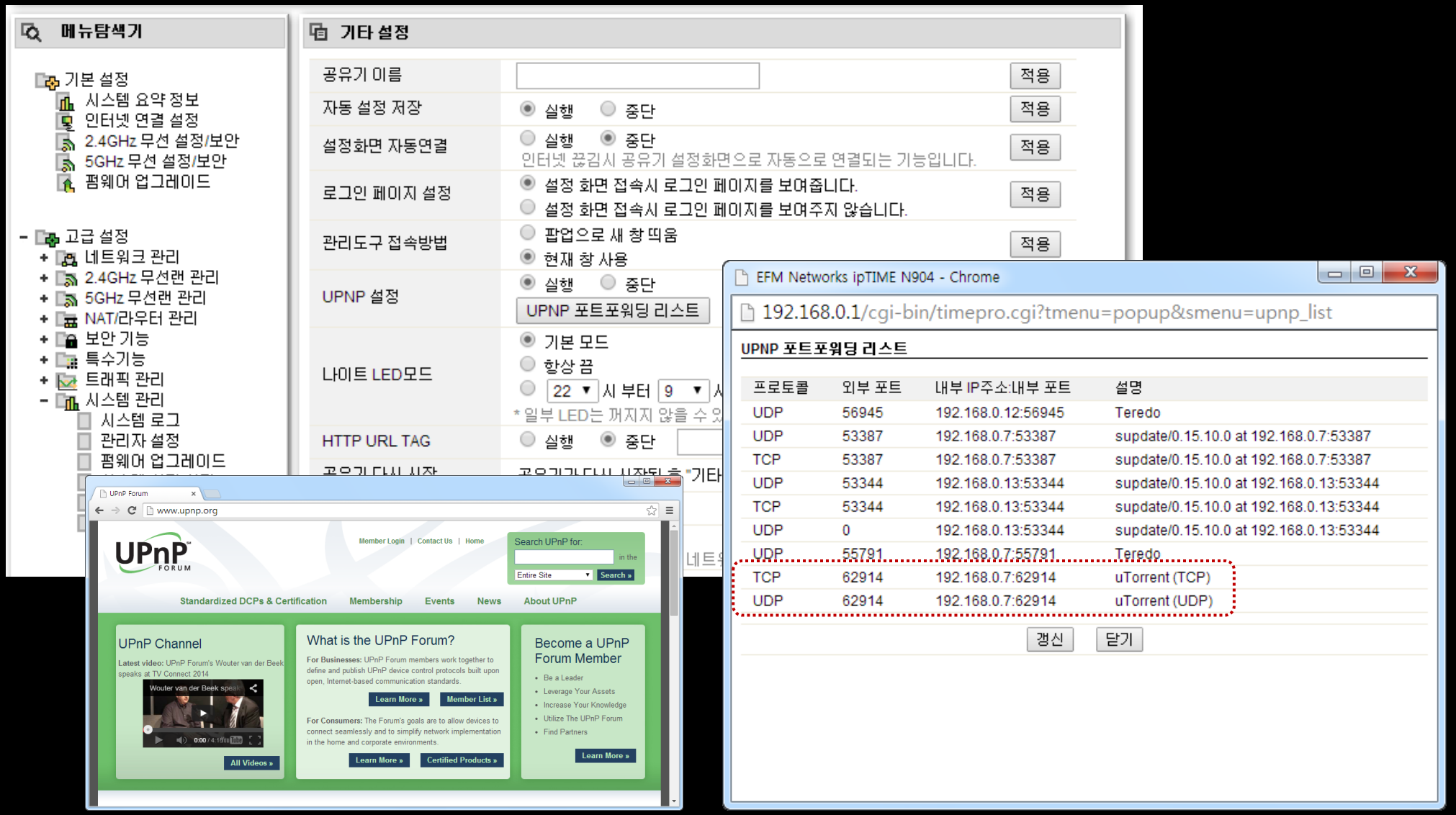
192.168.0.10:8080과 15.15.15.15:5555간의 통신만 허용하고 나머지는 모두 차단된다.

포트 포워딩

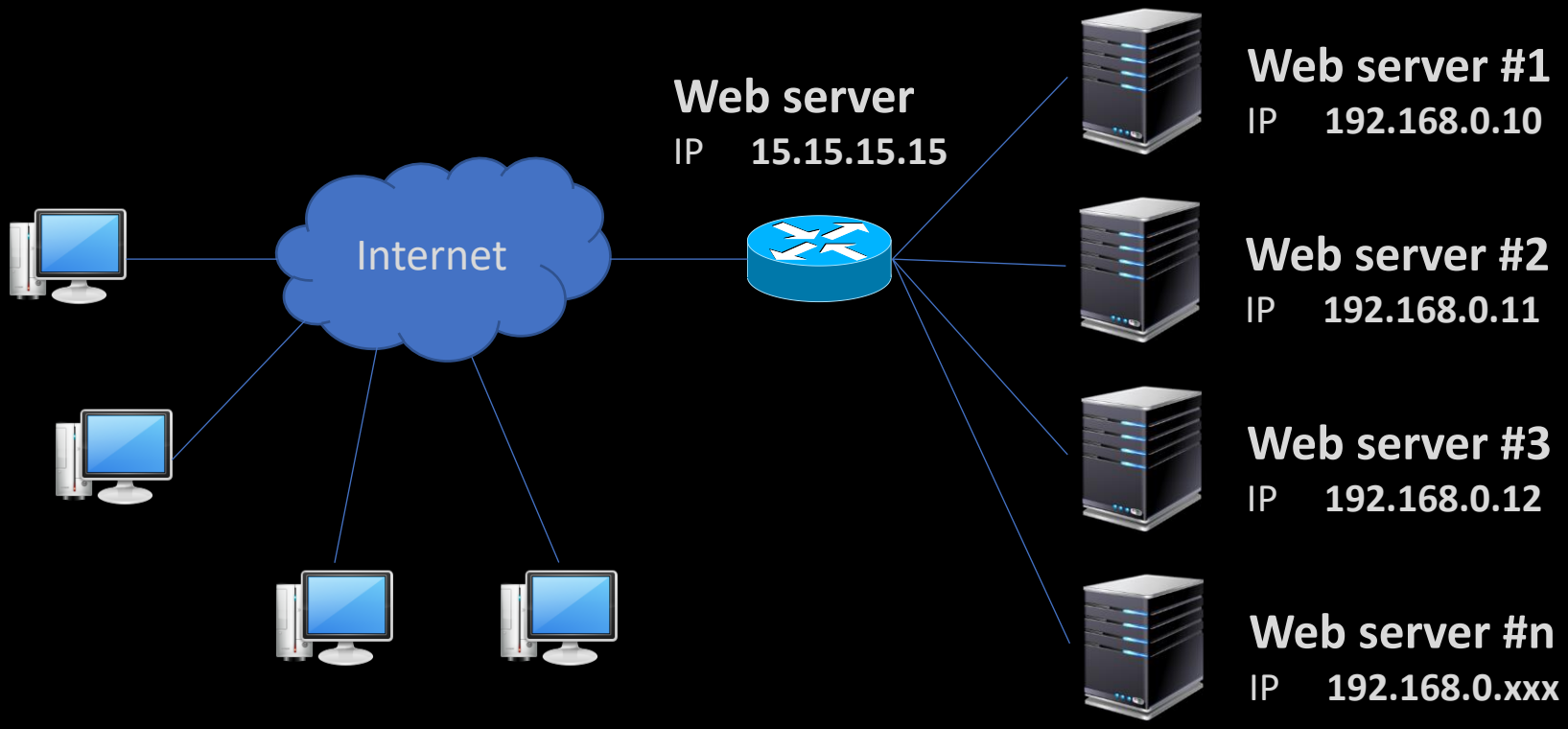


Local IP	Local Port	External Port	Remote Port	Protocol
192.168.0.12	80	80	Any	TCP

UPnP


메뉴탐색기
기본 설정
시스템 요약 정보
인터넷 연결 설정
2.4GHz 무선 설정/보안
5GHz 무선 설정/보안
펌웨어 업그레이드
고급 설정
네트워크 관리
2.4GHz 무선랜 관리
5GHz 무선랜 관리
NAT/라우터 관리
보안 기능
특수기능
트래픽 관리
시스템 관리
시스템 로그
관리자 설정
펌웨어 업그레이드
기타 설정
공유기 이름
적용
자동 설정 저장
실행
중단
적용
설정화면 자동연결
실행
중단
적용
인터넷 끊김시 공유기 설정화면으로 자동으로 연결되는 기능입니다.
로그인 페이지 설정
설정 화면 접속시 로그인 페이지를 보여줍니다.
설정 화면 접속시 로그인 페이지를 보여주지 않습니다.
적용
관리도구 접속방법
팝업으로 새 창 띄움
현재 창 사용
적용
UPNP 설정
실행
중단
UPNP 포트포워딩 리스트
나이트 LED모드
기본 모드
항상 끔
22 시 부터 9
HTTP URL TAG
실행
중단
EFM Networks ipTIME N904 - Chrome
192.168.0.1/cgi-bin/timepro.cgi?tmenu=popup&smenu=upnp_list
UPNP 포트포워딩 리스트
프로토콜 외부 포트 내부 IP주소:내부 포트 설명
UDP 56945 192.168.0.12:56945 Teredo
UDP 53387 192.168.0.7:53387 supdate/0.15.10.0 at 192.168.0.7:53387
TCP 53387 192.168.0.7:53387 supdate/0.15.10.0 at 192.168.0.7:53387
UDP 53344 192.168.0.13:53344 supdate/0.15.10.0 at 192.168.0.13:53344
TCP 53344 192.168.0.13:53344 supdate/0.15.10.0 at 192.168.0.13:53344
UDP 0 192.168.0.13:53344 supdate/0.15.10.0 at 192.168.0.13:53344
UDP 55791 192.168.0.7:55791 Teredo
TCP 62914 192.168.0.7:62914 uTorrent (TCP)
UDP 62914 192.168.0.7:62914 uTorrent (UDP)
갱신
닫기
UPnP Forum
www.upnp.org
UPnP FORUM
Member Login | Contact Us | Home
Search UPnP for:
Entire Site
Search »
Standardized DCPs & Certification
Membership
Events
News
About UPnP
UPnP Channel
Latest video: UPnP Forum's Wouter van der Beek speaks at TV Connect 2014
All Videos »
What is the UPnP Forum?
For Businesses: UPnP Forum members work together to define and publish UPnP device control protocols built upon open, Internet-based communication standards.
Learn More »
Member List »
For Consumers: The Forum's goals are to allow devices to connect seamlessly and to simplify network implementation in the home and corporate environments.
Learn More »
Certified Products »
Become a UPnP Forum Member
Be a Leader
Leverage Your Assets
Increase Your Knowledge
Utilize The UPnP Forum
Find Partners
Learn More »

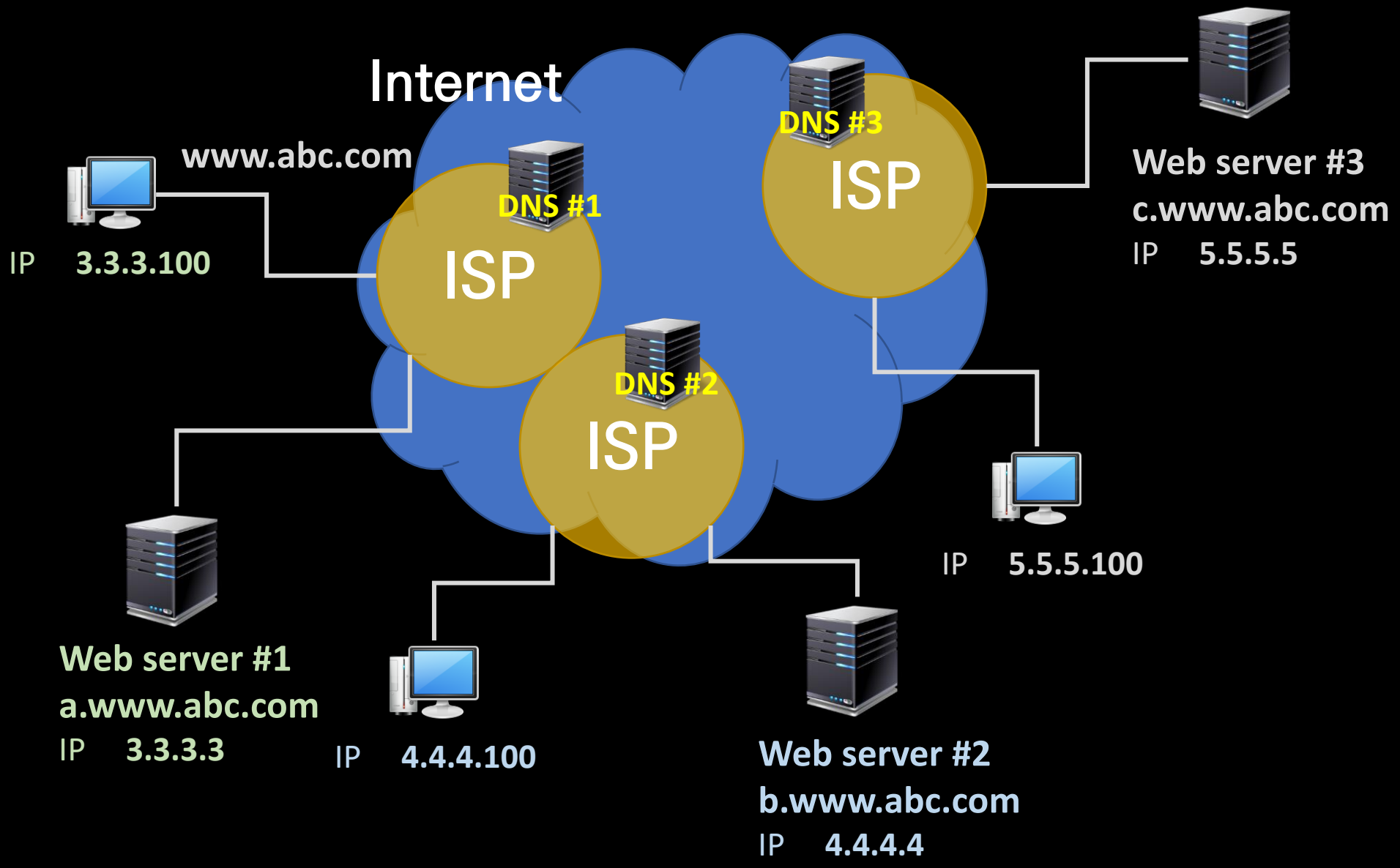
L4 부하분산


Web server
IP 15.15.15.15
Internet
Web server #1
IP 192.168.0.10
Web server #2
IP 192.168.0.11
Web server #3
IP 192.168.0.12
Web server #n
IP 192.168.0.xxx

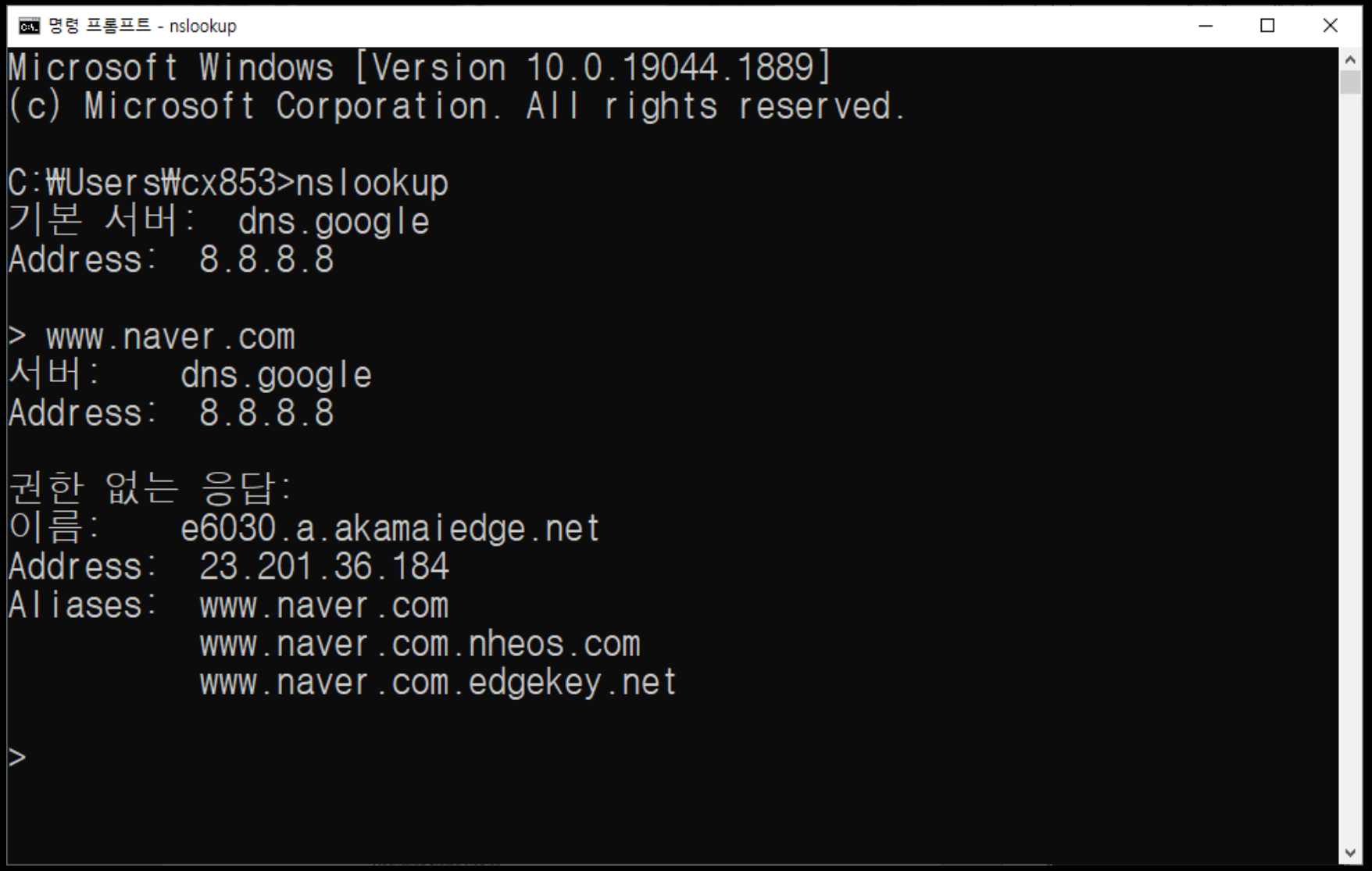
GSLB

- Global Server Load Balancing
- **DNS 체계를 활용**하는 구조
- 각 서버들의 콘텐츠는 **CDN을 활용**해 동기화 하는 것이 대부분
- 부하 상태, Health check 결과, **클라이언트의 지리적 위치** 등을 고려한다.

GSLB


Internet
www.abc.com
IP 3.3.3.100
DNS #1
ISP
DNS #3
ISP
Web server #3
c.www.abc.com
IP 5.5.5.5
DNS #2
ISP
IP 5.5.5.100
Web server #1
a.www.abc.com
IP 3.3.3.3
IP 4.4.4.100
Web server #2
b.www.abc.com
IP 4.4.4.4

GSLB


명령 프롬프트 - nslookup
Microsoft Windows [Version 10.0.19044.1889]
(c) Microsoft Corporation. All rights reserved.
C:₩Users₩cx853>nslookup
기본 서버: dns.google
Address: 8.8.8.8
> www.naver.com
서버: dns.google
Address: 8.8.8.8
권한 없는 응답:
이름: e6030.a.akamaiedge.net
Address: 23.201.36.184
Aliases: www.naver.com
www.naver.com.nheos.com
www.naver.com.edgekey.net
>

VPN 기술

- 보안 서비스 기술
  - 내부 사설망을 외부로부터 스스로 보호하고, 사용자 인증을 통한 접근통제가 가능해야 한다.
- 데이터 인증 및 암호화 기술
  - 사설망 간의 Traffic을 무결성과 기밀성을 유지 하기 위해서, 모든 Traffic에 인증 메커니즘을 적용하거나, 정보 유출의 방지를 위해서 암호화 할 수 있어야 한다.
- 터널링 기술
  - 기존의 공개 네트워크에서 가상의 사설 망을 구성하기 위해서, 기존 네트워크에서 정보 이동이 가능하도록 정보를 캡슐화 하고, 다시 풀어 내어 논리적으로 두 네트워크를 연결하는 기술(망연계)이다.

IPSec

- IPSec은 네트워크 계층에 보안 서비스를 제공하며 패킷 단위에 적용된다. IPSec은 현재 사용 중인 IPv4, IPv6를 모두 지원한다. IPSec은 GtoG VPN 구현을 위해서 현재 가장 많이 사용되고 있는 방식으로 다음과 같은 서비스를 제공한다.
    - Access control
    - Connectionless integrity
    - Data original authentication
    - Protection against replay
    - Confidentiality
- IPSec은 IP수준(L3) 보안을 제공한다. 따라서 응용 프로그램에 대한 의존성이 없고 IP기반 통신을 모두 보호할 수 있다는 장점이 있다.
- IPSec VPN은 대부분 GtoG(망대망) VPN에 주로 활용한다.

IPSec Protocol

- ISAKMP
  - Internet Security Association Key Management Protocol은 보안 협상 및 암호화 키들을 관리하는 메커니즘을 제공한다.

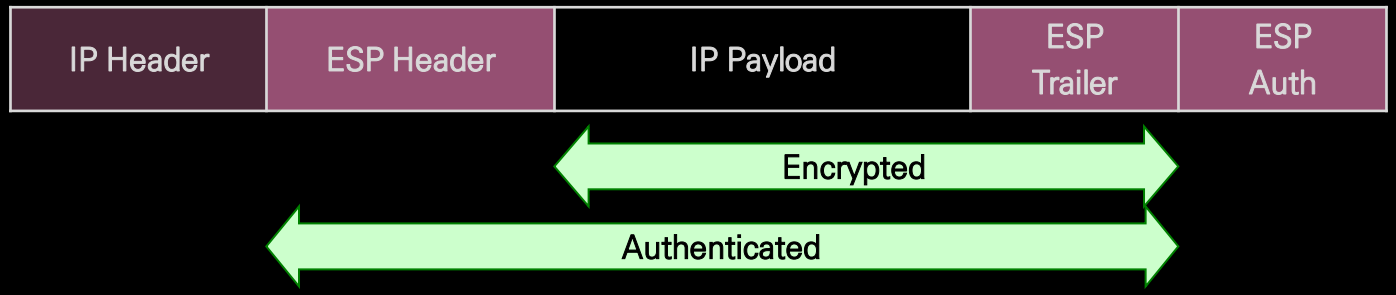
- IP AH (Authentication Header)
  - AH는 데이터의 원본 인증 및 무결성 재연공격 방지 기능을 제공한다.

- IP ESP (Encapsulation Security Payload)
  - ESP는 데이터의 기밀성, 원본 인증 및 기밀성 및 재연공격 방지 기능을 제공한다.

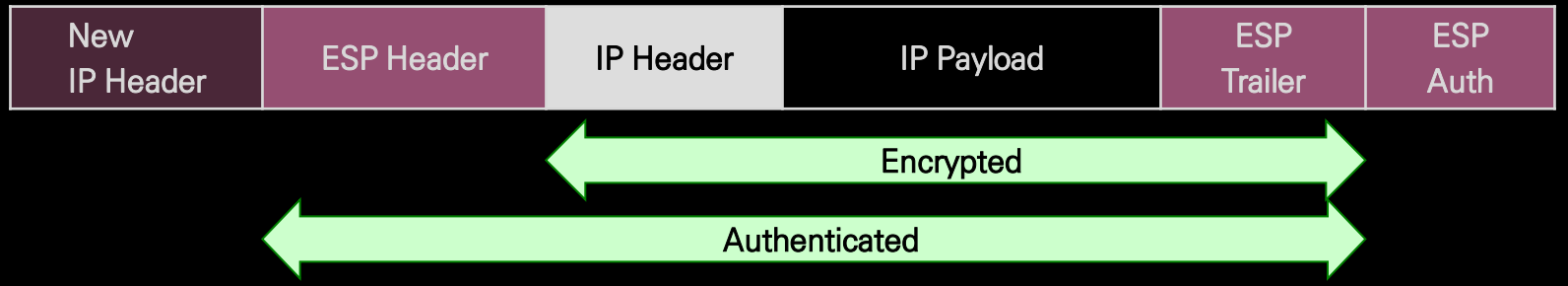
VPN Tunneling

Original Datagram

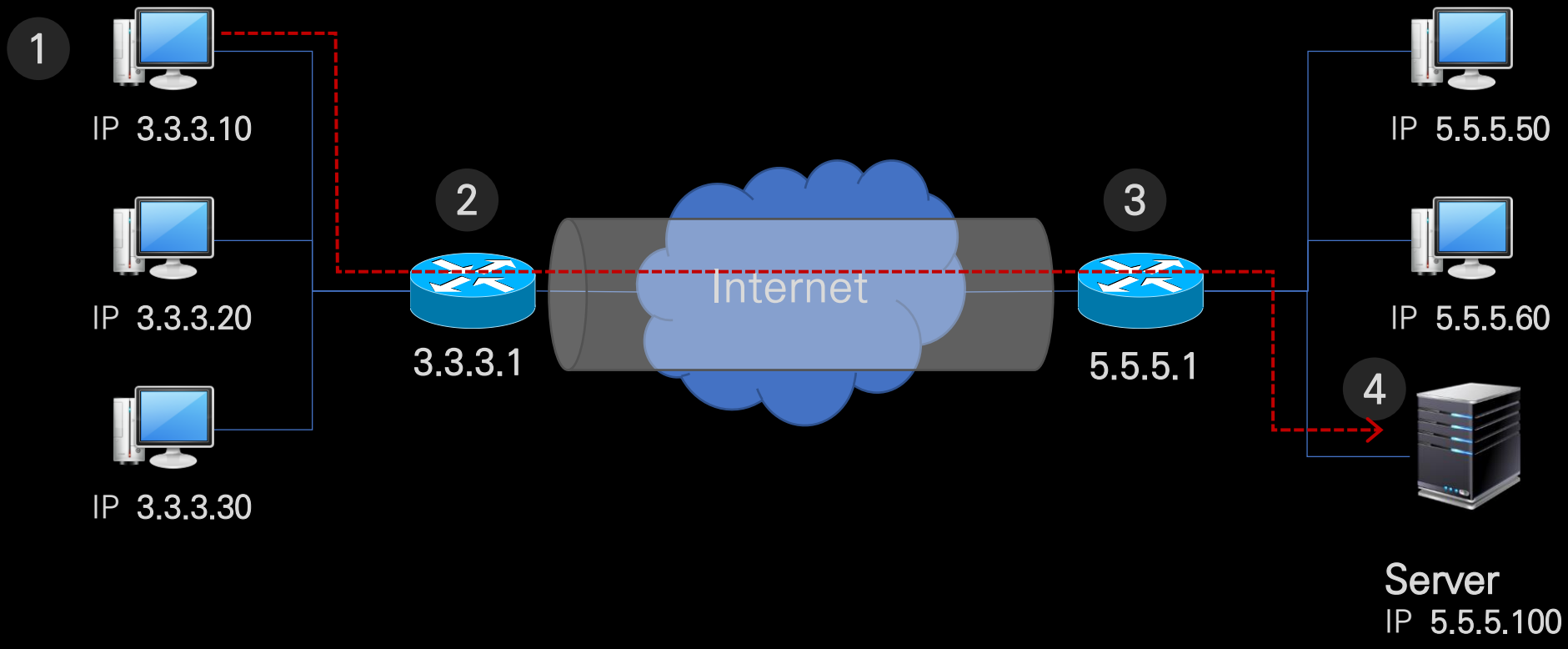
Original Datagram protected by ESP–Transport mode



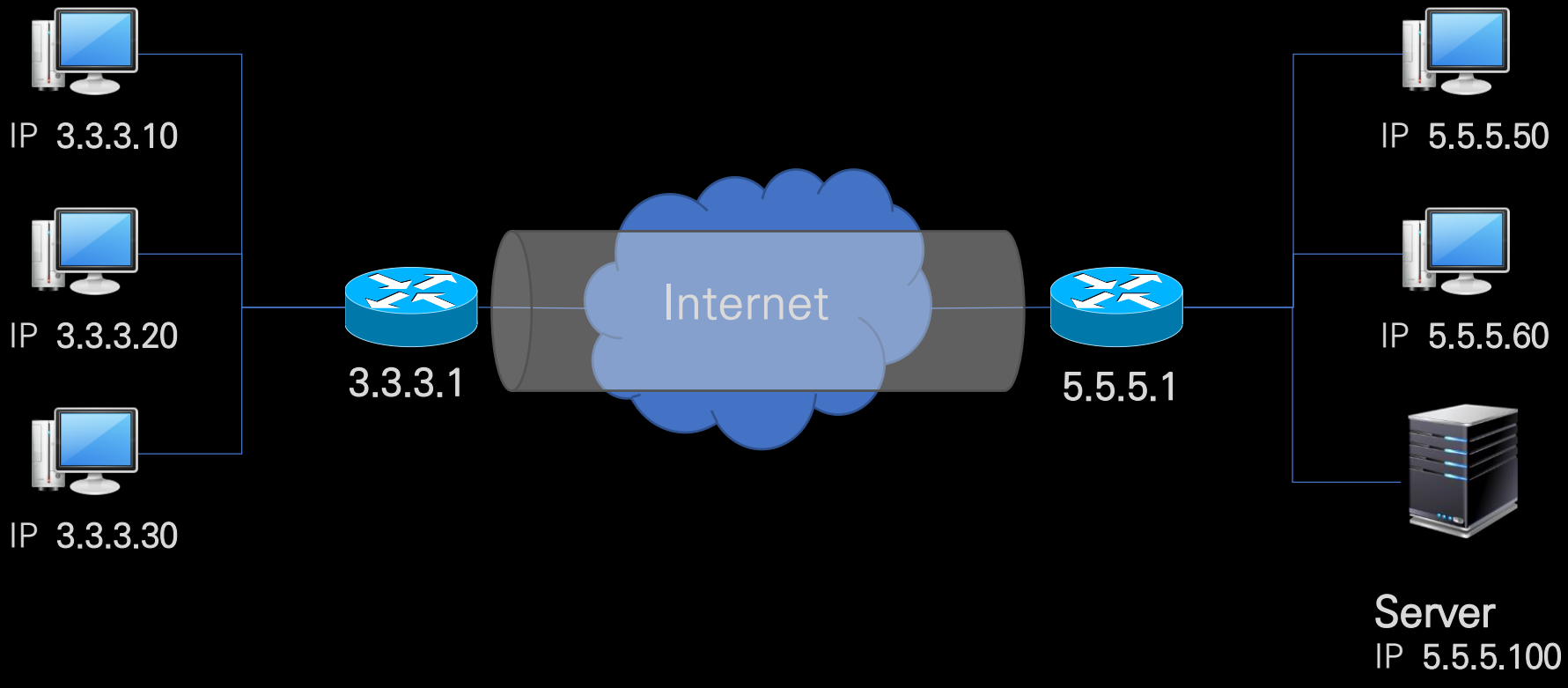
Original Datagram protected by ESP–tunnel



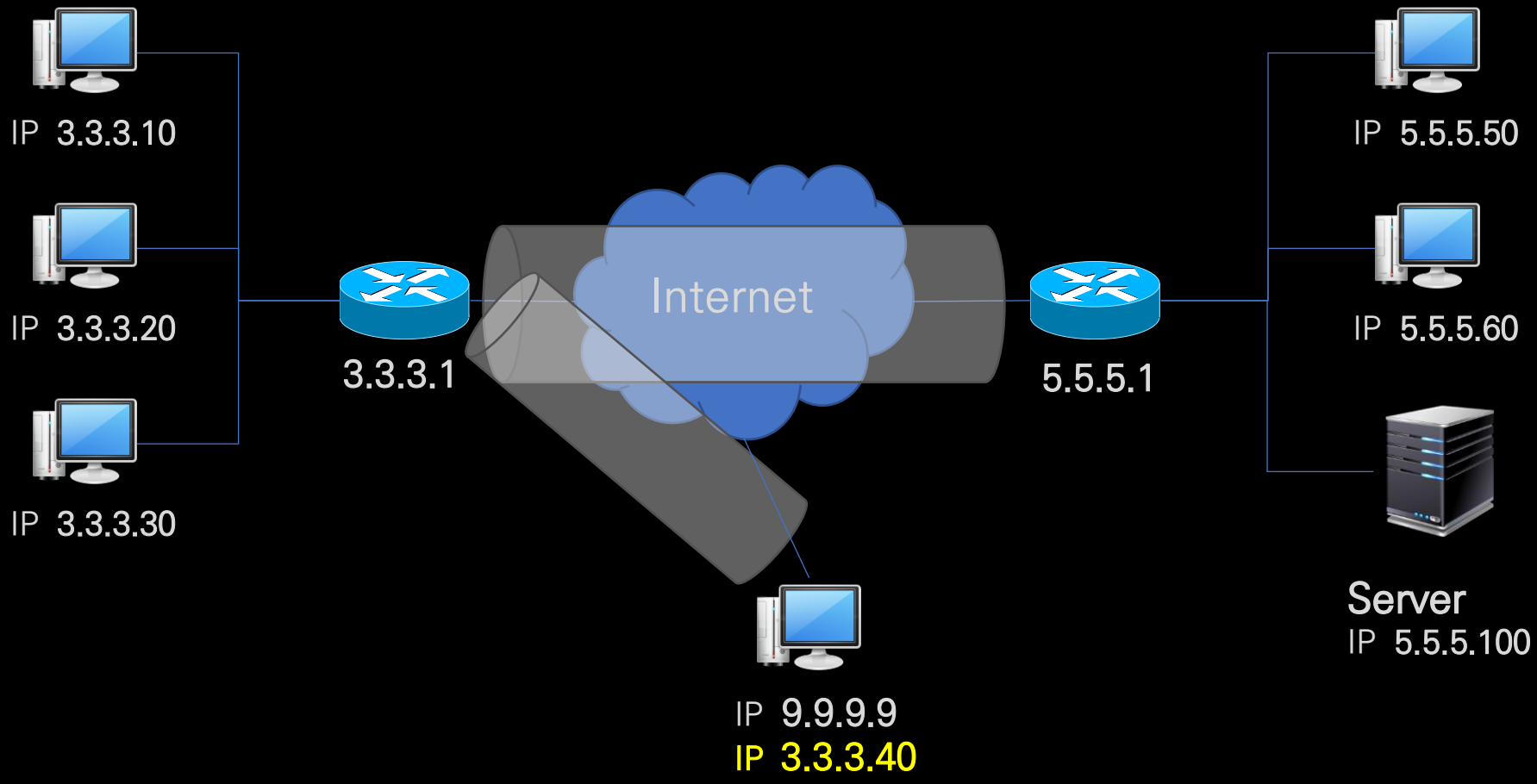
VPN GtoG


1
IP 3.3.3.10
IP 3.3.3.20
IP 3.3.3.30
2
3.3.3.1
Internet
3
5.5.5.1
IP 5.5.5.50
IP 5.5.5.60
4
Server
IP 5.5.5.100

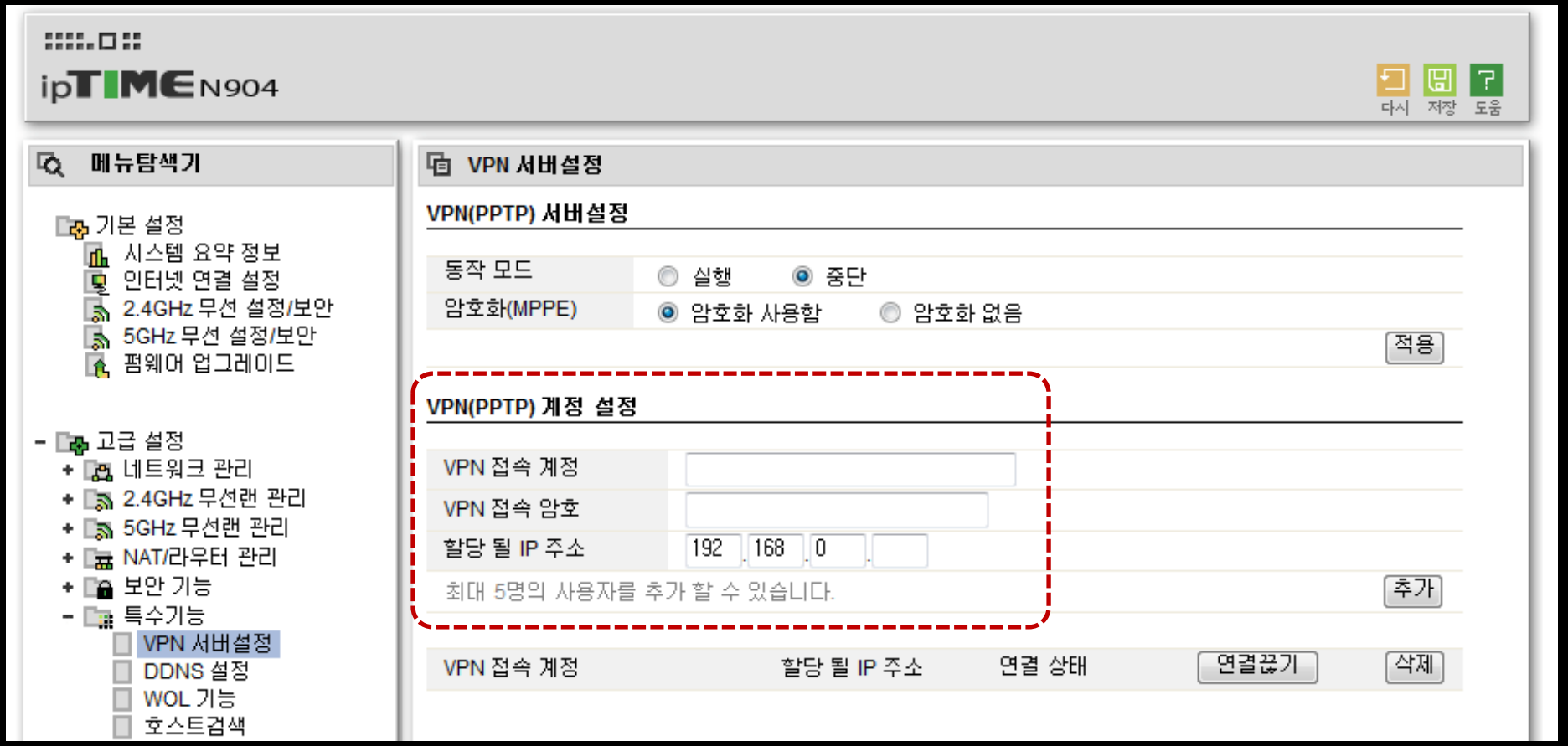
VPN GtoG


IP 3.3.3.10
IP 3.3.3.20
IP 3.3.3.30
3.3.3.1
Internet
5.5.5.1
IP 5.5.5.50
IP 5.5.5.60
Server
IP 5.5.5.100

VPN GtoE


IP 3.3.3.10
IP 3.3.3.20
IP 3.3.3.30
3.3.3.1
Internet
5.5.5.1
IP 5.5.5.50
IP 5.5.5.60
Server
IP 5.5.5.100
IP 9.9.9.9
IP 3.3.3.40

VPN 악용

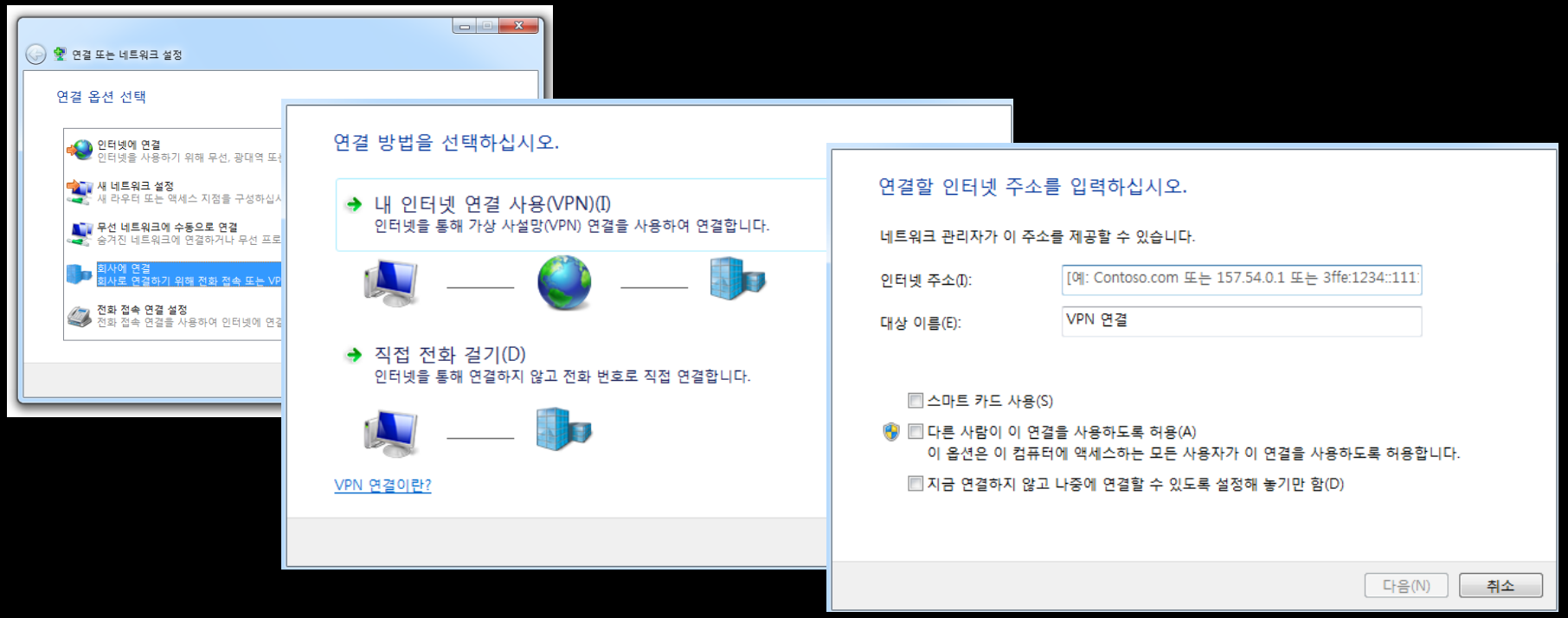

ipTIME N904
다시
저장
도움
메뉴탐색기
기본 설정
시스템 요약 정보
인터넷 연결 설정
2.4GHz 무선 설정/보안
5GHz 무선 설정/보안
펌웨어 업그레이드
고급 설정
네트워크 관리
2.4GHz 무선랜 관리
5GHz 무선랜 관리
NAT/라우터 관리
보안 기능
특수기능
VPN 서버설정
DDNS 설정
WOL 기능
호스트검색
VPN 서버설정
VPN(PPTP) 서버설정
동작 모드
실행
중단
암호화(MPPE)
암호화 사용함
암호화 없음
적용
VPN(PPTP) 계정 설정
VPN 접속 계정
VPN 접속 암호
할당 될 IP 주소
192
168
0
최대 5명의 사용자를 추가 할 수 있습니다.
추가
VPN 접속 계정
할당 될 IP 주소
연결 상태
연결끊기
삭제

Point-to-Point Protocol

1. PPP 링크 설정
2. 물리적인 연결을 설정함
3. 사용자 인증
4. Call back 제어 단계(Option)
5. Call back이 구현되어 있다면, 인증서버가 사용자 인증 후 연결을 종료하고 다시 클라이언트에게 연결함
6. 네트워크 제어 프로토콜 호출 단계
7. 사용자에게 동적으로 주소 할당

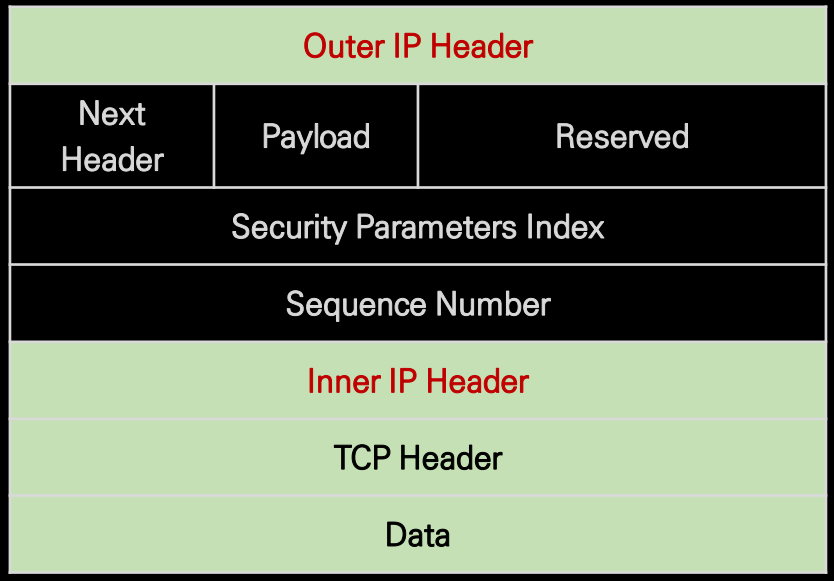
Point-to-Point Tunneling Protocol

- MS사가 개발한 것으로 IP, IPX, NetBEUI 를 암호화하고 IP 헤더로 캡슐화 한다.

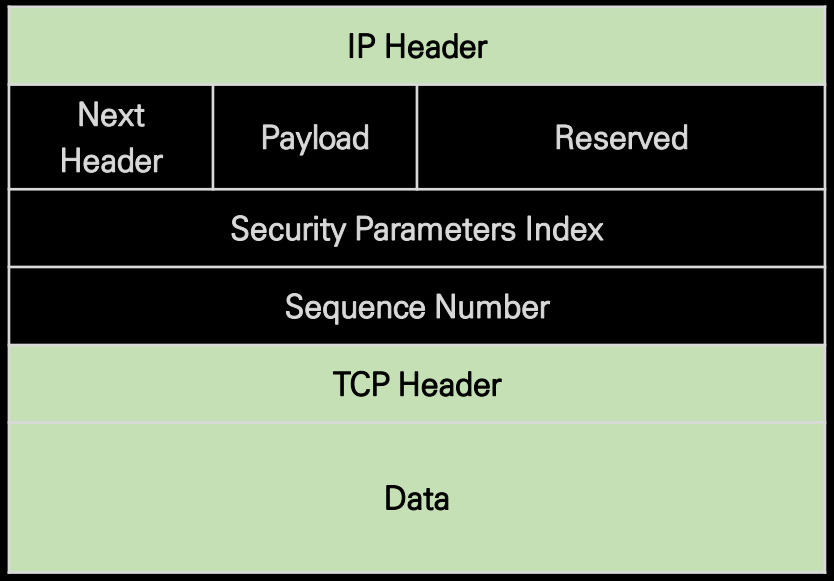


AH Header

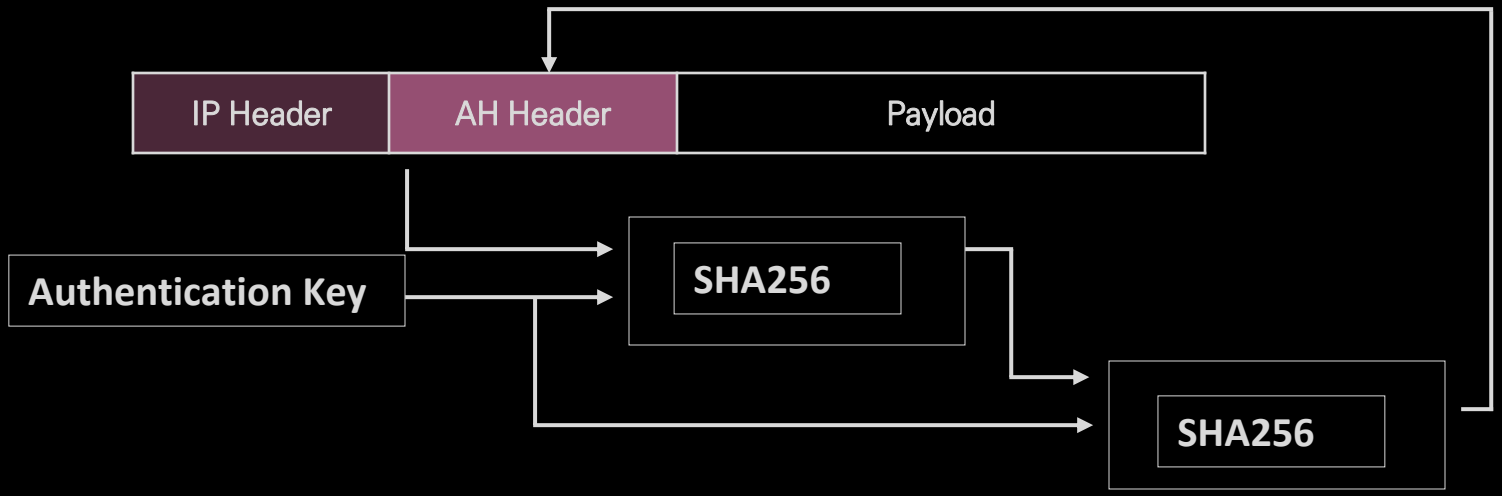
AH in tunnel mode



AH in transport mode



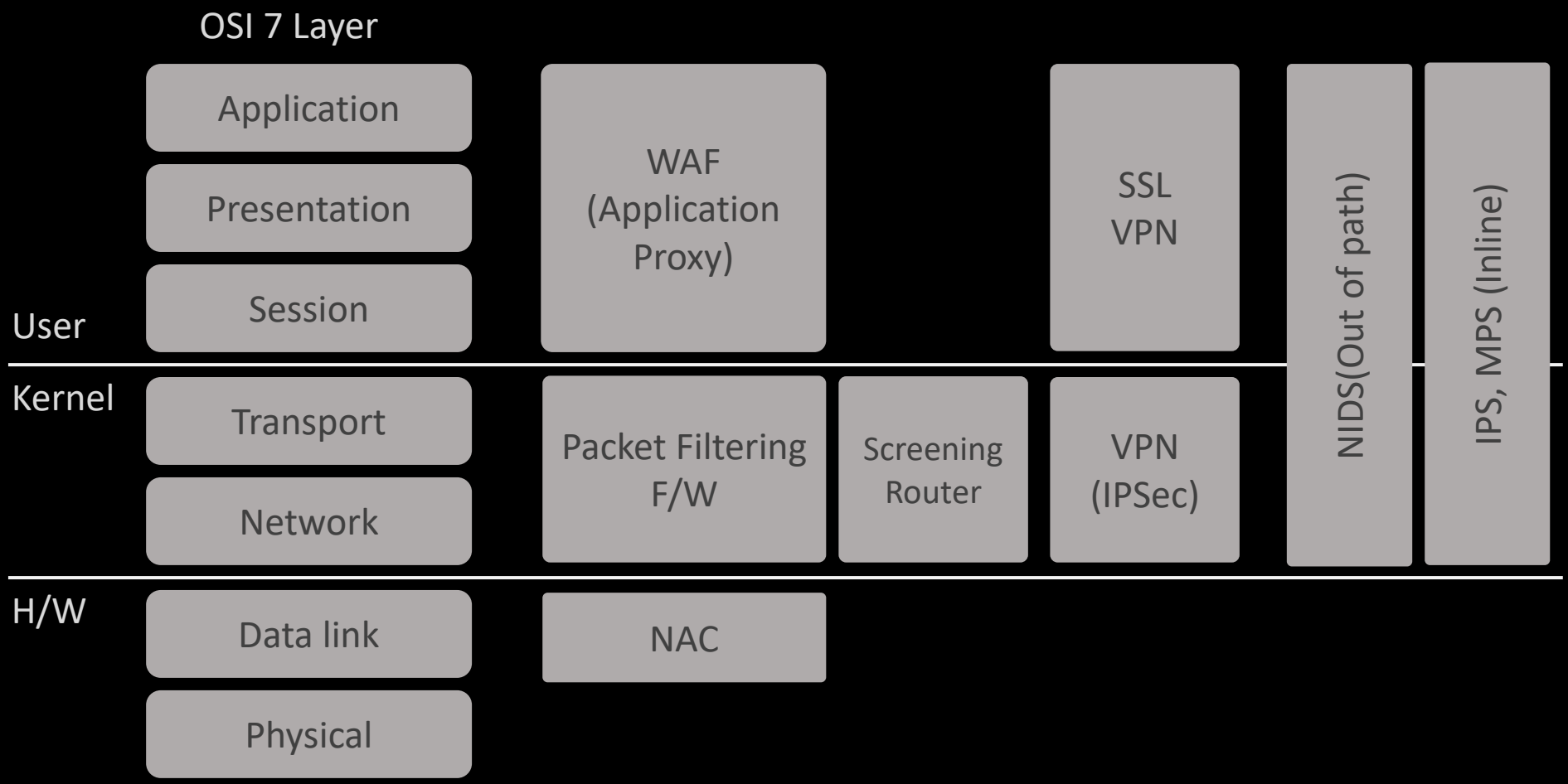
패킷 무결성 검사


IP Header
AH Header
Payload
Authentication Key
SHA256
SHA256

네트워크 보안 솔루션 종류

- PC방화벽
- NAC
- 방화벽, IPS, NIDS
- UTM
- VPN, SSL VPN,
- 망분리, 망연계

네트워크 보안 솔루션 종류별 대응 계층



NIDS 침입탐지 규칙

```
alert TCP any any -> any 80 (
        msg: “TestAttack”;
        content: “Test”;
        sid:12345;
        rev:1;
)
```

NIDS 침입탐지 규칙

```
alert tcp any any -> any 80 (
    msg: “Web Test”;
    uricontent: “test/”; nocase;
)
```

Name	Descriptions
Action	alert (경고)
Protocol	TCP
Source	룰 적용대상 출발지(공격자) IP주소 및 포트는 ‘전체’
Direction	전체 네트워크
Destination	룰 적용대상 홈 네트워크 IP는 전체, 포트는 80번 한정
Message	“Web Test”
Pattern	URI에 “test/”라는 문자열이 있는지 검사. 단, 대/소문자는 고려하지 않는다.

NIDS 침입탐지 규칙

```
alert tcp any any -> 192.168.1.0/24 111 (
    msg:"mountd access";
    content:"|00 01 86 a5|";
)
```

Name	Descriptions
Action	alert (경고)
Protocol	TCP
Source	룰 적용대상 출발지(공격자) IP주소 및 포트는 '전체'
Direction	특정 네트워크 Inbound
Destination	192.168.1.x 네트워크 111 포트에 대한 접근
Message	"mountd access"
Pattern	TCP payload에서 Hexa 스트링 0x00, 0x01, 0x86, 0xA5 패턴을 찾는다.