

온프레미스 네트워크

Master SEO

topasvga@naver.com



네트워크 엔지니어

인프라 엔지니어

클라우드 엔지니어

전체 목차

사전 질문

SubnetMask?

라우팅?

학습목표 : 네트워크 이해



온프레미스 (IDC)

온프레미스



amazon



Azure



Google

클라우드도 네트워크는 필수로 알아야 함
온프레미스 네트워크부터 이해해야 한다.

1주차 목차

1장. 네트워크란?

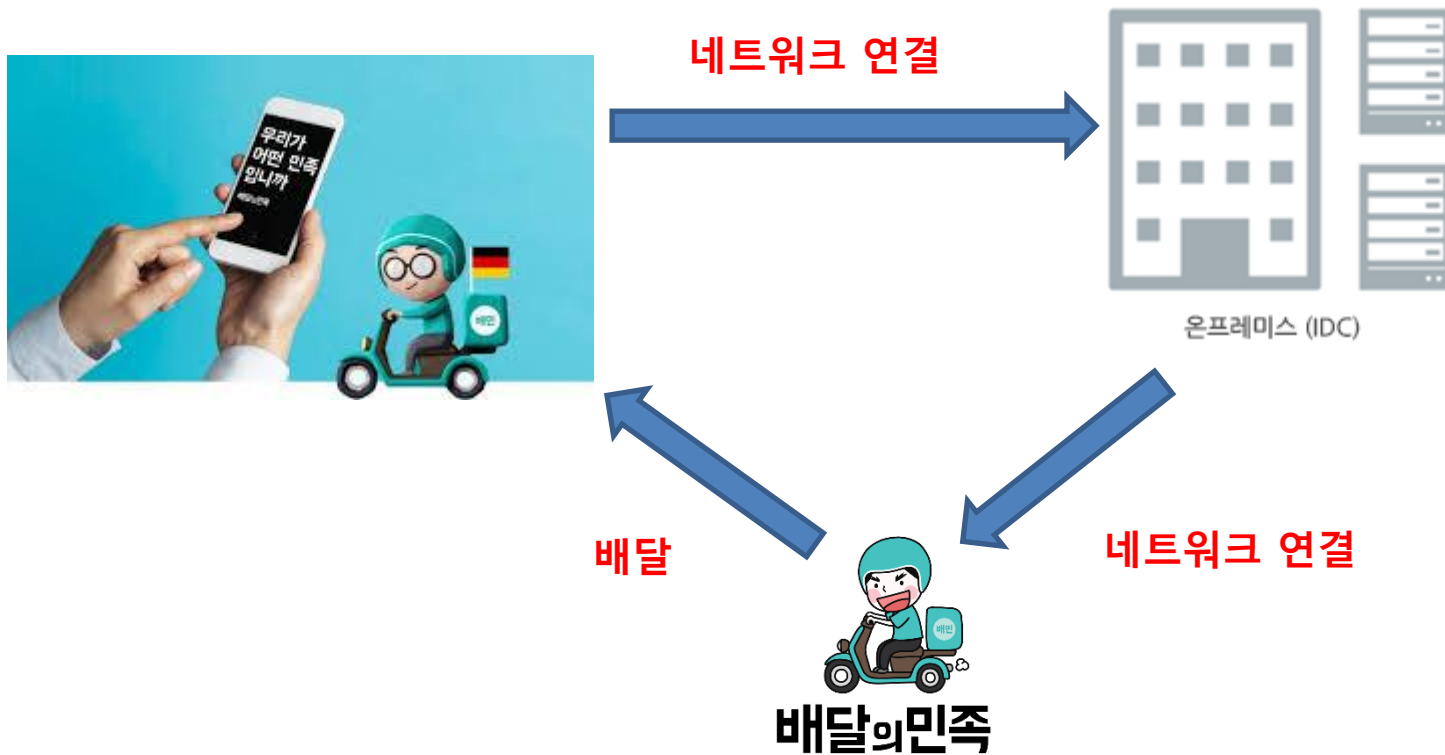
2장. 온프레미스 네트워크 이해

1장. 네트워크란?

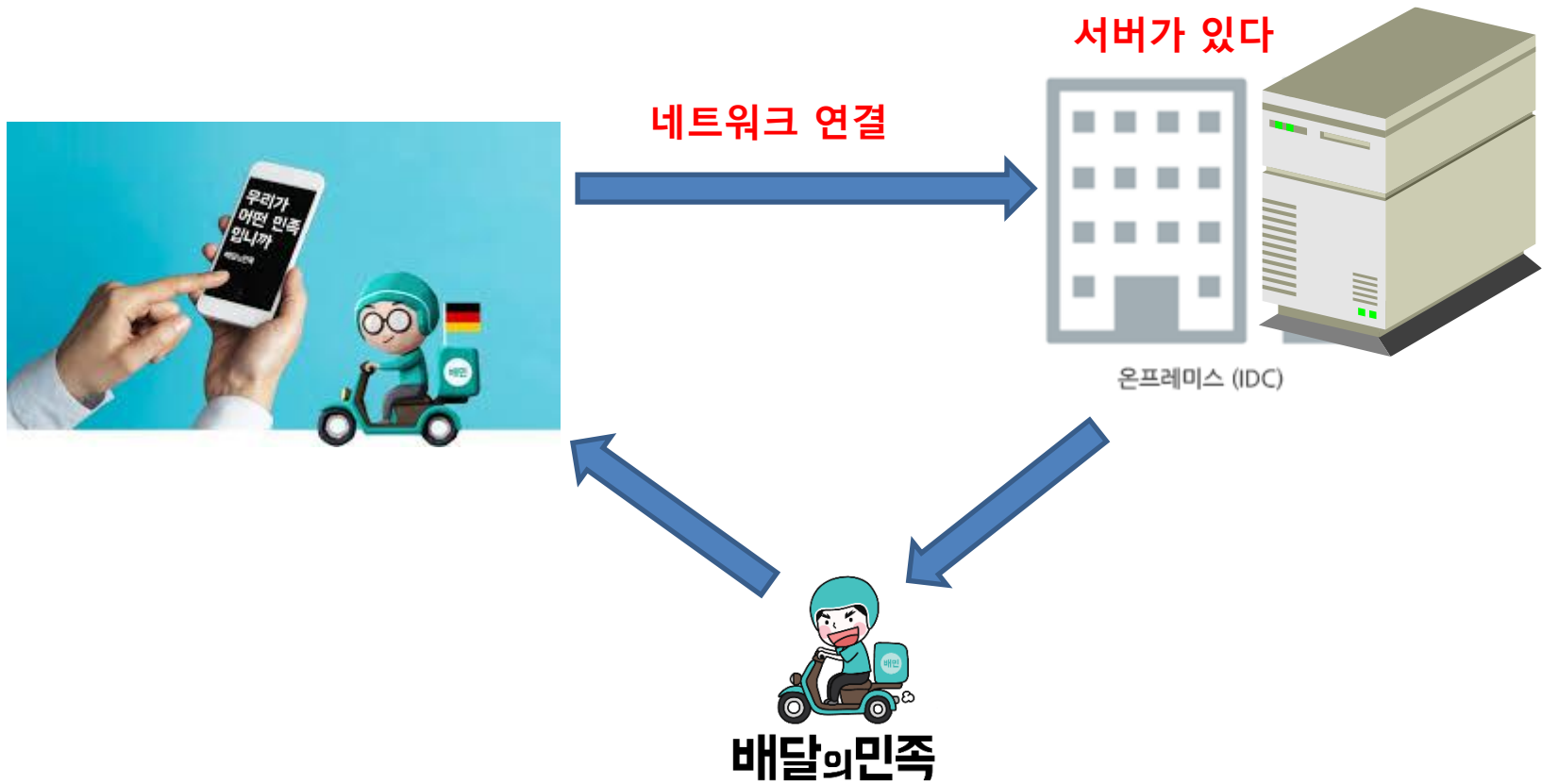


1. 네트워크는 서비스를 하기 위한 연결이다.

연결이다.



2. 네트워크는 서버와 연결을 하게 해준다.



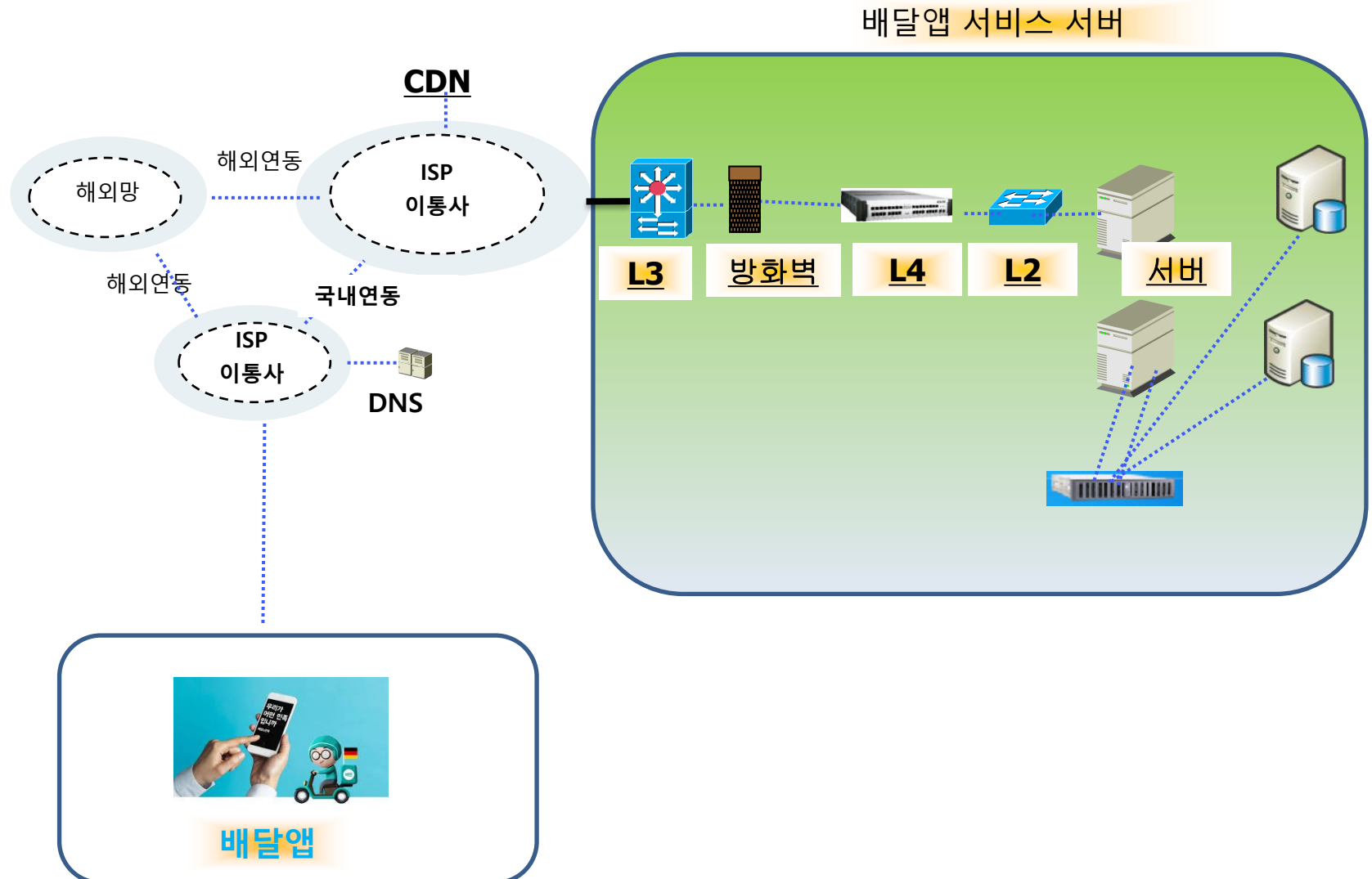
2장. 온프레미스 네트워크를 이해해야 한다.



온프레미스 (IDC)

3. 서버와 연결은 이렇게 된다.

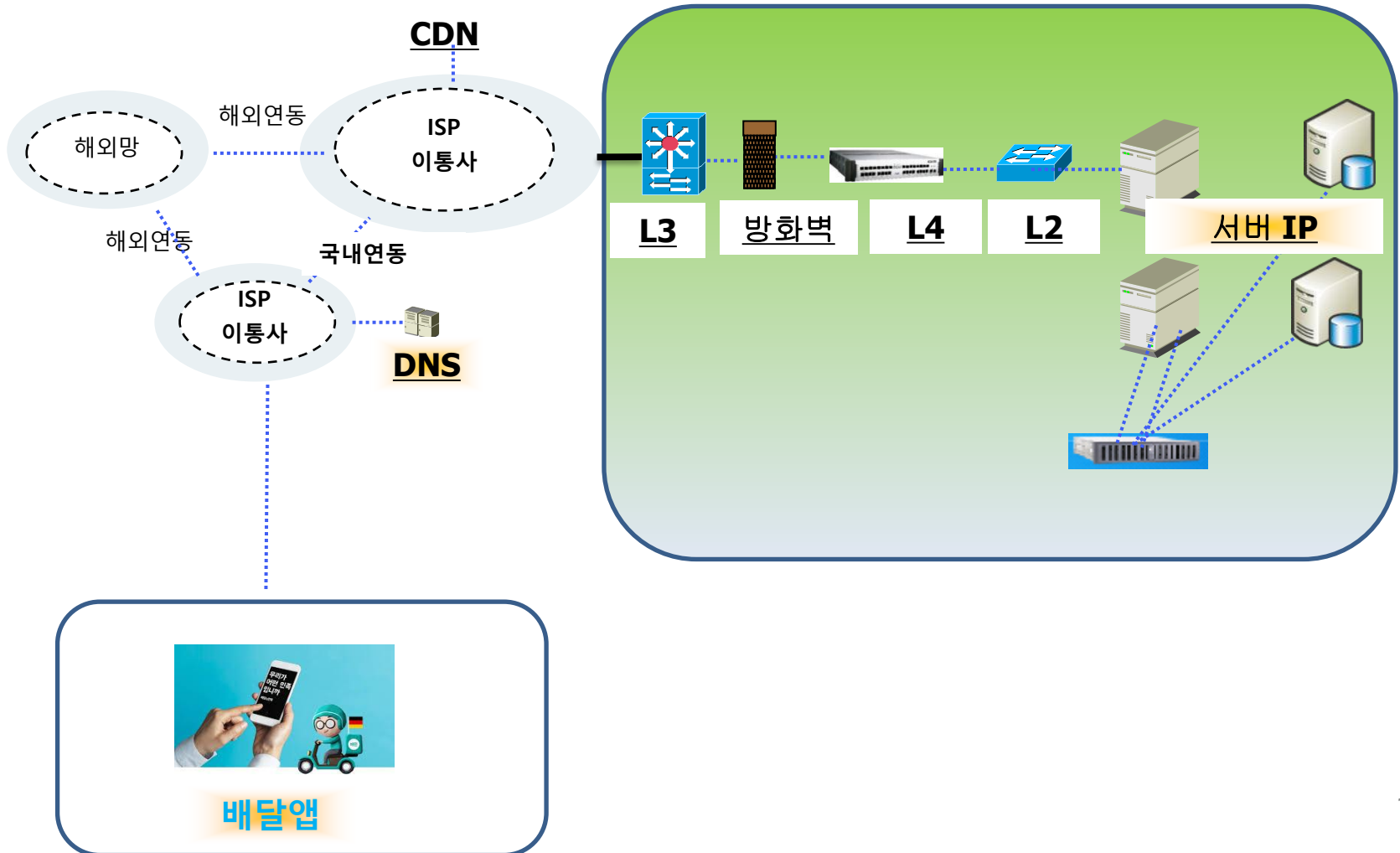
배달앱 -> L3 네트워크장비 -> 방화벽 -> L4 네트워크장비 -> L2 네트워크 장비 > 서버로 접속



4. 서버로는 IP로 접속 한다.

인터넷은 IP 기반으로 되어 있다.

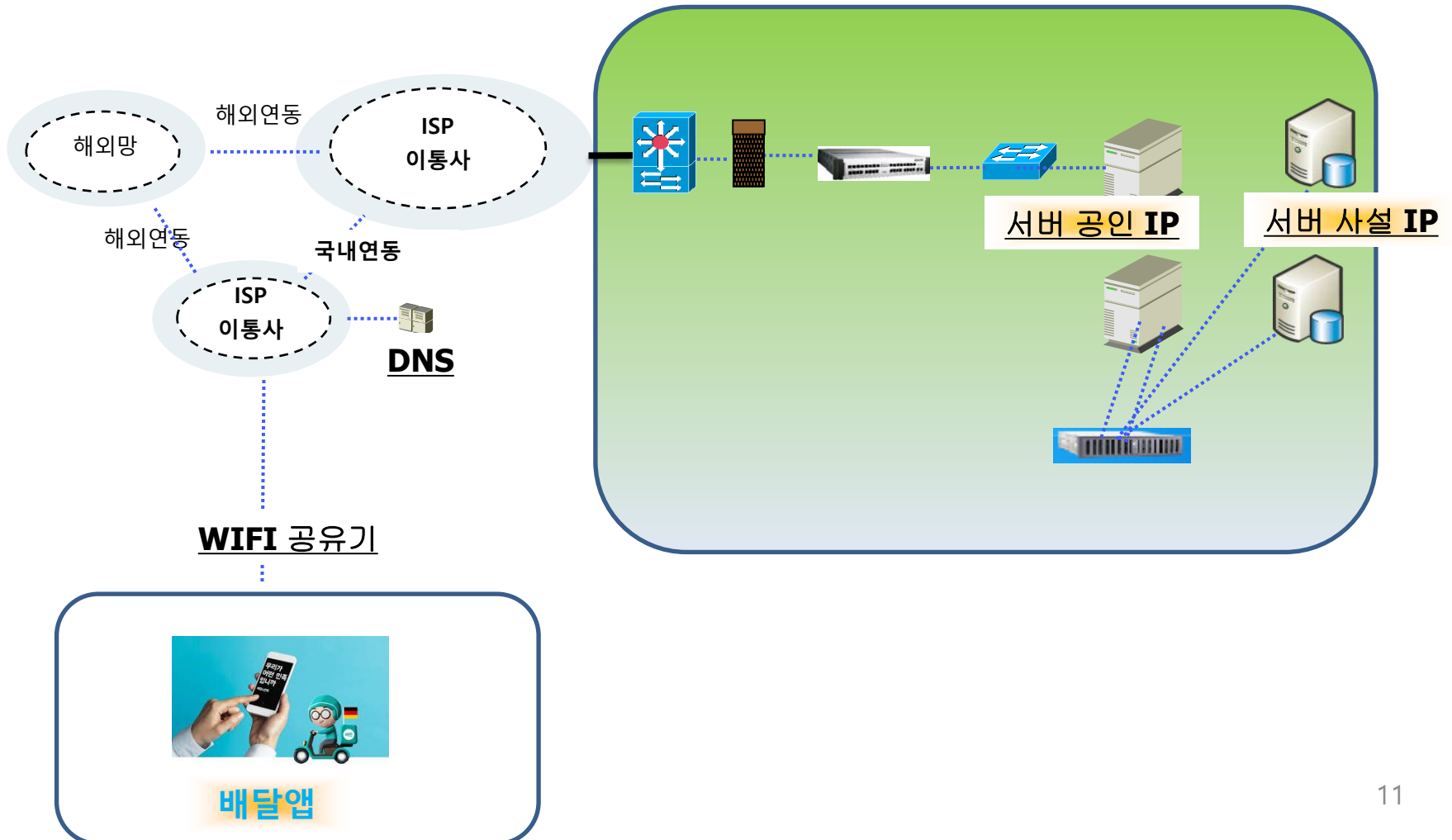
앱은 도메인으로 접속하는데, DNS가 이를 IP로 바꾸어 준다.



5. IP는 공인 IP와 사설 IP 2가지가 있다.

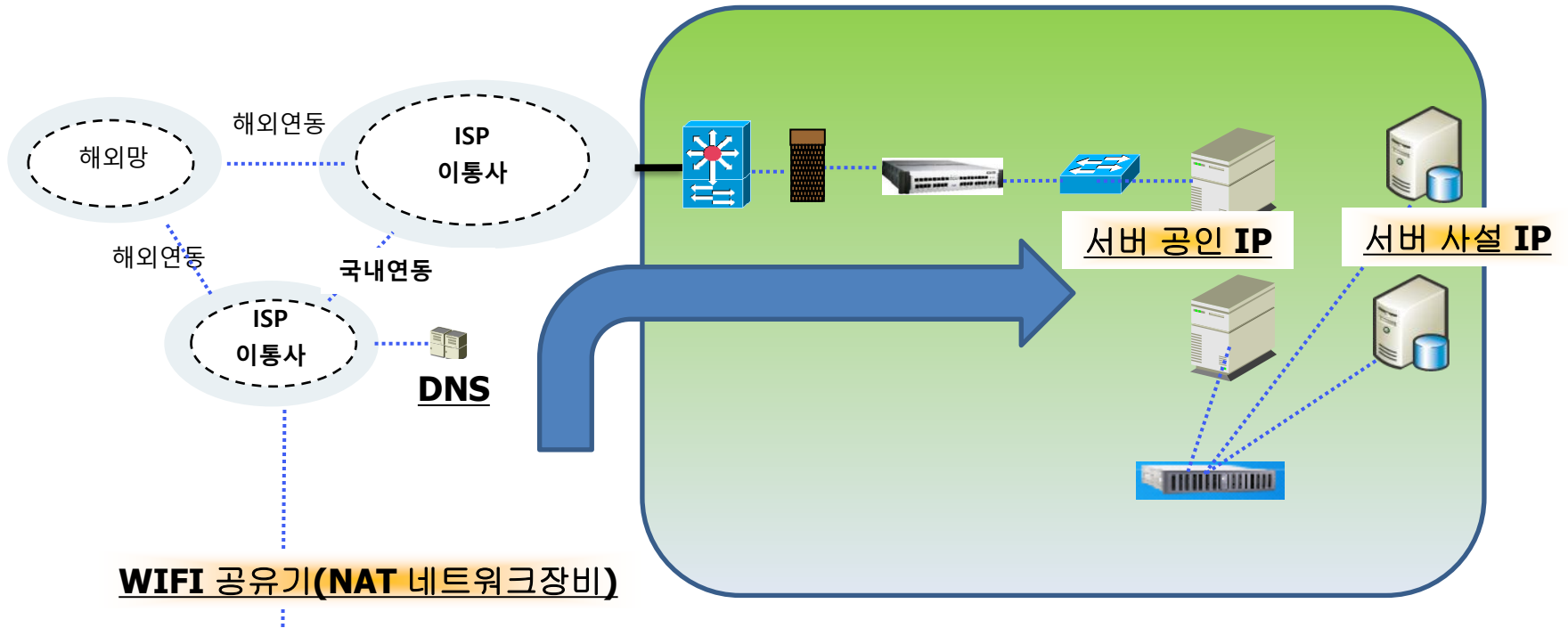
공인IP : 외부에서 접속가능한 IP , 인터넷이 되는 IP , 보통 웹서버

사설IP : 외부에서 접속이 불가능 IP , 인터넷 안되는 IP , DB서버



6. 우리집 네트워크부터 보자

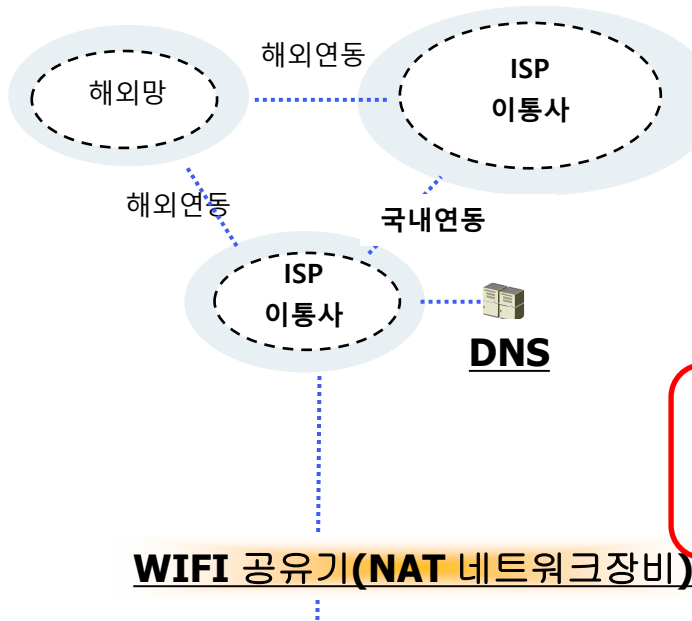
배달앱에서 배달앱 서버로 접속한다.



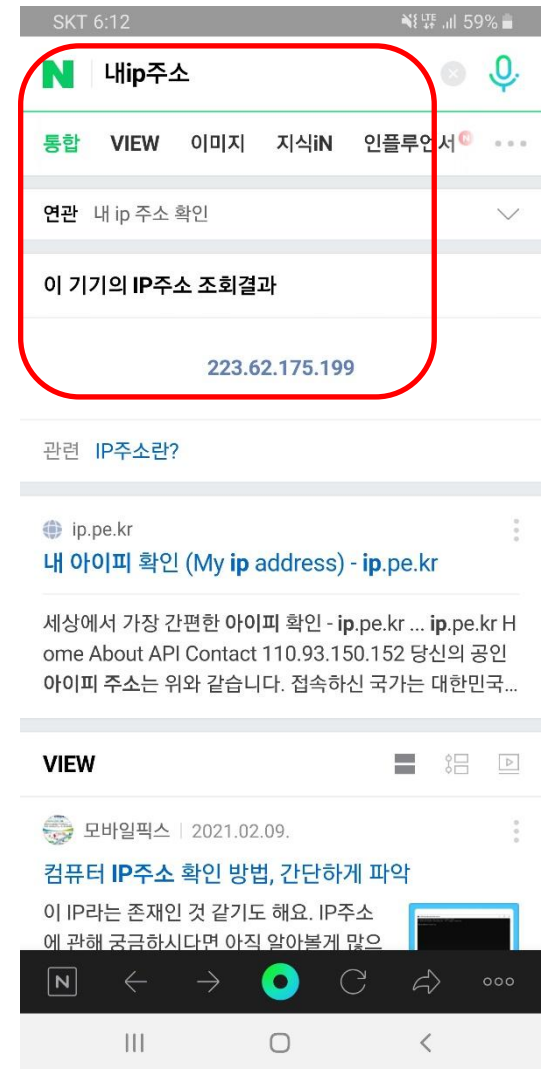
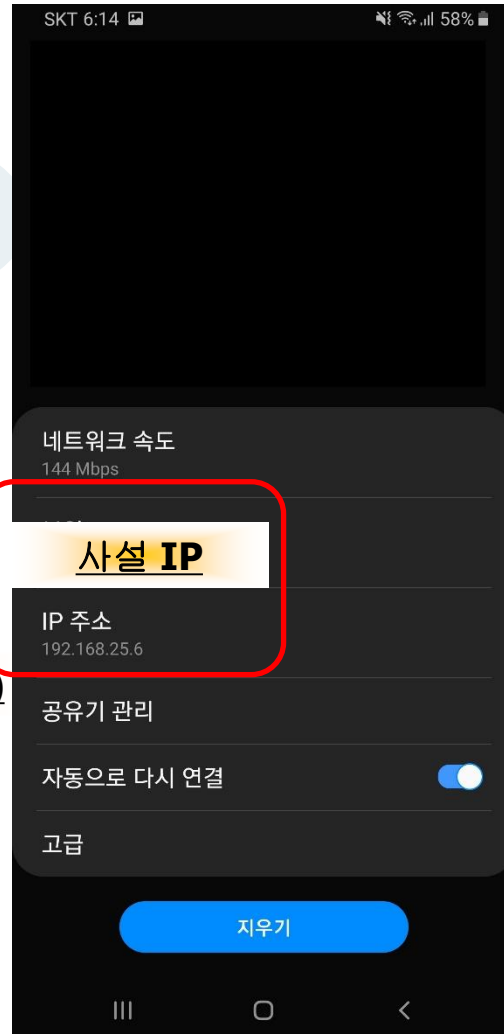
배달앱

7. 우리집 네트워크부터 보자

WIFI를 사용하는 내 스마트폰 IP는 ? 사설IP , 인터넷 안 되어야 하는데 된다?
왜? WIFI공유기가 인터넷을 되게 해준다. = NAT 사용하게 한다.

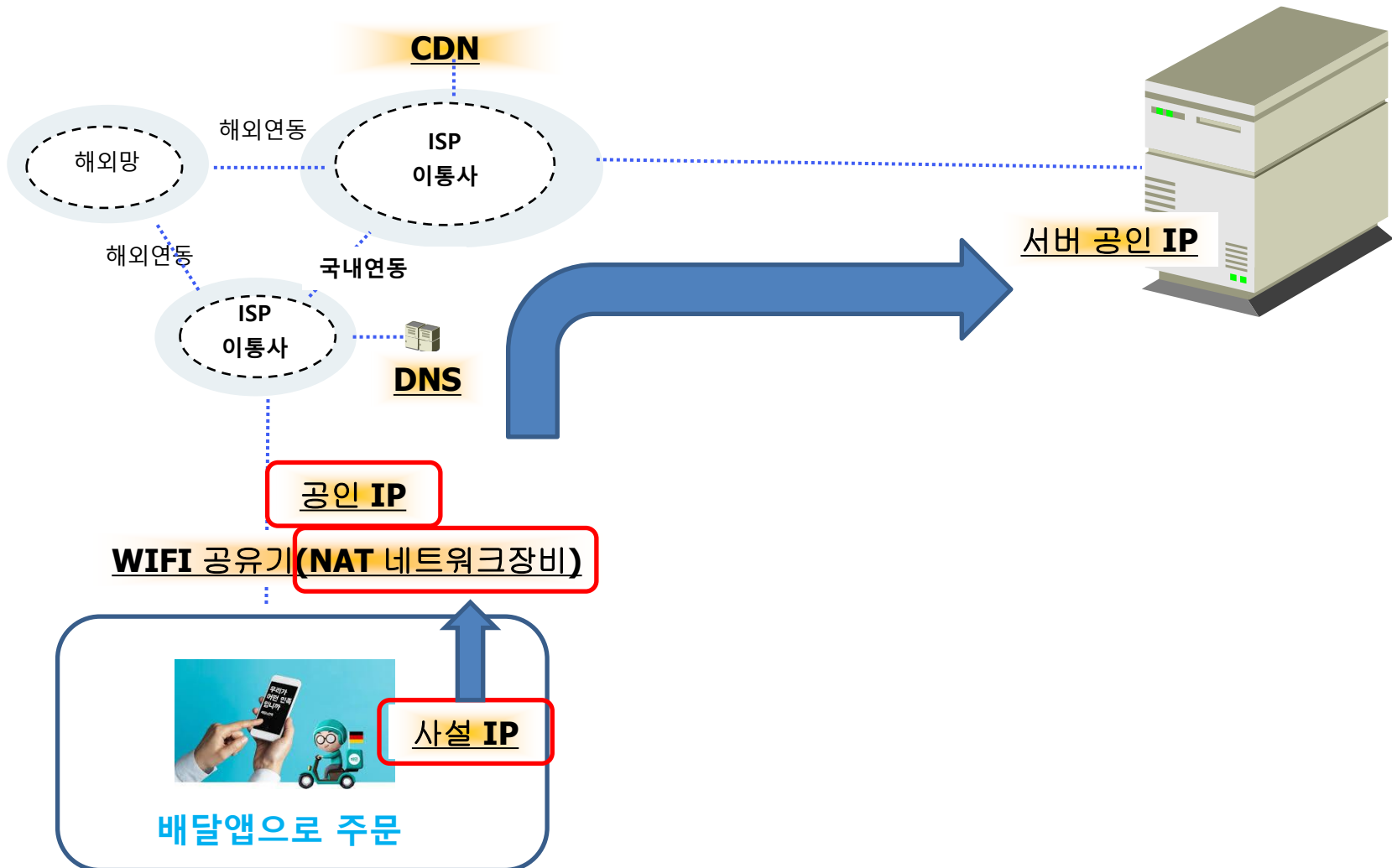


배달앱



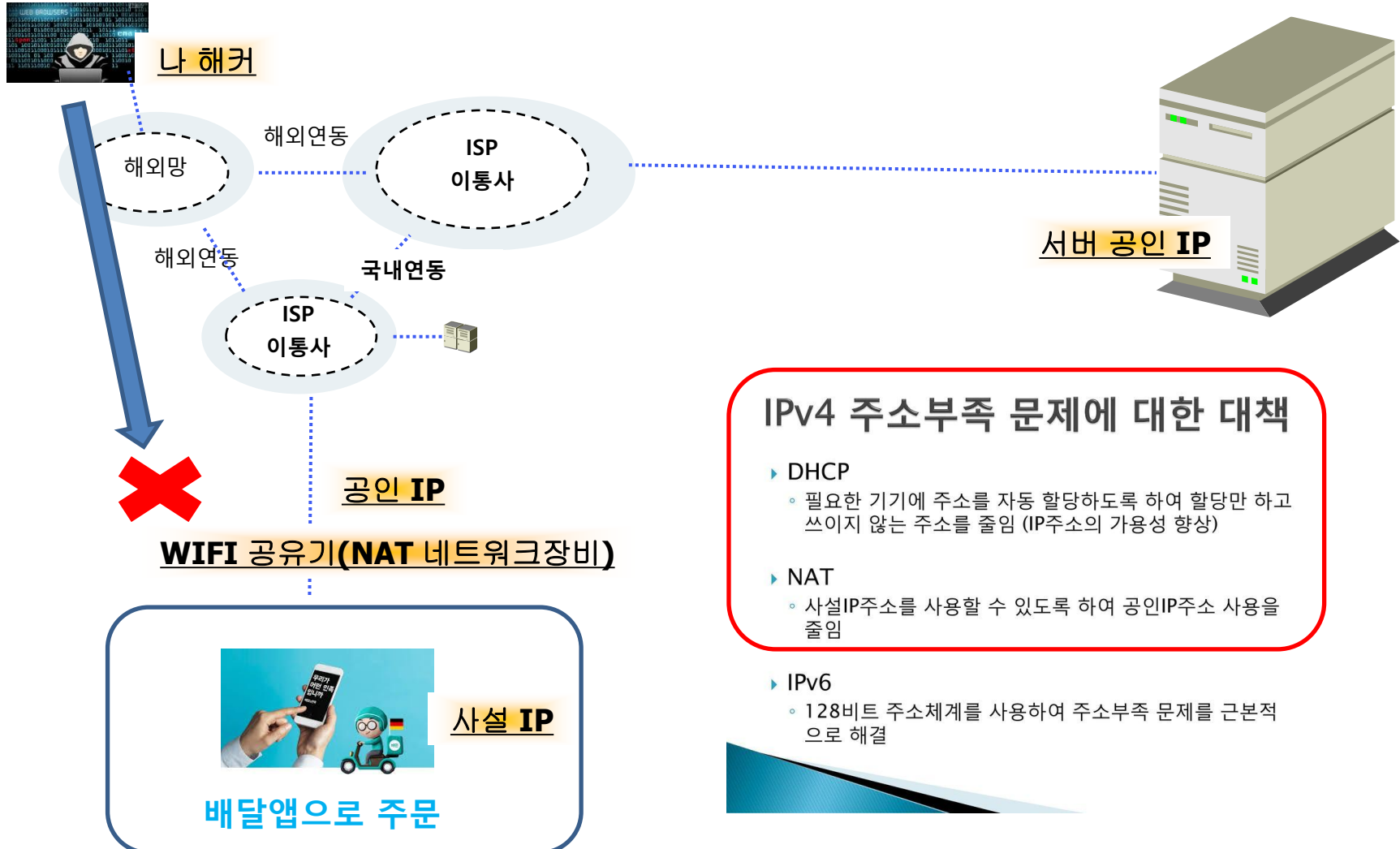
8. NAT란 ?

사설 IP를 공인IP로 매칭시켜 인터넷이 되도록 해주는 것



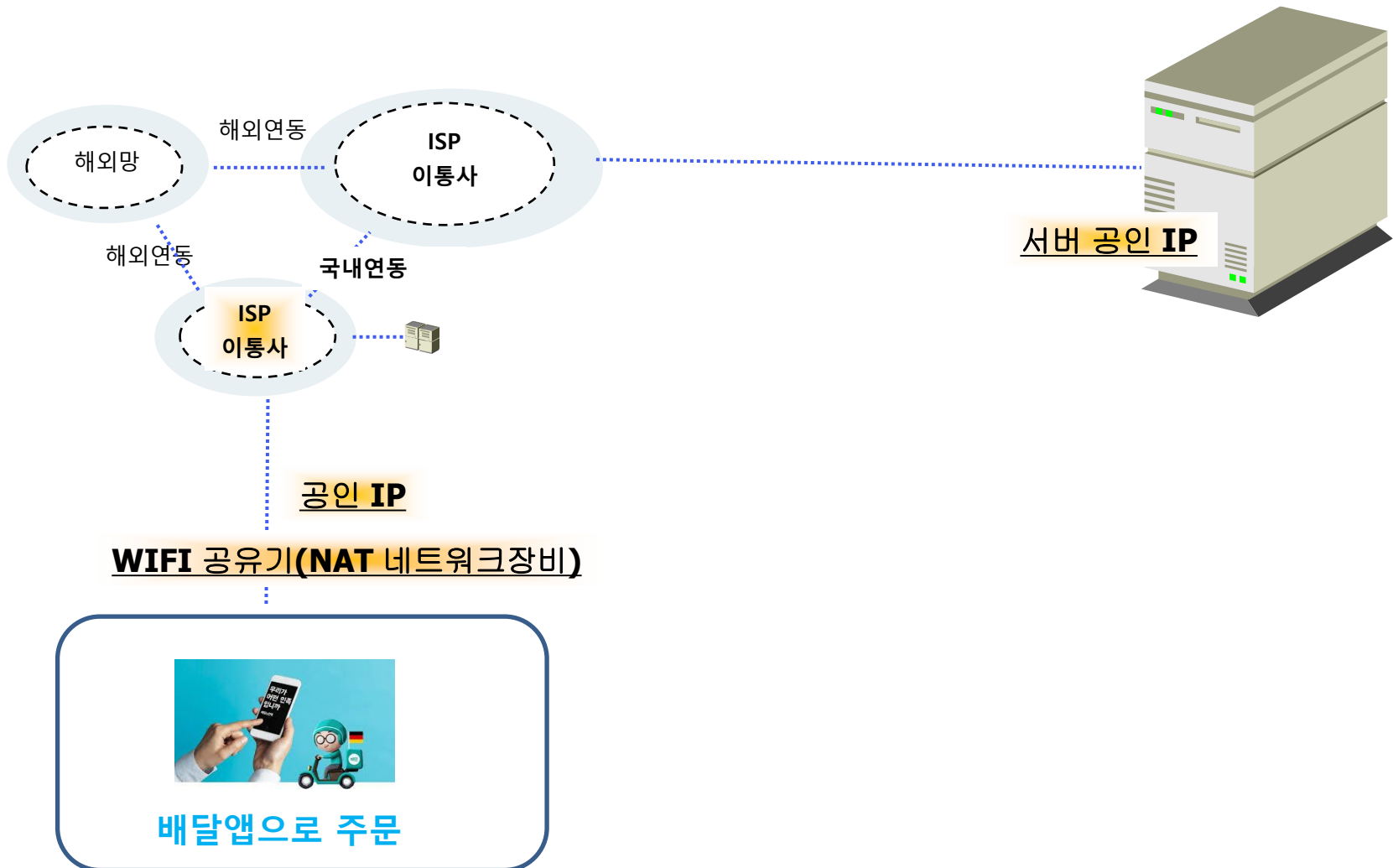
9. 왜 NAT를 사용하는가?

보안적으로 안전하다. = 외부에서 접속은 안 된다.
공인 IP 부족 (IPv4)

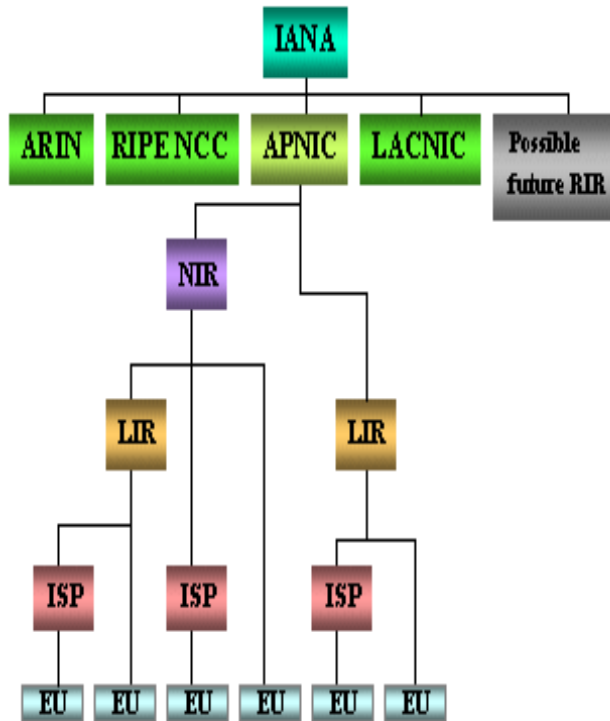


10. 공인IP 누가 할당 하는가?

ISP, 이동사가 한다.
WIFI 공유기에 공인 IP 1개가 매칭된다.



11. 공인IP는 어떻게 할당 되는가?

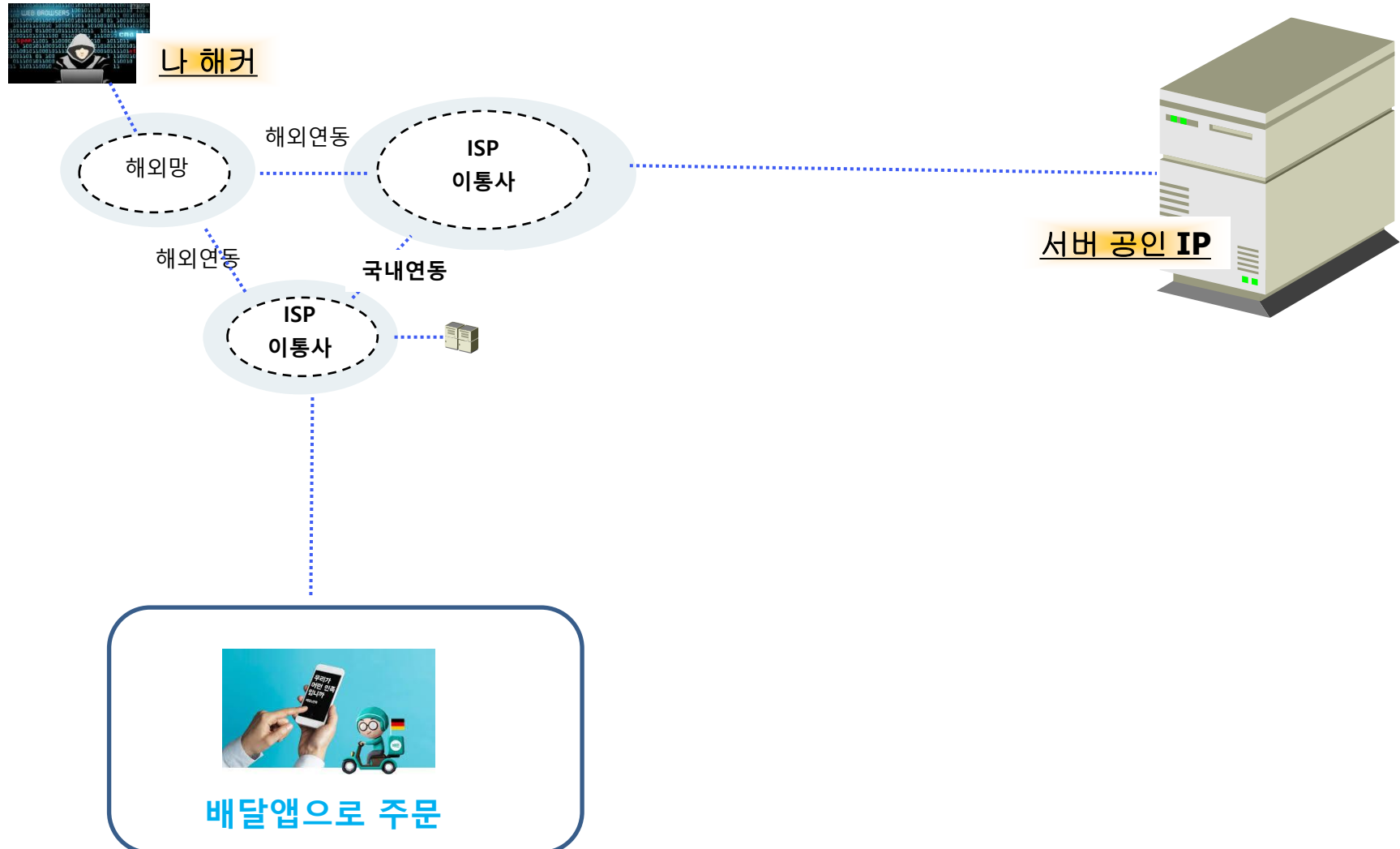


-  National Internet Registries
-  Local Internet Registries
-  Internet Service Provider
-  End-users

	구성	기관	사이트
1	최상위	IANA (Internet Assigned Numbers Authority)	http://www.iana.com/
2	미국	ARIN (American Registry for Internet Numbers)	http://ws.arin.net/cgi-bin/whois.pl
	유럽	RIPE (Réseaux IP Européens)	http://www.ripe.net/perl/whois/
	아시아	APNIC (Aisa Pacific Network Information Center)	http://www.apnic.net/search/index.html
3	각나라	NIR (National Internet Registries) 한국인터넷진흥원 (KISA)	http://whois.nic.or.kr/
4	ISP	ISP / 통신사 (Internet Service Provider)	SKT, KT, LG
5	사용자	EU (End-users)	일반기업, 개인사용자, 정부기관

12. 공인IP를 사용하다 보니 나 해커가 공격해오네~

해커의 공격을 막자



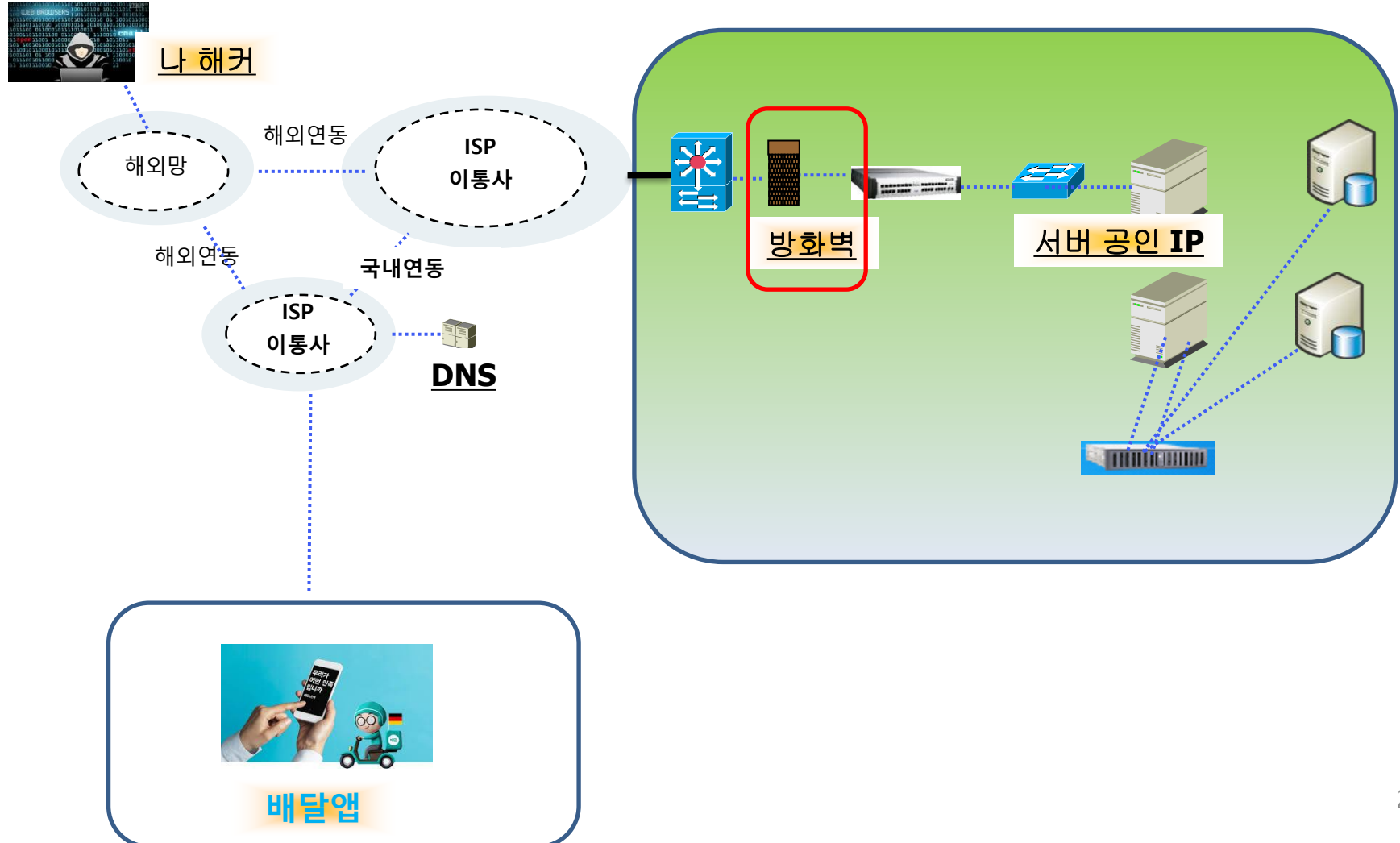
13. 방화벽이 있어야겠네~

인터넷과 같이 외부 네트워크에 연결되어 있는 서버를 보호하는 장치



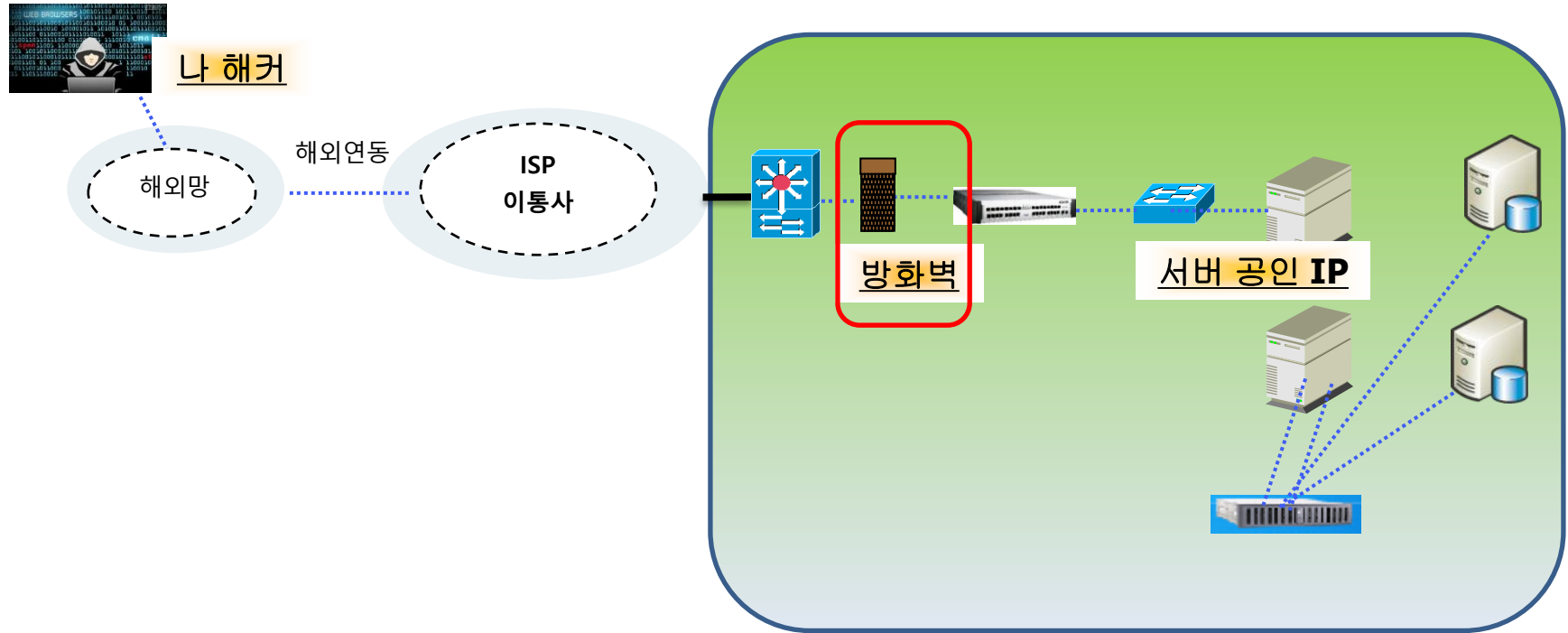
14. 방화벽을 두자

서버 공인IP로 접속하는 접근에 대해 해커가 접근 못하게 하자



15. 방화벽 규칙

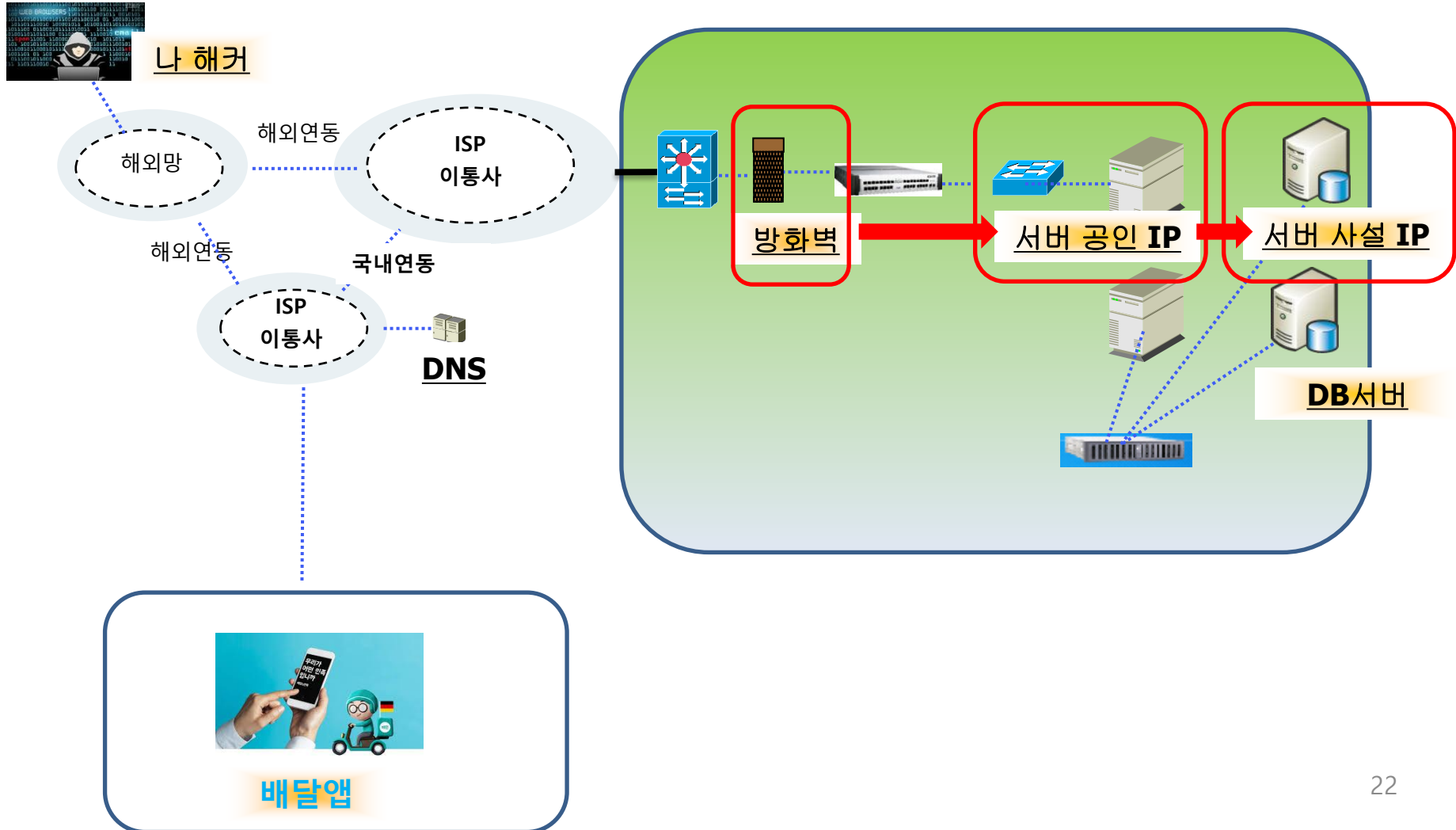
서버 공인IP로 접속하는 접근에 대해 해커가 접근 못하게 하자



소스 IP	소스포트	목적지IP	목적지 포트	정책
0.0.0.0/0	any	any	80	허용
210.0.0.0/24	any	any	22	허용

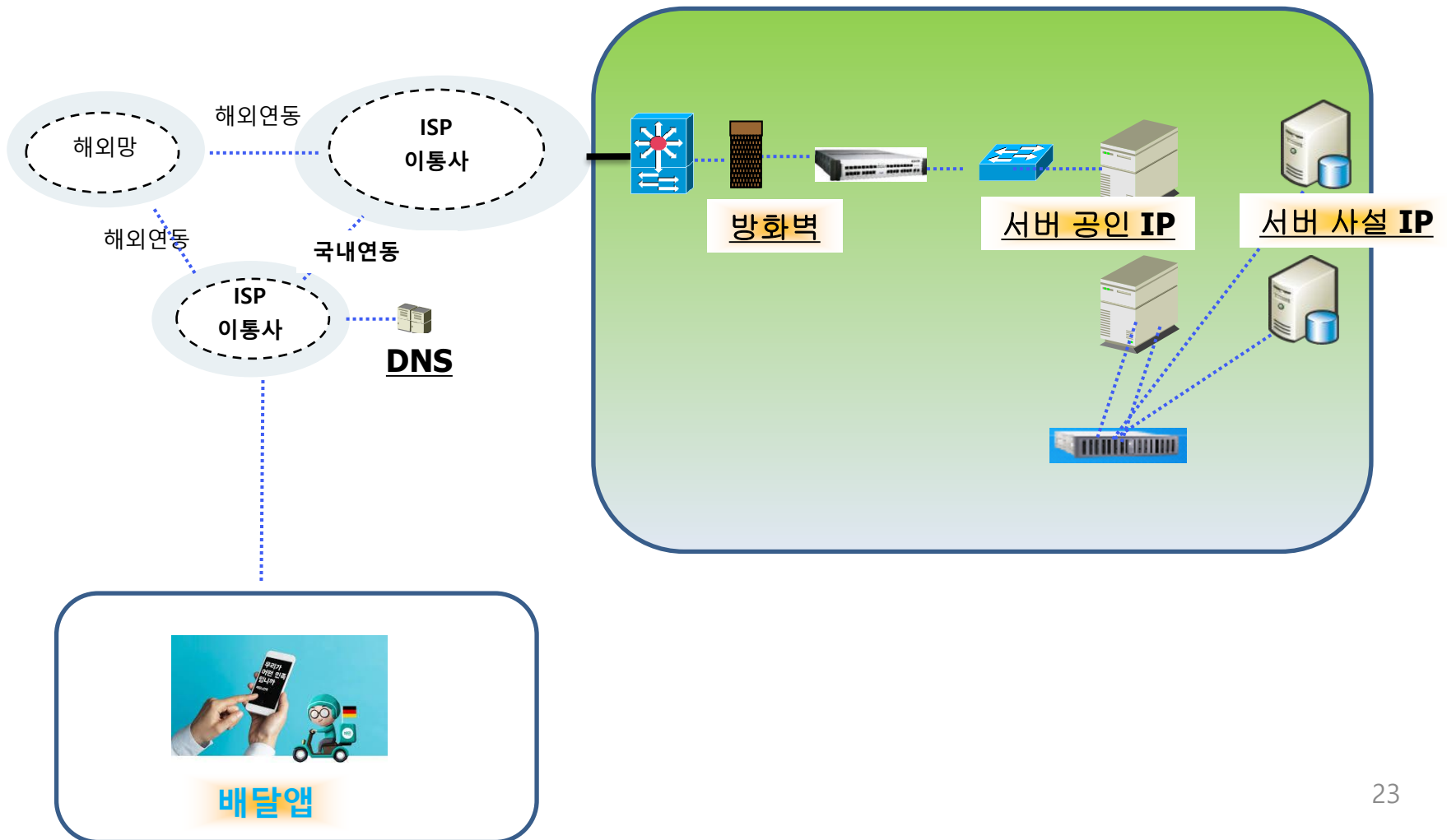
16. 그런데 해커가 들어왔다.

방화벽을 지나 > 서버 공인IP로 접속해 들어왔다.(취약한 웹서버)
서버 공인IP를 통해 > 서버 사설IP로 들어왔다.
DB서버 데이터가 털렸다~ 경찰서에 가서 내가 잡혀간다.



17. 보안 강화를 위해 외부에서 접속할 필요가 없는 서버는 사설IP로 바꾸자

사설 IP는 아무 IP나 써도 되나?



18. 사설IP는 내가 정해줄께~

사설IP도 IANA에서 정해 주었다.

3. Private Address Space

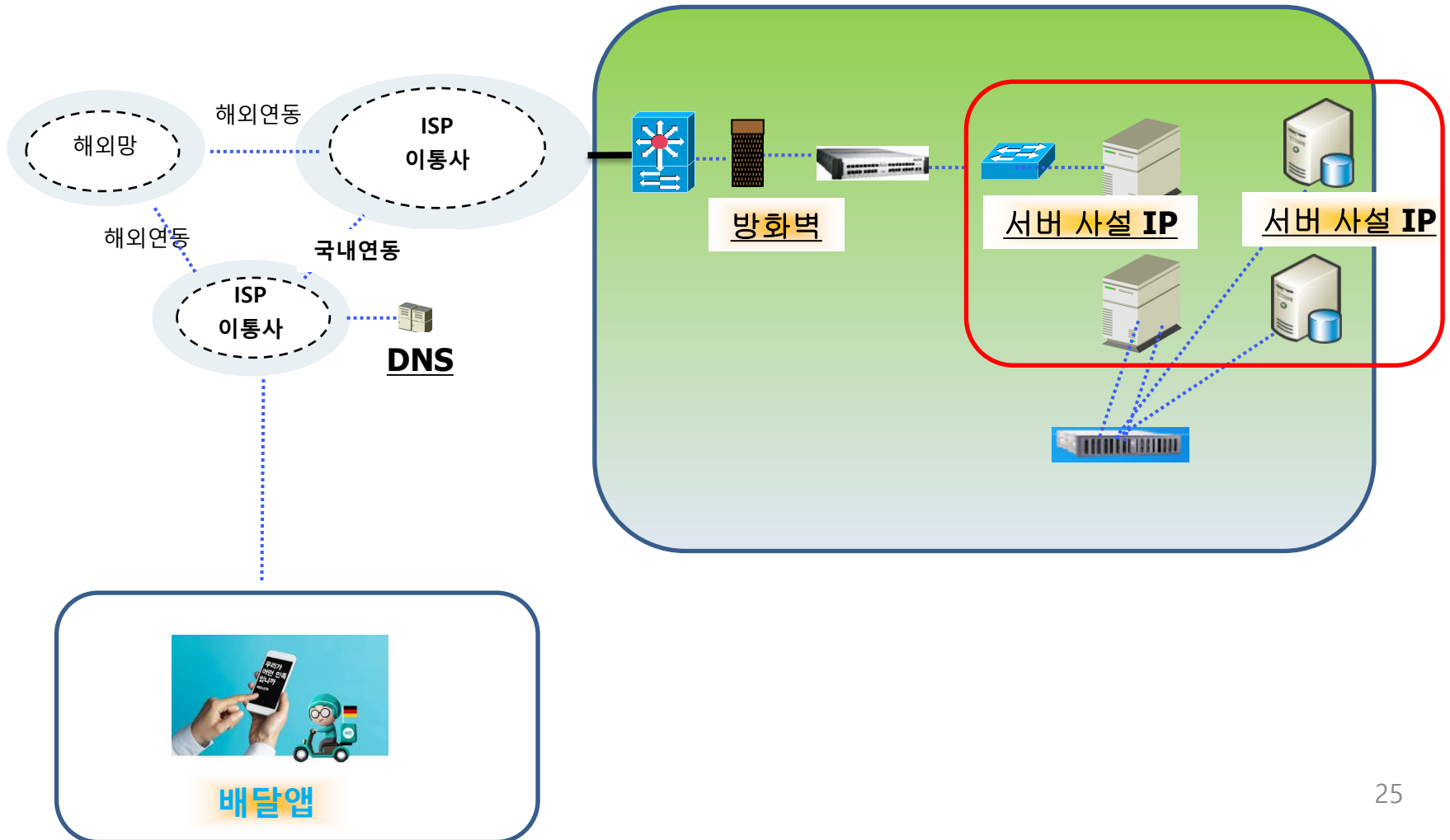
The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0	–	10.255.255.255	(10/8 prefix)
172.16.0.0	–	172.31.255.255	(172.16/12 prefix)
192.168.0.0	–	192.168.255.255	(192.168/16 prefix)

19. 서버를 모두 사설IP로 바꾸면 서버가 안전해지겠네?

모든 서버 IP를 사설로 바꿔보자~

그런데, 외부에서 접속하려면 공인IP가 있어야 한다고 했는데?



20. 그럼 공인IP는 다른 장비에서 하도록 하면 되겠다?

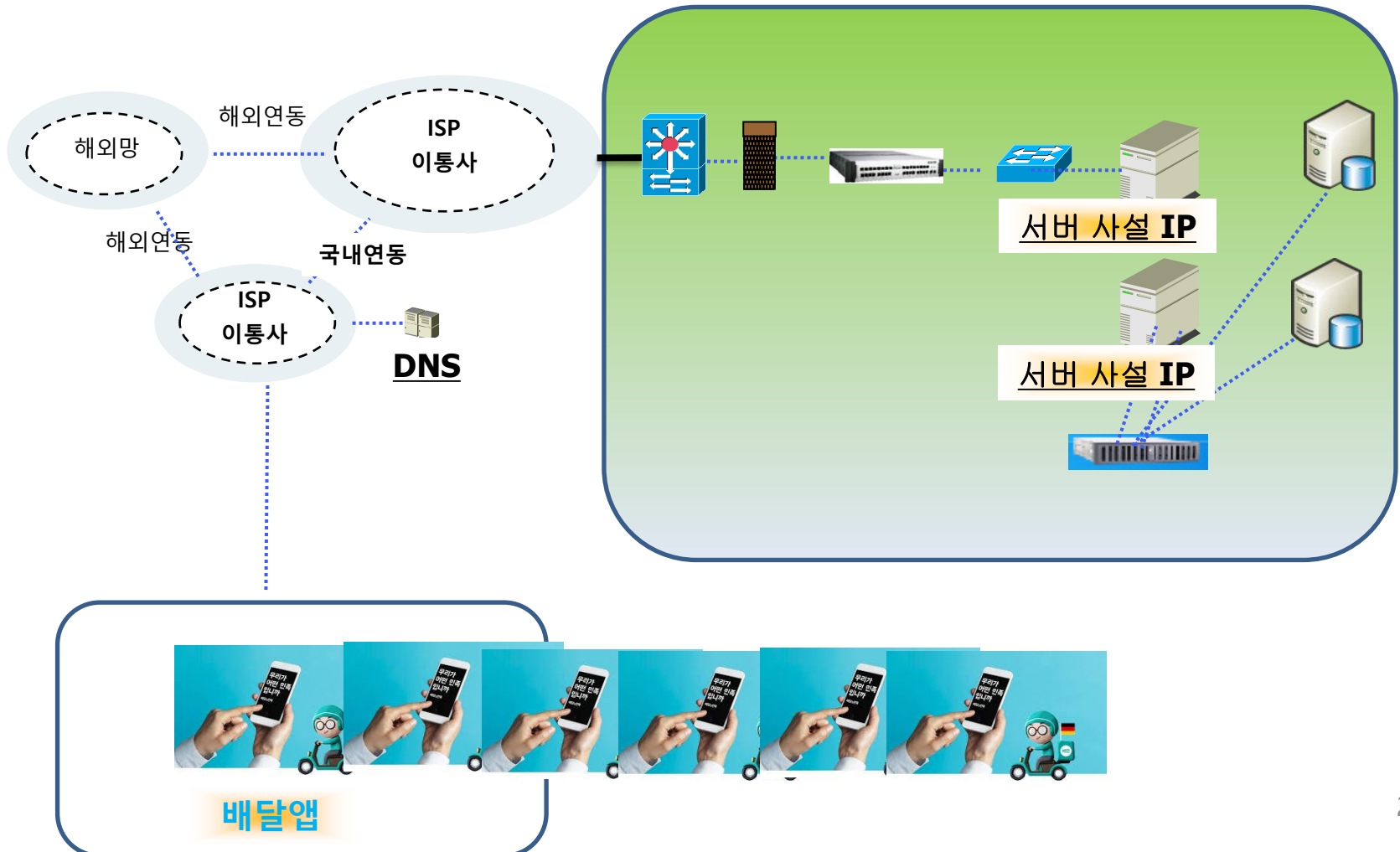
앞단의 L4장비에 공인IP를 부여하고 , 뒷단 사설IP와 연결하자



21. 아~ 그런데 사용자가 늘어 서버가 다운되네~

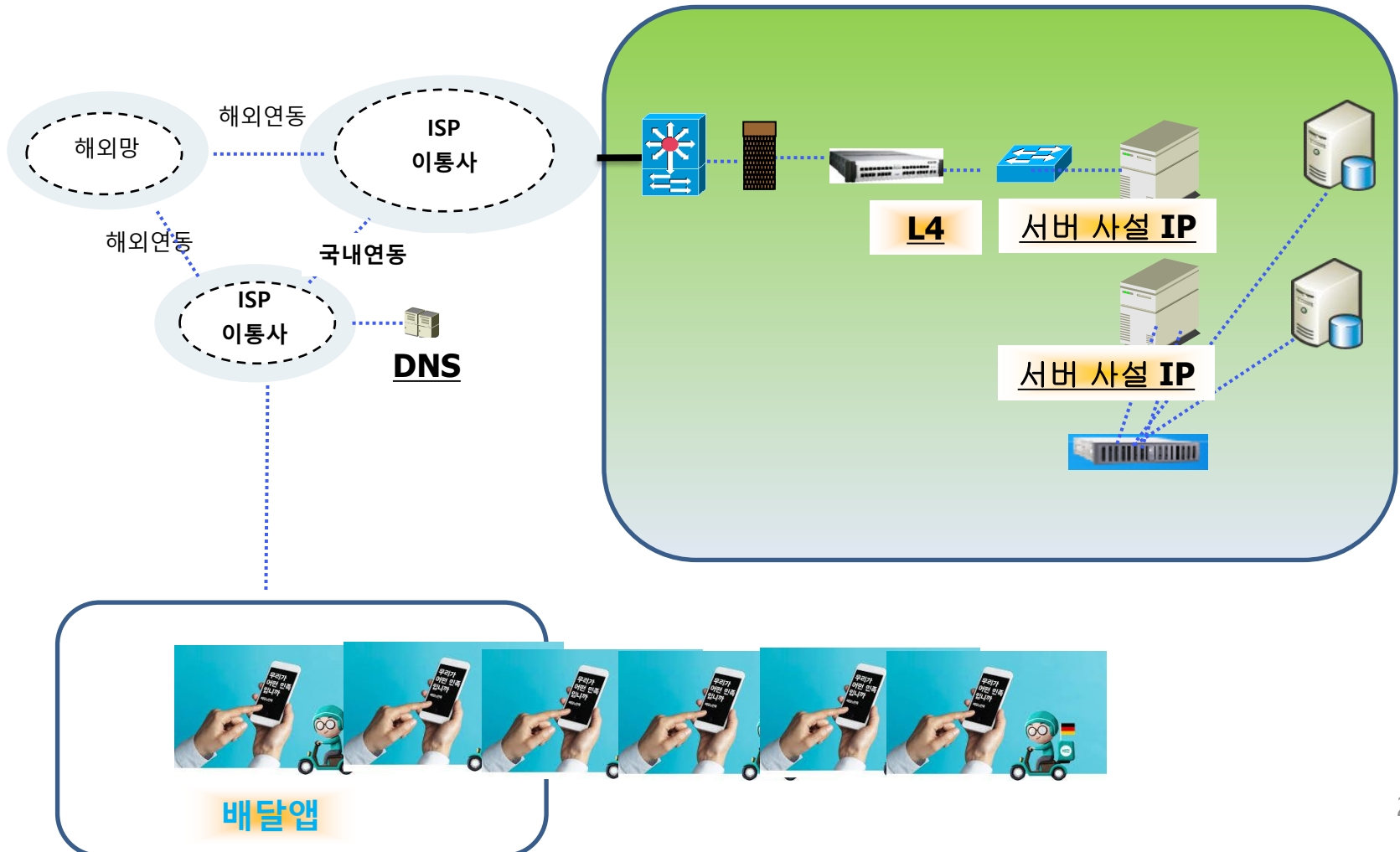
2대로 늘려야 겠다.

그런데 2대중 1대가 죽으니 배달앱이 제대로 안되네~



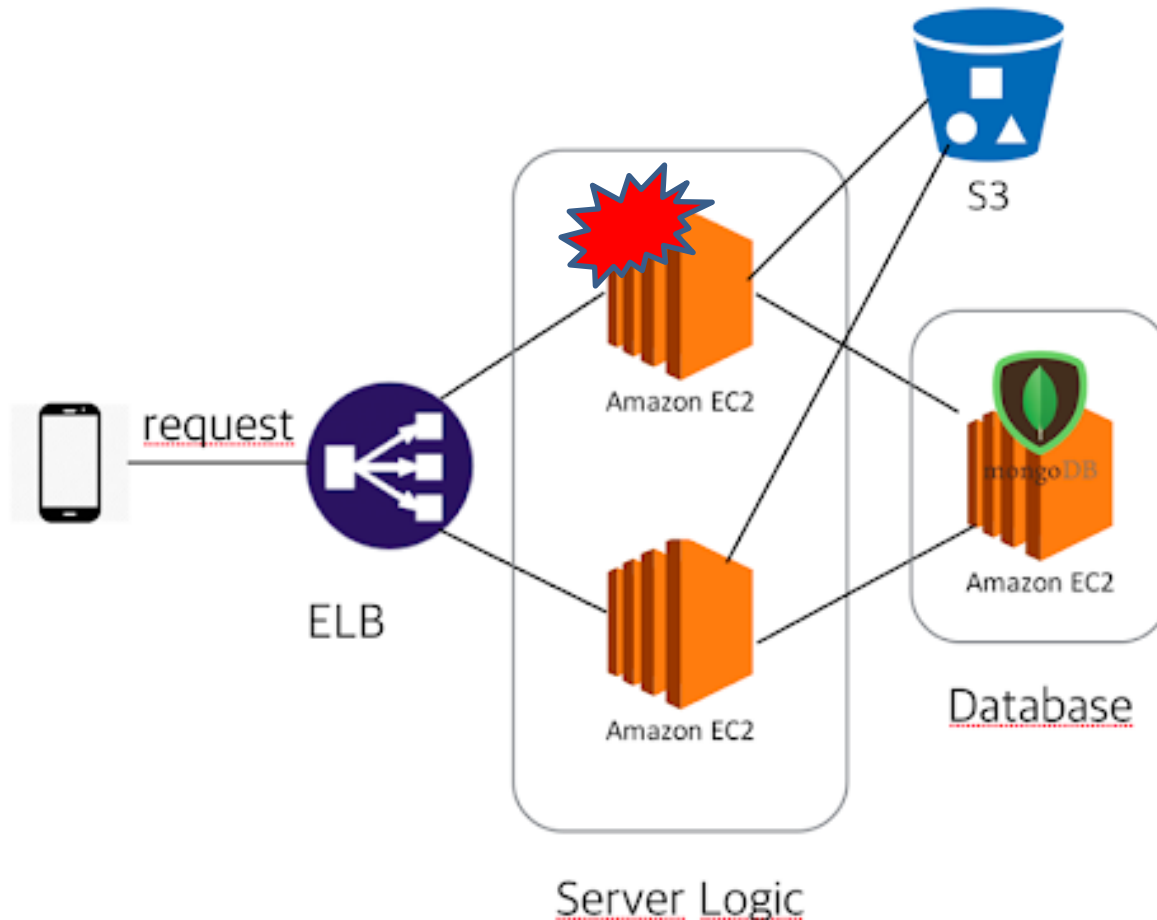
22. 로드 밸런서 사용 - L4, L7

L4 로드밸런서로 서버 2대를 연결하자. 1대가 죽으면 다른쪽으로 서비스가 되게 하자.



23. 로드 밸런싱(Load Balancing)

네트워크 기술로 네트워크 트래픽을 하나 이상의 서버나 장비로 분산하기 위한 기술
Round Robin, Hash , Least Connection 연결이 있다.

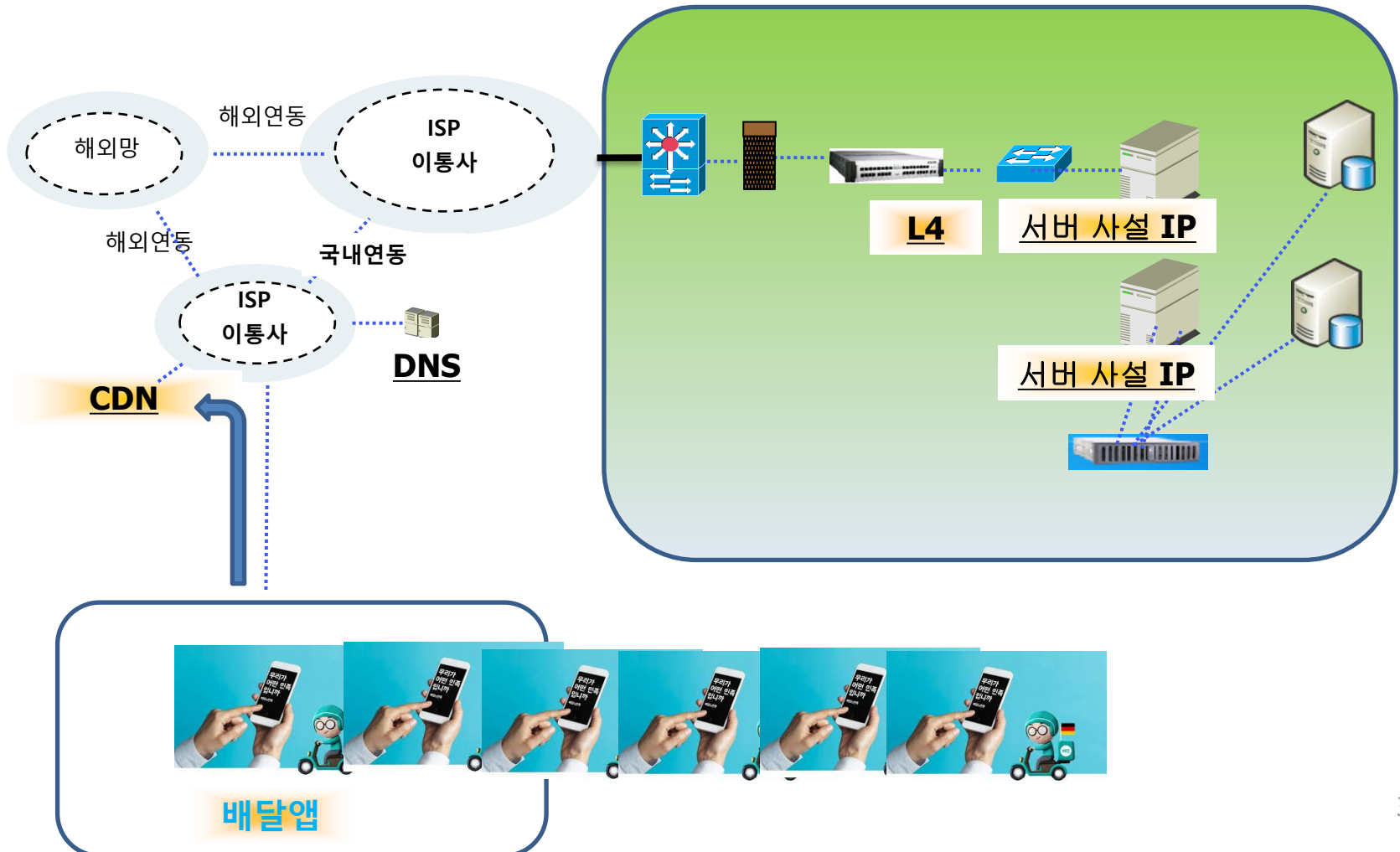


24. CDN 사용

사용자가 늘어 서버에서 받는 게임 파일 다운로드가 느리다고 하네?

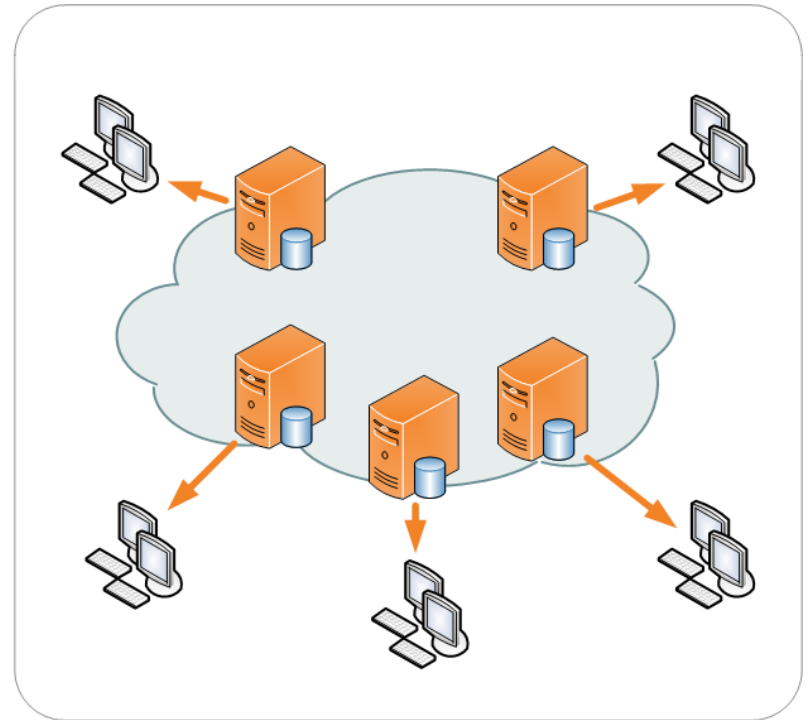
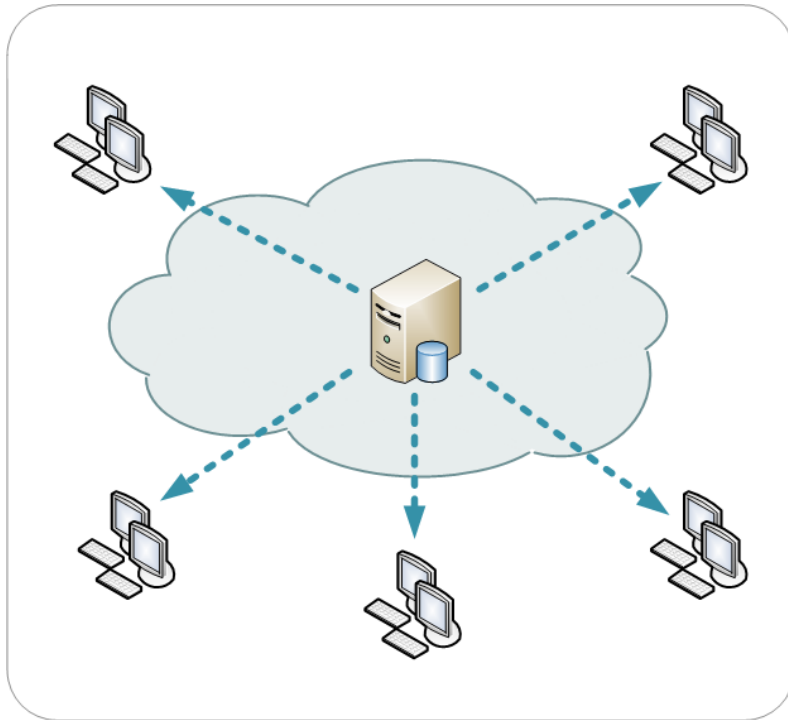
CDN을 사용하자

게임 파일 다운로드를 사용자에게 가까운 CDN에서 받도록 한다. 예지, Edge에서 받아라~



25. CDN(Content Delivery Network)

CDN은 콘텐츠를 효율적으로 전달하기 위해 구성된 네트워크이다.
게임 다운로드의 경우, 가까운 곳에서 다운로드 받도록 하는 것이다.



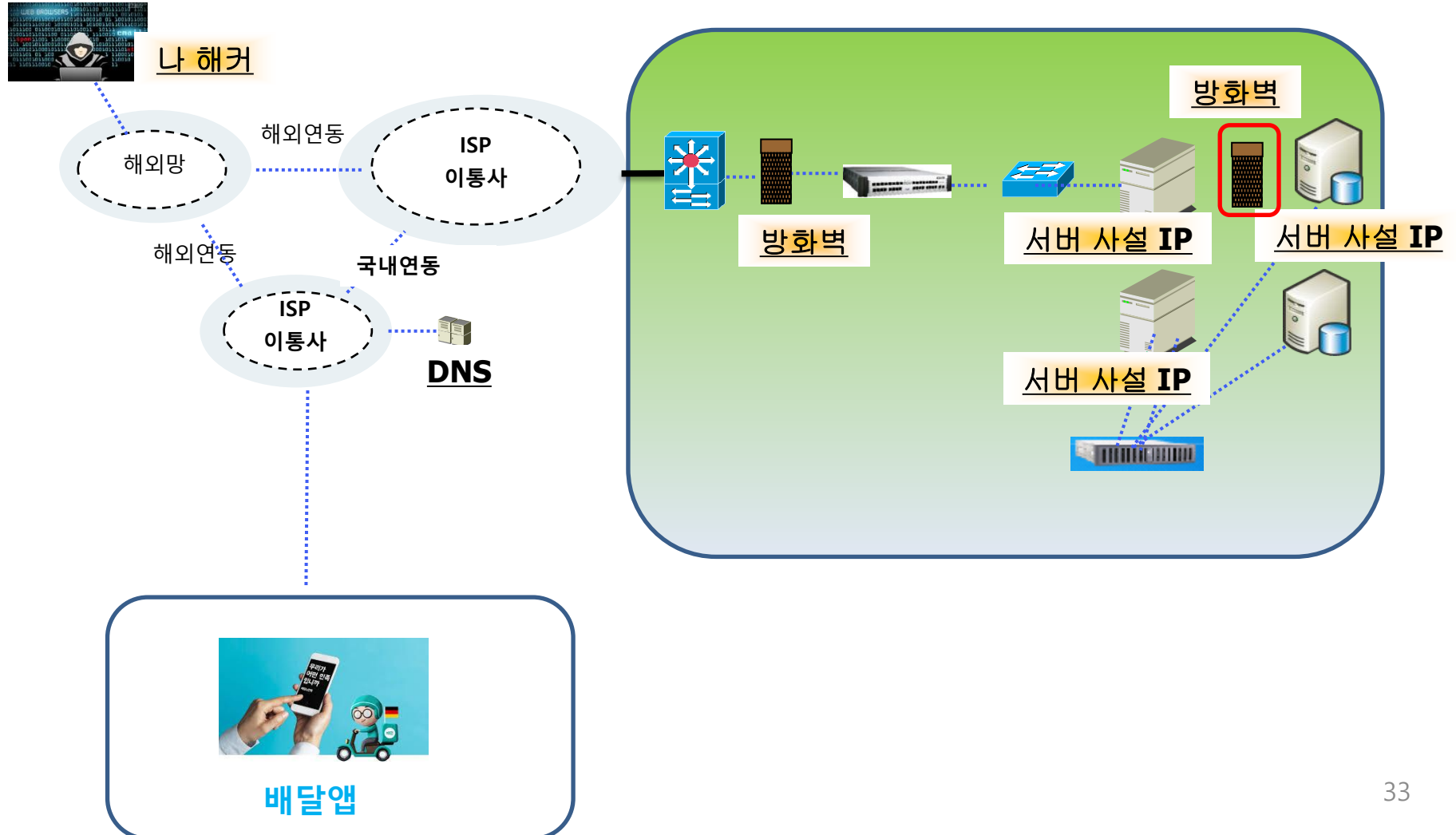
26. 그런데, L4를 통해 서버로 들어온 놈이 DB서버로 접속하네~

외부에서 접속 되는 서버 사설IP와 DB서버 사설IP와 분리해야 겠네~
네트워크를 나눠야 하겠네 ~
서브네팅해야 겠네~



27. 사설IP간 네트워크를 나누고 방화벽을 두어야 겠다~

네트워크를 나누고, 둘 사이에 방화벽을 두자~
그럼 좀 안전해지겠네~



28. 우선 IP에 대해 알아보자

IP는 32bits 구성됨.

8 bits 8 bits 8 bits 8 bits
11111111. 11111111. 11111111. 11111111
255.255.255.255

$$= 8\text{bit} * 4 = 32\text{bit}$$

CIDR표기법 /8, /16 , /24

A Class

IP 10.0.0.0/8 = 8bit
11111111.00000000.00000000.00000000
Subnet Mask 255.0.0.0
사용IP는 10.0.0.0~ 10.255.255.255

B Class

IP 10.0.0.0/16 = 16bit
Subnet Mask 255.255.0.0
사용IP는 10.0.0.0~ 10.0.255.255

C Class

IP 10.0.0.0/24 = 24bit
Subnet Mask 255.255.255.0
사용IP는 10.0.0.0~ 10.0.0.255 (IP 256개)

29. B Class를 서브네팅 해보자1

할당	2개로	4개로
10.0.0.0/16	10.0.0.0/17 10.0.0.128/17	10.0.0.0/18 10.0.0.64/18 10.0.0.128/18 10.0.0.192/18

/16	/17	/18	-	/20	/21	/22	/23	/24
0~255	0~127	0~63		0~15	0~7	0~3	0 1	
							2 3	
		64~127				4~7	4 5	
							6 7	
		128~191			8~15	8~11	8 9	
							10 11	
		192~255				12~15	12 13	
							14 15	
				16~31	16~23	16~19	16 17	
							18 19	
						20~23	20 21	
							22 23	
					24~31	24~27	24 25	
	128~255						26 27	
						28~31	28 29	

30. 서브네팅 해보자2

할당	2개로	4개로
10.0.0.0/20	10.0.0.0/21 10.0.8.0/21	10.0.0.0/22 10.0.4.0/22 10.0.8.0/22 10.0.12.0/22

/16	/17	/18	-	/20	/21	/22	/23	/24
0~255	0~127	0~63		0~15	0~7	0~3	0 1	
							2 3	
		64~127				4~7	4 5	
							6 7	
		128~191			8~15	8~11	8 9	
							10 11	
		192~255				12~15	12 13	
							14 15	
				16~31	16~23	16~19	16 17	
							18 19	
						20~23	20 21	
							22 23	
					24~31	24~27	24 25	
	128~255						26 27	
						28~31	28 29	

31. 서브네팅 해보자3

할당	2개로	4개로
10.0.16.0/20	10.0.16.0/21 10.0.24.0/21	10.0.16.0/22 10.0.20.0/22 10.0.24.0/22 10.0.28.0/22

/16	/17	/18	-	/20	/21	/22	/23	/24
0~255	0~127	0~63		0~15	0~7	0~3	0 1	
							2 3	
		64~127				4~7	4 5	
							6 7	
		128~191			8~15	8~11	8 9	
							10 11	
		192~255				12~15	12 13	
							14 15	
				16~31	16~23	16~19	16 17	
							18 19	
						20~23	20 21	
							22 23	
					24~31	24~27	24 25	
	128~255						26 27	
						28~31	28 29	

32. 서브네팅 해보자4

할당	2개로	4개로
10.0.0.0/22	10.0.0.0/23 10.0.1.0/23	10.0.0.0/24 10.0.1.0/24 10.0.2.0/24 10.0.3.0/24

/16	/17	/18	-	/20	/21	/22	/23	/24
0~255	0~127	0~63		0~15	0~7	0~3	0 1	
							2 3	
		64~127				4~7	4 5	
							6 7	
		128~191			8~15	8~11	8 9	
							10 11	
		192~255				12~15	12 13	
							14 15	
				16~31	16~23	16~19	16 17	
							18 19	
						20~23	20 21	
							22 23	
					24~31	24~27	24 25	
	128~255						26 27	
						28~31	28 29	

33. 서브네팅 해보자5

할당	2개로	4개로
10.0.4.0/22	10.0.4.0/23 10.0.6.0/23	10.0.4.0/24 10.0.5.0/24 10.0.6.0/24 10.0.7.0/24

/16	/17	/18	-	/20	/21	/22	/23	/24
0~255	0~127	0~63		0~15	0~7	0~3	0 1	
							2 3	
		64~127				4~7	4 5	
							6 7	
		128~191			8~15	8~11	8 9	
							10 11	
		192~255				12~15	12 13	
							14 15	
				16~31	16~23	16~19	16 17	
							18 19	
						20~23	20 21	
							22 23	
					24~31	24~27	24 25	
	128~255						26 27	
						28~31	28 29	

34. 서브네팅 해보자6

할당	2개로	4개로
10.0.4.0/23	10.0.4.0/24 (ip 253개) 10.0.5.0/24 (ip 253개)	10.0.4.0 /25 (ip125개) 10.0.4.128 /25 (ip125개) 10.0.5.0 /25 (ip125개) 10.0.5.128 /25 (ip125개)

/16	/17	/18	-	/20	/21	/22	/23	/24
0~255	0~127	0~63		0~15	0~7	0~3	0 1	
							2 3	
		64~127				4~7	4 5	
							6 7	
		128~191			8~15	8~11	8 9	
							10 11	
		192~255				12~15	12 13	
							14 15	
				16~31	16~23	16~19	16 17	
							18 19	
						20~23	20 21	
							22 23	
					24~31	24~27	24 25	
	128~255						26 27	
						28~31	28 29	

35. 서브네팅이란 host자리를 1로 채우는것이다.

네트워크 비트			호스트 비트
11111111	11111111	11111111	0
255	255	255	0
11111111	11111111	11111111	10000000
255	255	255	128

C Class

IP 10.0.0.0/24 =/24 = 8bit, 8bit, 8bit , 0bit = 8bit * 3= 24bit
Subnet Mask 255.255.255.0
사용IP는 10.0.0.0~ 10.0.0.255

/24는 /25 2개 네트워크로 나뉜다

IP 10.0.0.0/25 = /25 = 8bit, 8bit, 8bit , 1bit = 25bit
Subnet Mask 255.255.255.128
(ip 0~127) 10.0.0.0~10.0.0.127

IP 10.0.0.128/25
Subnet Mask 255.255.255.128
(ip 128~255) 10.0.0.128~10.0.0.255

36. 사설IP는

3. Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0	–	10.255.255.255	(10/8 prefix)
172.16.0.0	–	172.31.255.255	(172.16/12 prefix)
192.168.0.0	–	192.168.255.255	(192.168/16 prefix)

37. 서버가 공인IP를 가지는 경우

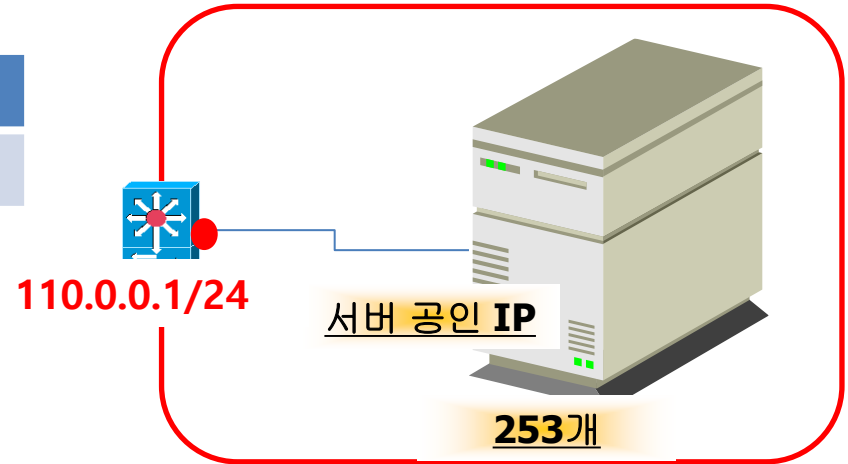
네트워크 할당
서브네팅 하기 public 1개
서버에 공인IP를 할당한다.

할당	서브네팅
110.0.0.0/24	110.0.0.0/24

1
서브네팅 IP
110.0.0.0~10.0.0.255

2
사용불가 IP 3개
0은 네트워크
255는 브로드캐스트
Ip1개는 게이트웨이

$256 - 3 = 253$ 개 IP 사용가능



38. 서버가 사설IP를 가지는 경우

서브네팅 하기 public 1개

서버는 사설 IP, 외부 노출 필요한 서버만 공인IP와 매칭시킴

할당	서브네팅
110.0.0.0/24	110.0.0.0/24
10.0.0.0/24	10.0.0.0/24

1
서브네팅 IP
110.0.0.0~10.0.0.255

2
사용불가 IP 3개
0은 네트워크
255는 브로드캐스트
IP 1개는 게이트웨이

256-3=253개 IP 사용가능



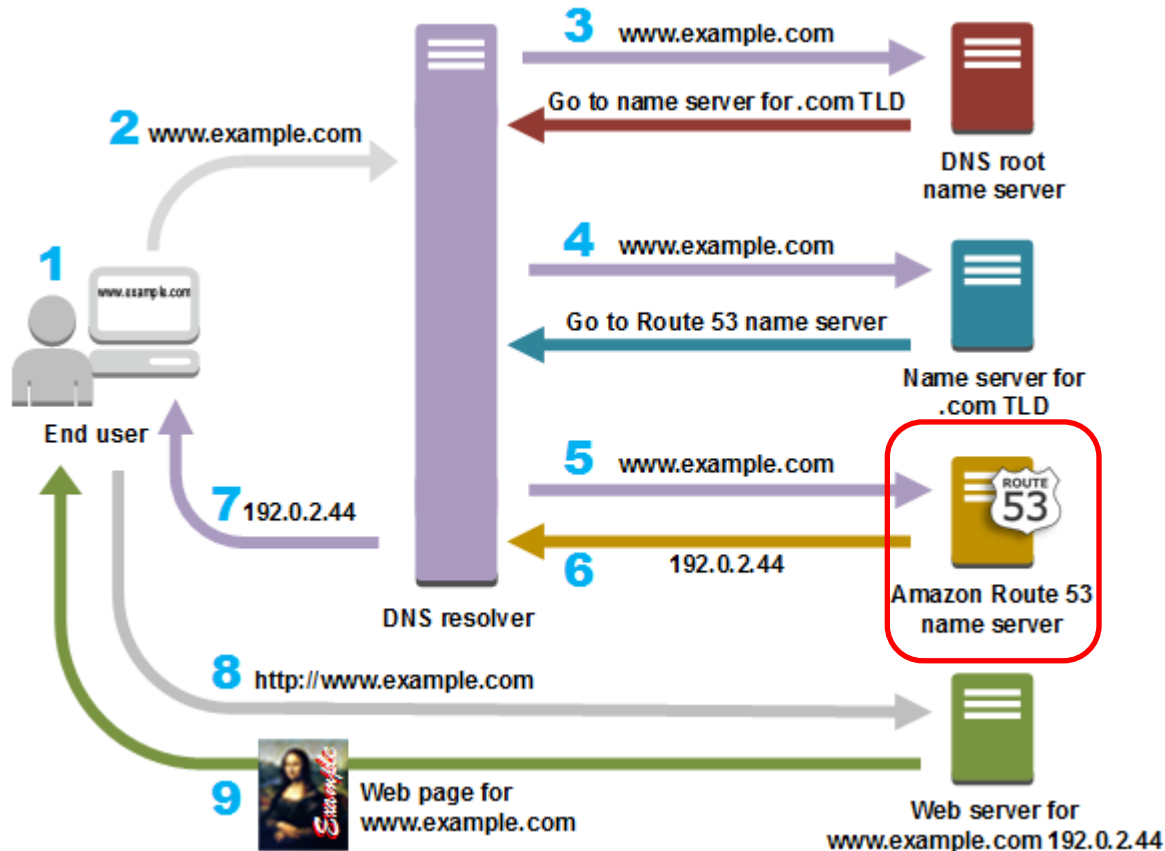
39. DNS 네임서버와 웹서버 IP를 매칭하자

도메인으로 서비스 하자~



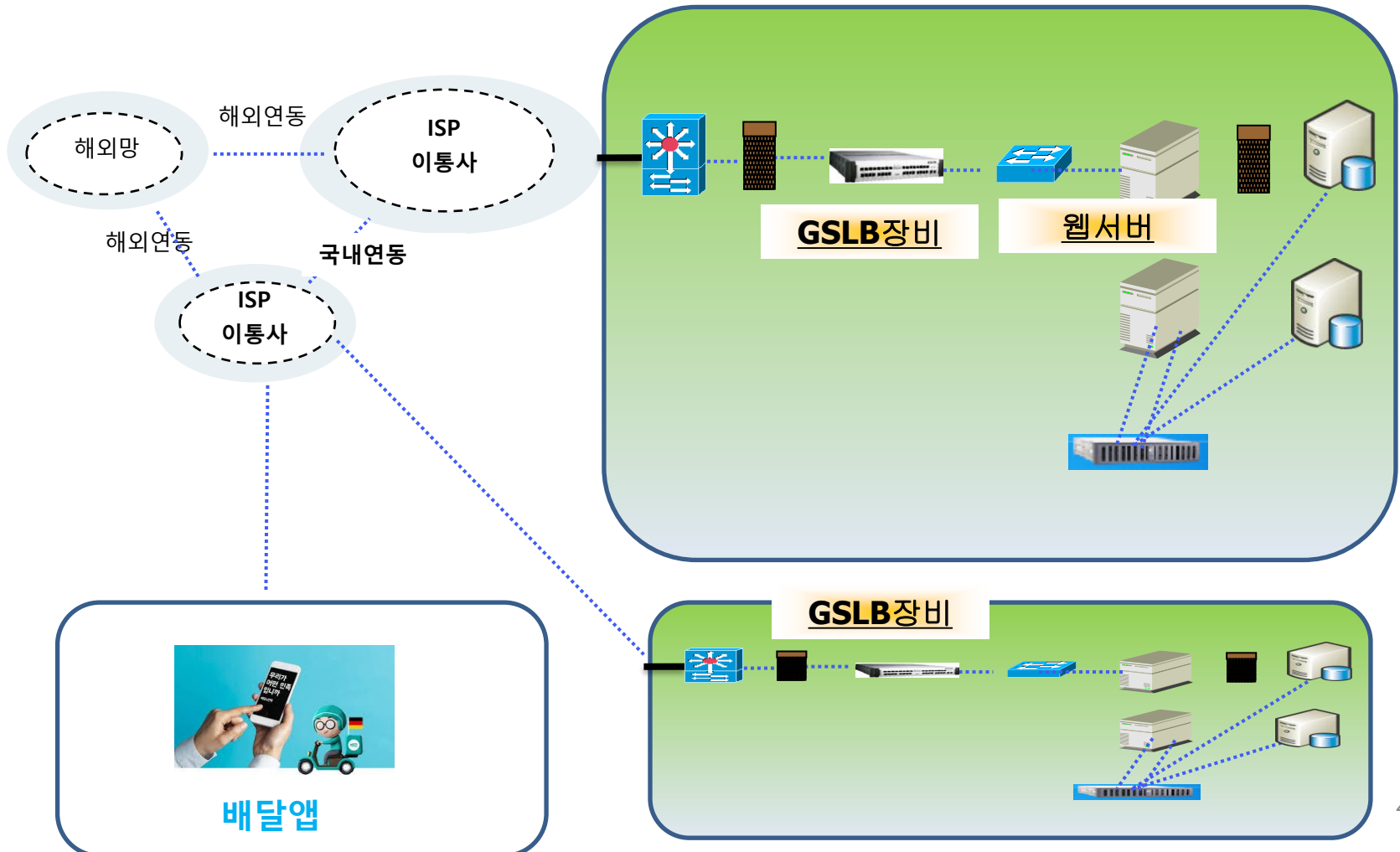
40. DNS (Domain Name Sysetm) 상세

www.facebook.com 을 컴퓨터나 스마트폰 등 여러 디바이스에서 읽을수 있도록 IP로 변경해주는 서비스



41. GSLB 장비로 IDC 이중화 하자

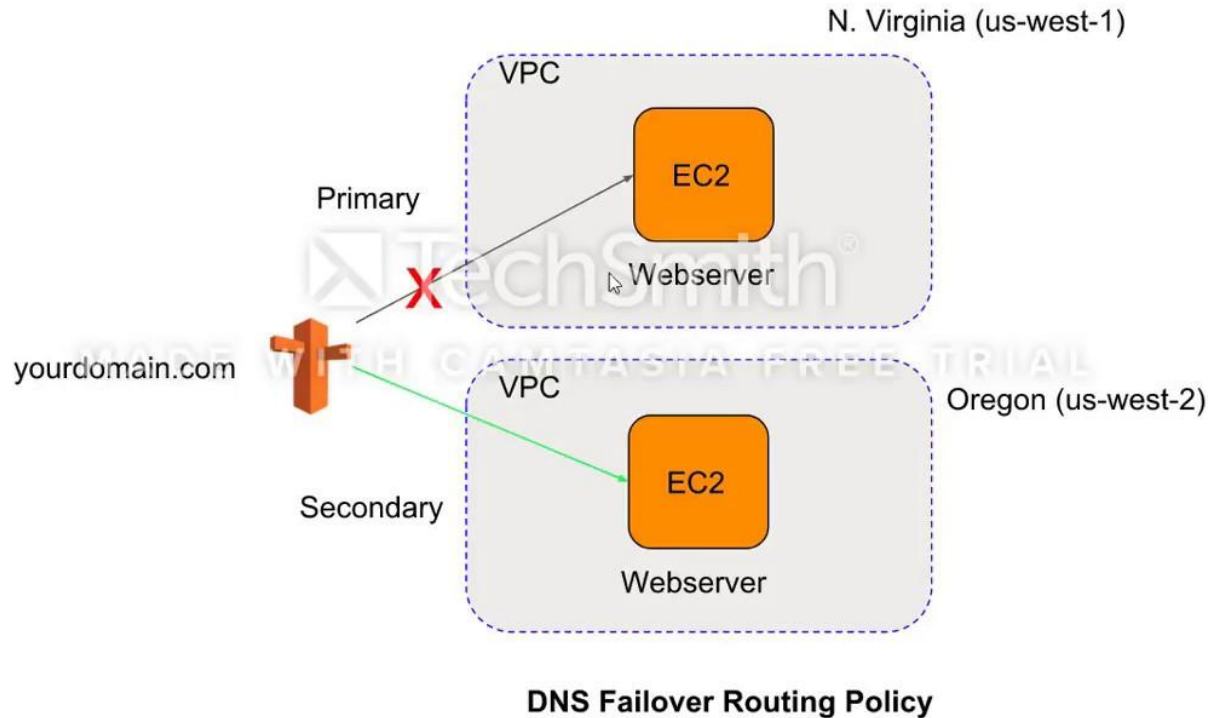
GSLB로 하나의 IDC장애시도 서비스 되도록 하자
Global Server Load Blancer



42. GSLB 장비로 IDC 이중화 하자

GSLB로 하나의 IDC장애시도 서비스 되도록 하자
Global Server Load Blancer

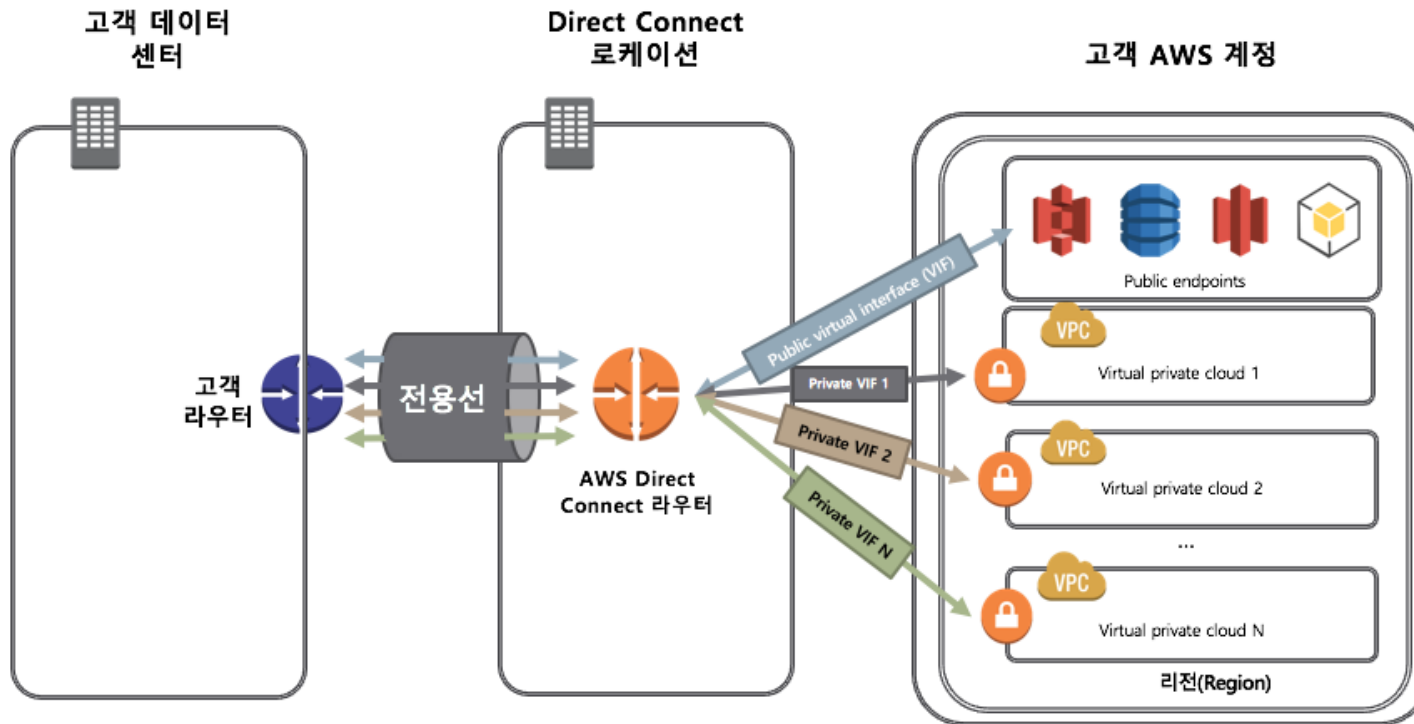
Assignment - DNS Failover across AWS Regions



43. 전용선

원하는 곳까지 물리적인 회선을 연결하는 것이다.

인터넷 통신이 아닌 내부 통신(보안)을 위해 전용선을 연결한다.



44. VPN 연결

전용회선 대체로 많이 사용한다. 인터넷을 이용한 보안 회선 이다.

전용선보다 저렴하다. 트래픽 제한이 있어서 대규모 서비스에는 적합하지 않다.

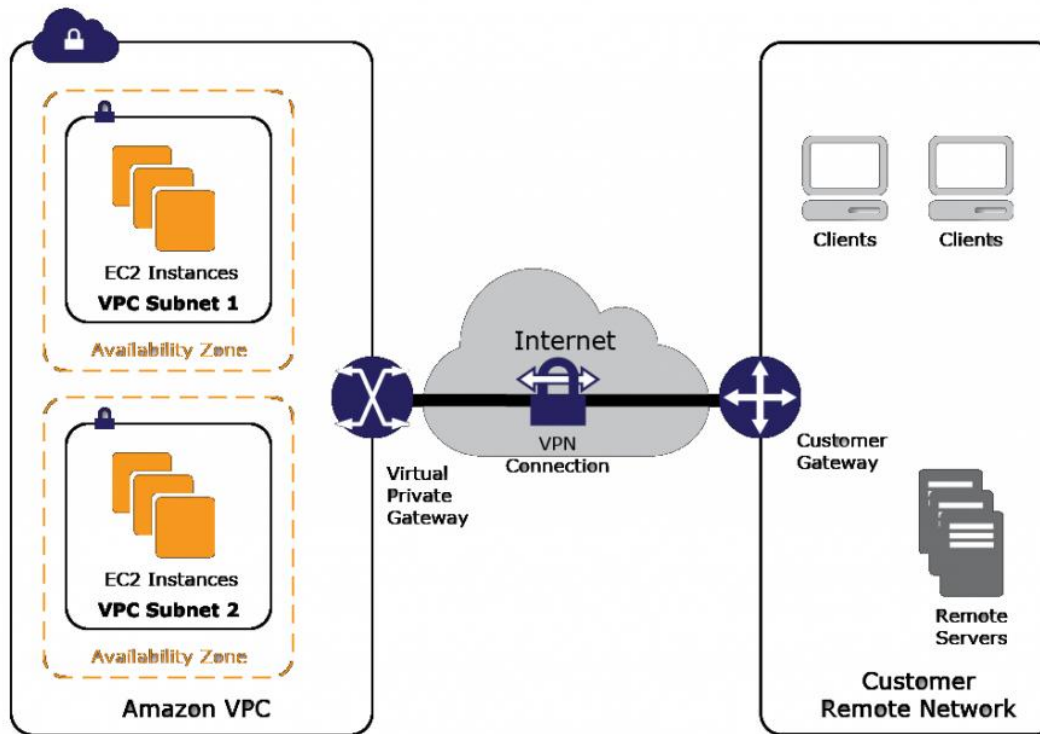


Figure 1: AWS managed VPN



감사합니다.