

모두를 위한

TTFB의 Load Balancer 이야기

- 엘사(L4) 어렵지 않아요 ^^



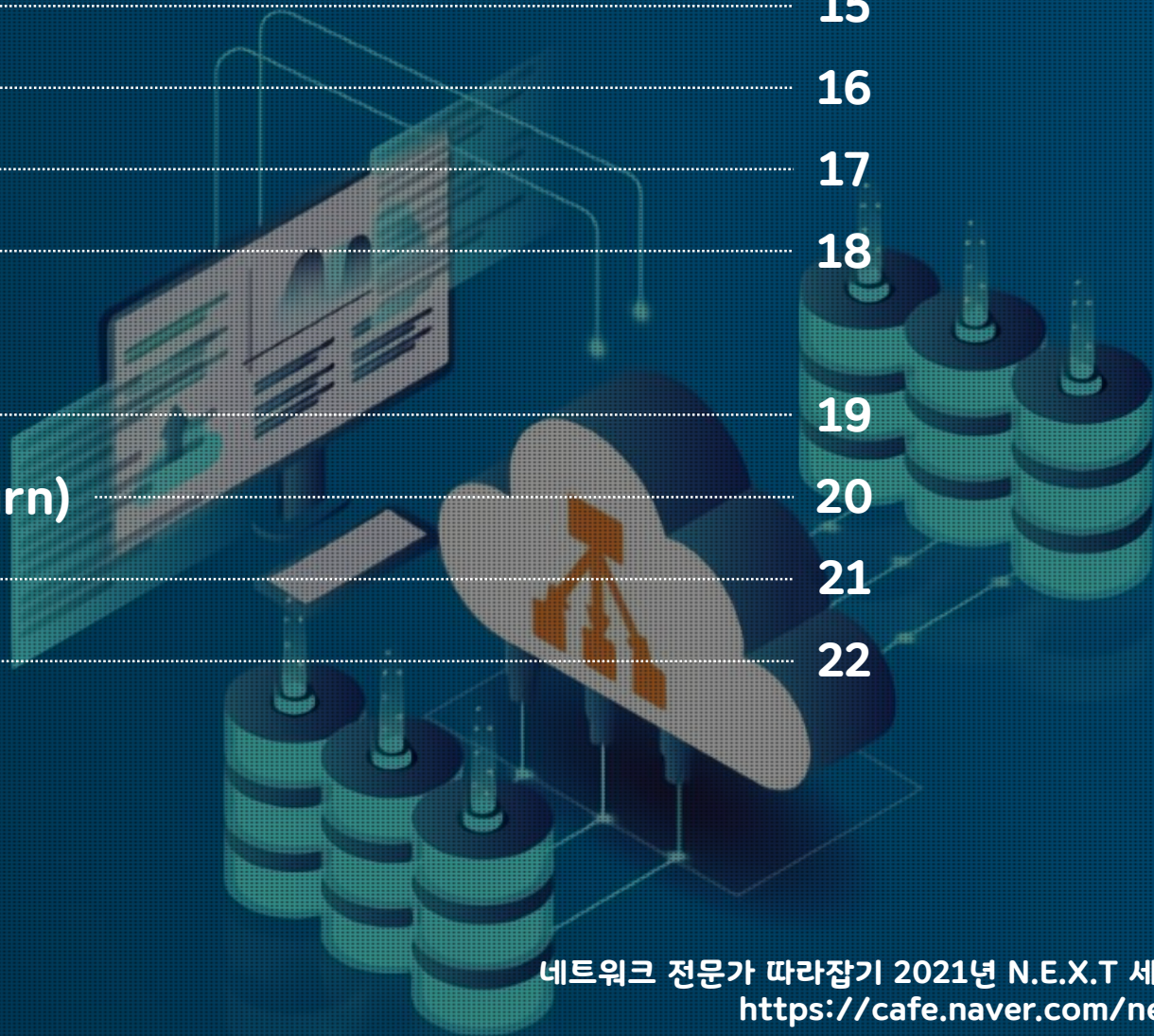
네트워크 전문가 따라잡기 - 29회 - N.EX.T 정기세미나(2021)
<https://cafe.naver.com/neteg>

❄️ AGENDA

1. L4스위치(Load Balancer)의 등장 배경	04
2. 네트워크 장비의 Load Balancing 문제점 / Server의 한계점	05
3. Scale-Up / Scale-Out	06
4. Load Balancing이란?	07
5. L4스위치의 Transaction	08
6. 기존 환경의 한계	
: 구성의 문제점	09
: 서비스의 문제점	10
7. ADC(Application Delivery Controller)란?	11
8. ADC(Application Delivery Controller)의 기능	12
9. ADC의 Transaction	14

❄️ AGENDA

10. Proxy란	15
11. Proxy의 종류	16
12. SLB에 필요한 정보	17
13. 부하분산 방식(LB Method)	18
14. One-Arm? In-Line?	
: One-Arm Mode(Proxy)	19
: One-Arm Mode(Direct Server Return)	20
: In-Line Mode	21
15. Load Balancer의 사용 범위	22



L4스위치(Load Balancer)의 등장 배경



2000년 초반 인터넷 사용자 폭발적 증가

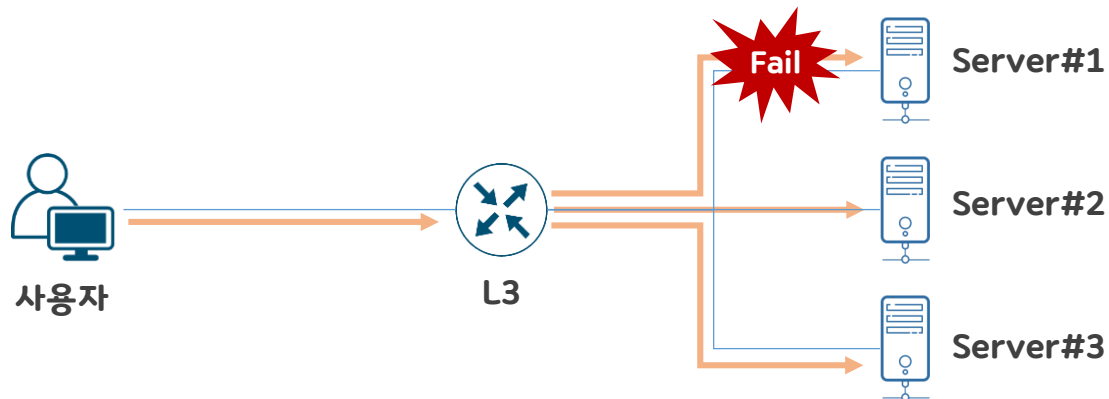
서비스 콘텐츠와 Application의 증가로 인해 서버의 업무 처리량 폭주 (이미지, 스트리밍, PHP, ASP, JSP, CGI, Perl 등..)

인터넷 서버, 방화벽, 캐시 서버 등 트래픽 균형 조절 요구

빠르고 안정적인 서비스를 위해, 높은 대역폭 및 전문 기술 엔지니어 필요 및 수요 발생

네트워크 장비의 Load Balancing 문제점 / Server의 한계점

네트워크 장비에서 Load Balancing 수행 시 문제점



- L3장비에서 SLB대상인 Real Server로 Health Check 제한적
예) ICMP Check
- ICMP가 정상적으로 응답한다고 해서 서비스가 정상인지 아닌지 판별 불가

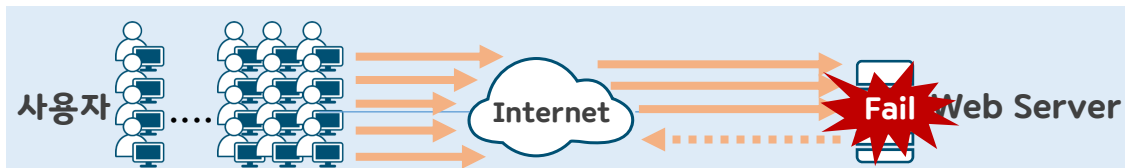
Server에서의 한계점

- 사용자가 한 명 또는 두 명인 경우 서버가 한대라면?



: 사용자의 요청 값에 대해 서버가 정상적으로 응답해 줌

- 사용자가 수백명 / 수천명인 경우 서버가 한대라면?

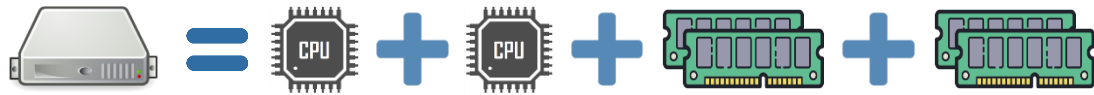


: 서버가 모든 사용자에게 응답을 해주려고 하지만 결국엔 서버의 부하로 서비스 이슈 발생

한계점을 극복하기 위해 서버의 성능을 향상 시키는
Scale-Up / Scale-Out이라는 아키텍처 등장!

Scale-Up / Scale-Out

Scale-Up



- 서버에서 CPU나 RAM등을 추가하여 서버의 성능을 향상하는 방법

장점

- 제어가 힘들거나 분할 구성이 어려운 복잡한 서비스를 처리할 수 있음

단점

- 서버 한 대에 모든 부하가 집중되므로 장애 시 영향을 크게 받을 수 있음
- 성능을 향상시키는데 한계가 있으며, 비용 증가 발생

Scale-Out



- 서버의 수를 늘려 처리 능력을 향상하는 방법

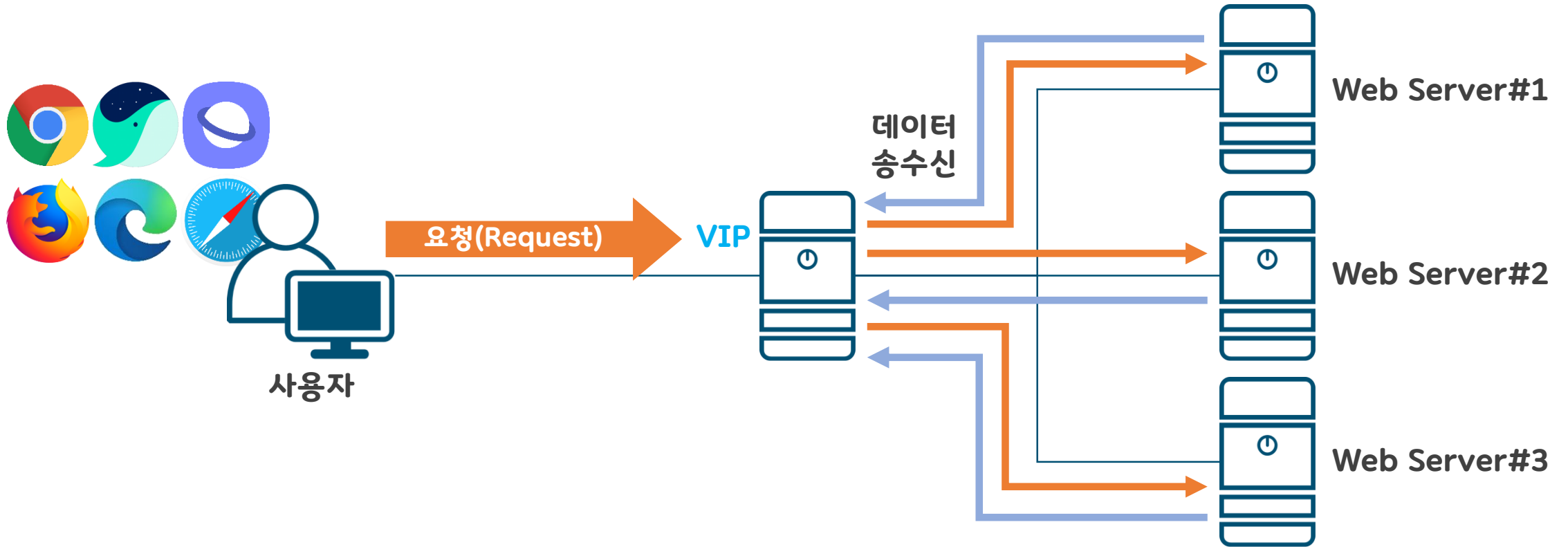
장점

- 하나의 장비에서 처리하던 일을 여러 장비에서 나눠서 처리
- 적은 비용으로 시스템 확장 가능

단점

- 모든 서버가 동일한 데이터를 가지고 있어야 함 (데이터 정합성)
- 여러 대의 서버를 균등하게 분산하기 위해 로드밸런싱을 해야 함

Load Balancing이란?



사용자의 요청(Request)를 여러 대의 서버로 균등하게 부하분산(Load Balancing)처리

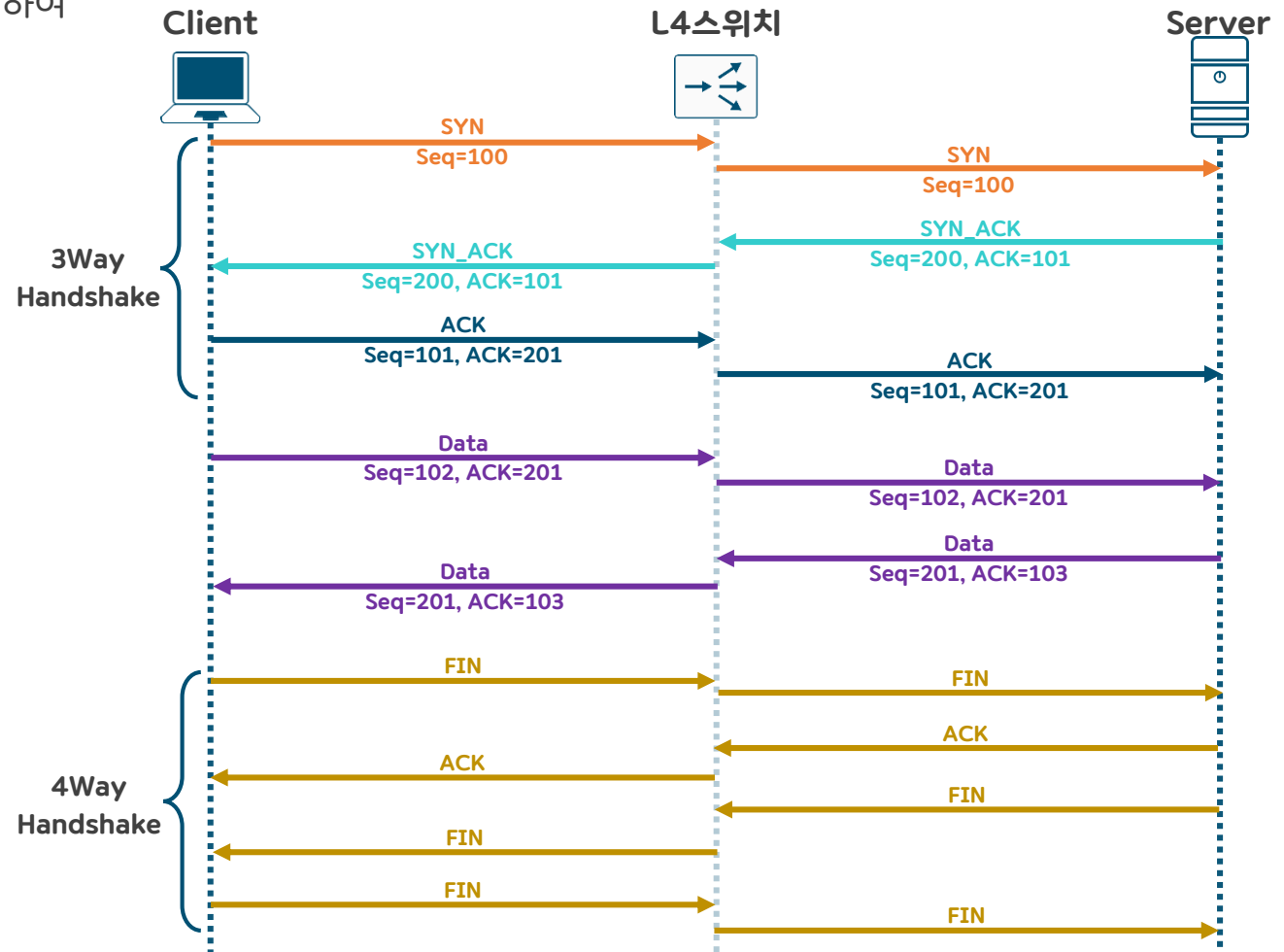
대표적인 장비 : L4스위치 / L7스위치(Application Delivery Controller)

L4스위치의 Transaction

L4스위치

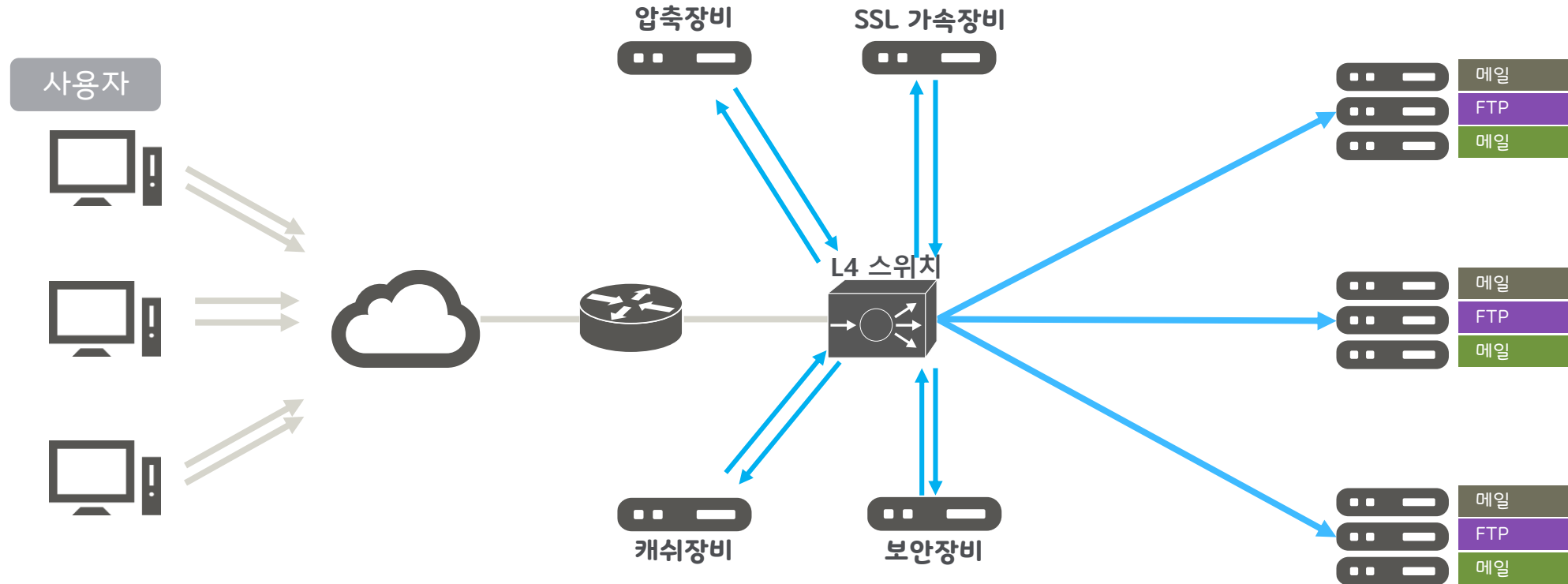
- OSI Layer 3~4에 속하는 IP주소 및 TCP/UDP 포트 정보를 참조하여 스위칭 하는 장비
- Server의 부하분산을 위해 사용되며, 세션들을 관리

OSI 7 Layer	TCP/IP Layer	Protocol
Application	Application	FTP(21) TELNET(23) SMTP(25) DNS(53) TFTP(69) SNMP(161)
Presentation		
Session		
Transport	Transport	TCP/UDP
Network	Internet	IP/ICMP ARP/RARP
Data Link	Network Access	Network Interface
Physical		



기존 환경의 한계

구성의 문제점



Result : 고비용 복잡성 속도저하 확장의 어려움

기존 환경의 한계

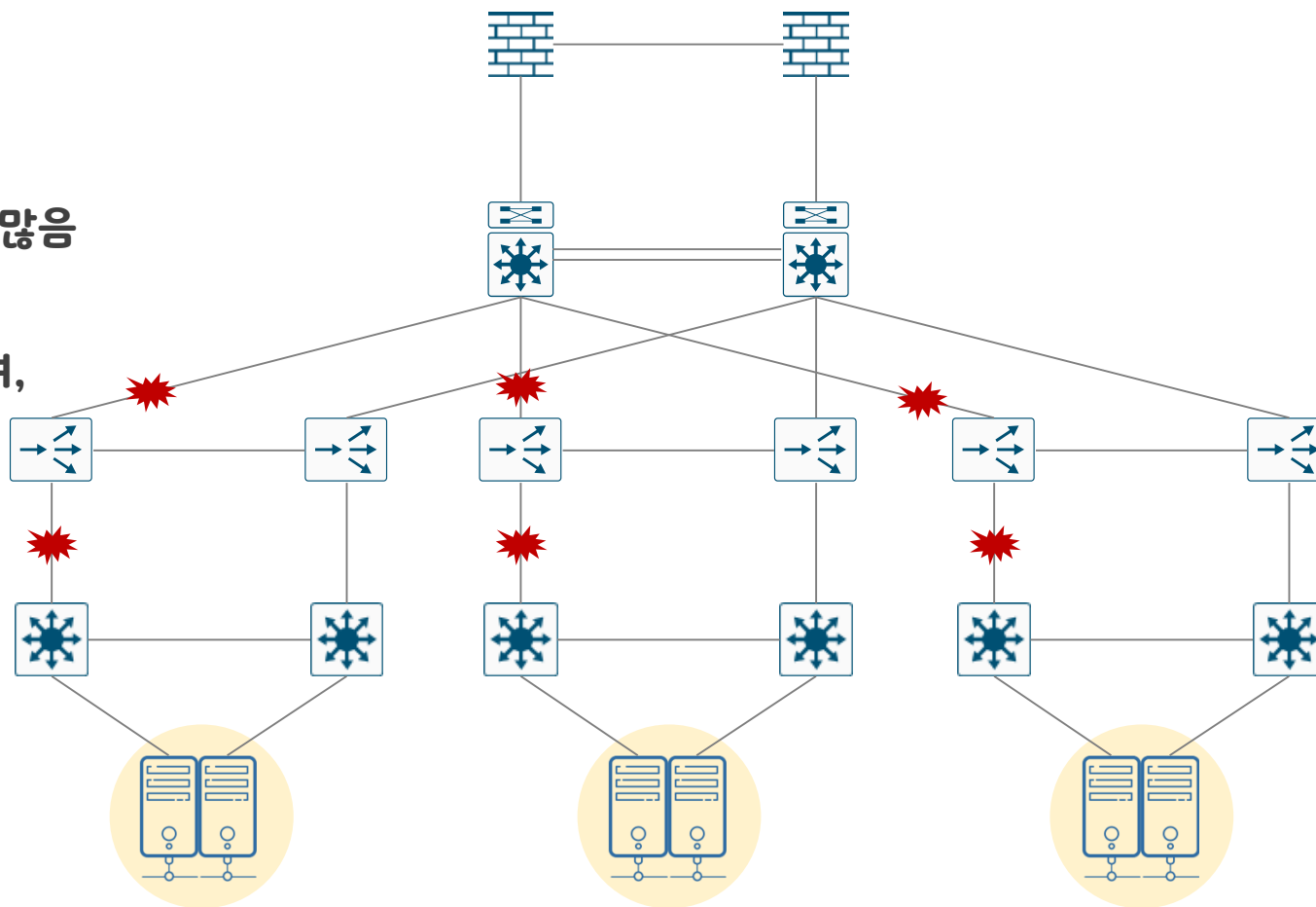
서비스의 문제점

SSL Traffic을 서버에서 처리하므로, 보안에 취약

타 장비와 호환성 검토가 필요
L4 구성 변경 시 단절 절차가 복잡하면 고려사항이 많음

장애가 발생하면 STP(Looping 구간)존재로 인하여,
Failover시 서비스 간헐적 단절 발생

관리 및 장애 관리할 포인트가 많아짐



ADC(Application Delivery Controller)란?

ADC는 어디서 근원이 되었을까?



- **F5 Networks(본사 : 미국 시애틀)**에서 시작 및 2008년부터 Gartner에서 ADC로 정의 및 용어 사용
- 이전에는 “L7스위치” 라고 불림

Gartner의 ADC 정의

일반적인 ADC정의

- Layer 4 through Layer 7 redirection and load balancing and failover
- TCP Connection Multiplexing
- Server offload (for example, SSL termination and TCP connection management)
- Data compression
- Network address translation
- Network level security functions, distributed DoS(Denial of Service) protection and server cloaking
- Compression
- Caching

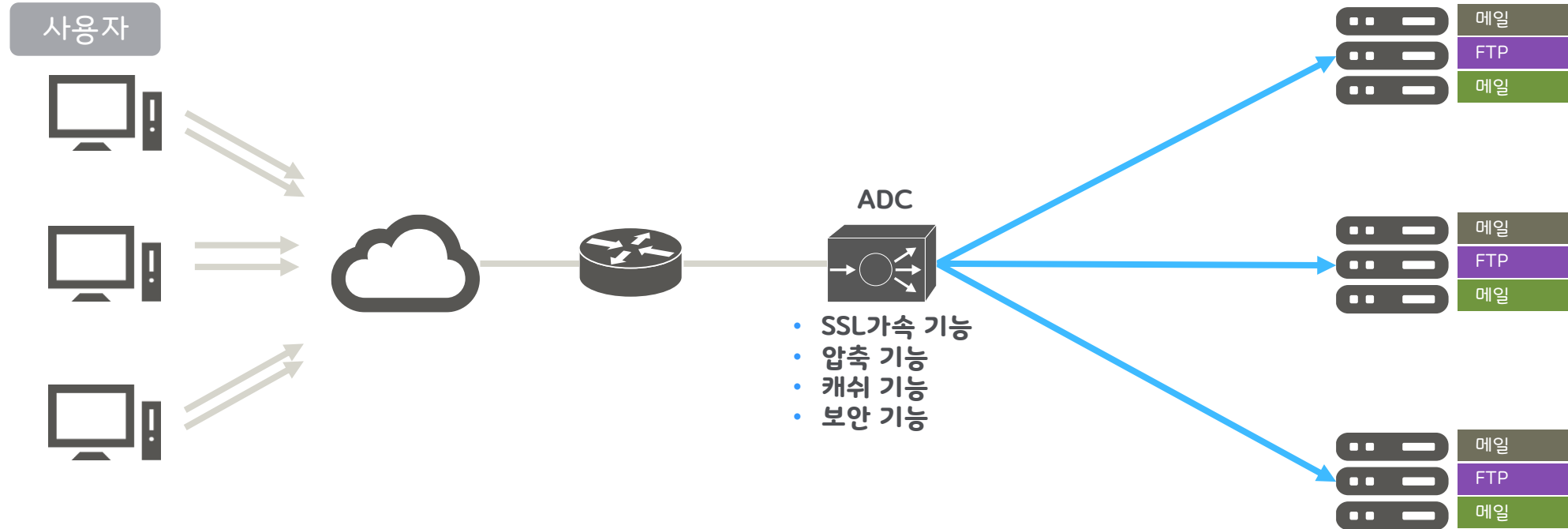
Advanced ADC정의

- Application layer proxy, which is often bidirectional and stateful
- Content transformation
- Adaptive compression
- Selective caching of dynamic content
- HTML or other application protocol optimizations
- Web application firewall
- XML validation and transformation
- Rules and programmatic interfaces

Major Vendor Product

Citrix : ADC(Netscaler) Product / F5Networks : BIG-IP Product

ADC(Application Delivery Controller)의 기능



Result : 비용절감 네트워크 구조 단순화 확장성 확보

ADC(Application Delivery Controller)의 기능

ADC(L7스위치)

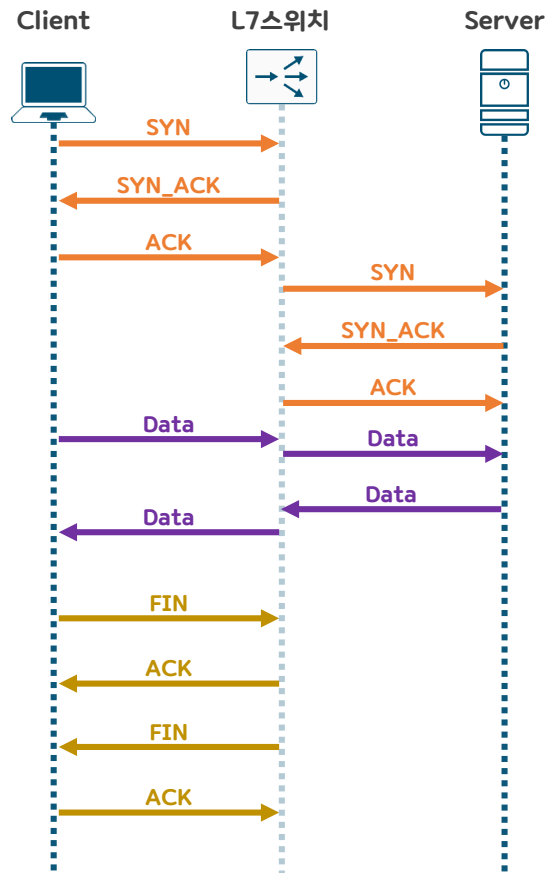
- IP, Port 정보 뿐만 아니라 URL정보, Cookie, Payload 정보 등을 이용한 Packet스위치
- L4스위치와 달리, Compression(압축), 캐싱(Cache), 가속(Offloading), 보안(DDoS/SYN or GET Flooding)기능 등이 포함되어 있음.

OSI 7 Layer	TCP/IP Layer	Protocol
Application	Application	FTP(21) TELNET(23) SMTP(25) DNS(53) TFTP(69) SNMP(161)
Presentation		
Session		
Transport	Transport	TCP/UDP
Network	Internet	IP/ICMP ARP/RARP
Data Link	Network Access	Network Interface
Physical		

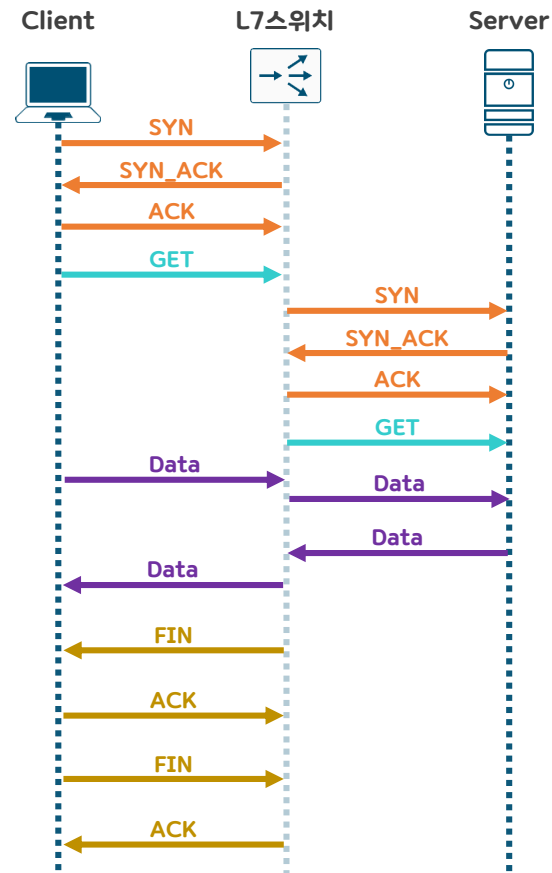


ADC의 Transaction

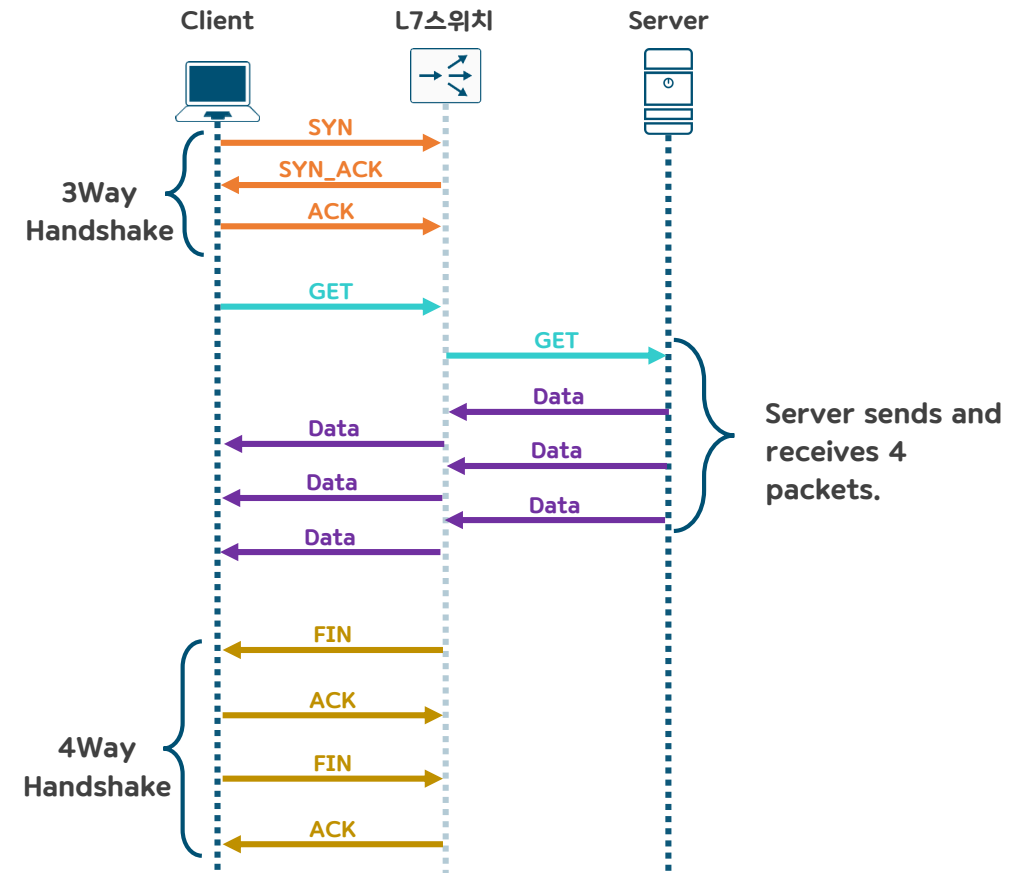
TCP / HTTP Transaction



No idle TCP Transaction



No idle HTTP Transaction



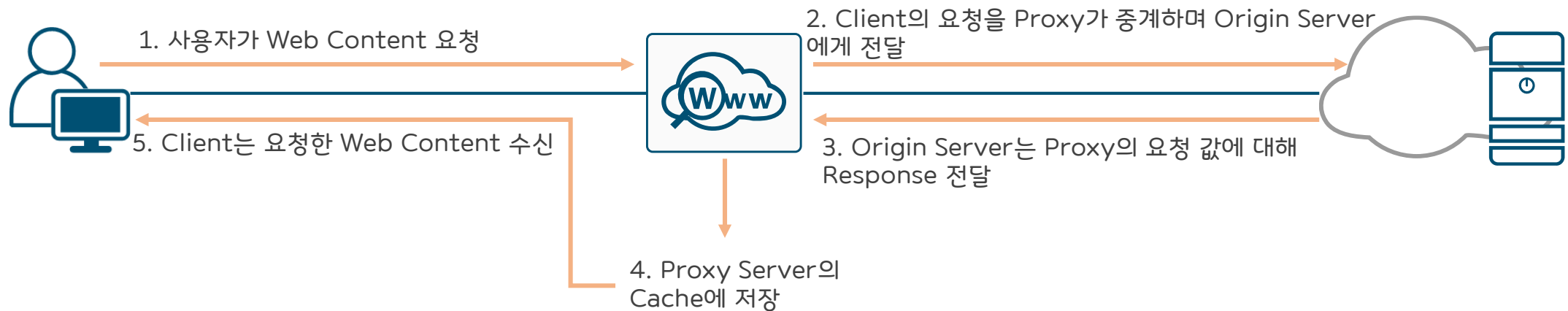
Idle HTTP Transaction

Proxy란?

Proxy란?

Cache를 가지고 있어 Client가 서비스를 요청하면 이를 대신해 수행 및 중계하는 역할

Proxy의 기본 동작



Proxy의 종류

Forward Proxy



- Client의 요청을 Proxy가 대신 인터넷을 통해 Origin 서버로 중계하는 방식
- 인터넷으로 향하는 Source IP는 Proxy IP로 변경되어 전달
- Client IP가 감춰지므로, 서버의 입장에서는 사용자의 정보를 알 수 없음

Reverse Proxy

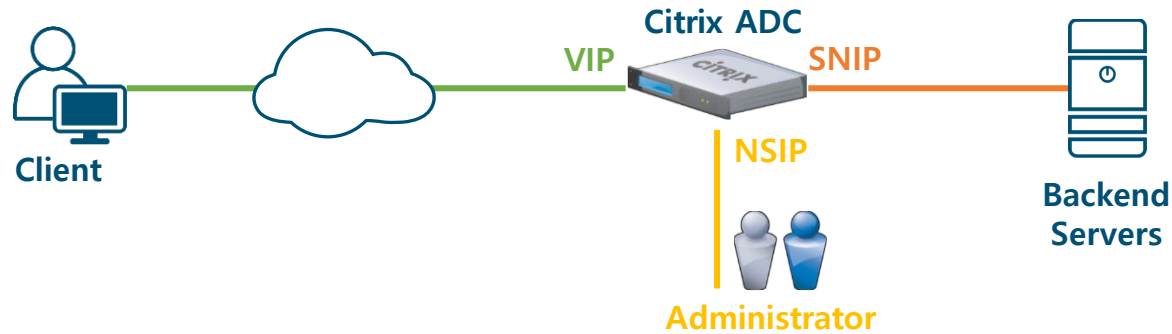


- 외부에 있는 Client가 데이터를 요청하면, Proxy가 이 요청을 받아 내부 서버에서 데이터를 받은 후 Client에게 전달하는 방식
- Client는 내부 서버에 대한 정보를 알 필요 없이 Proxy에게만 요청하면 되므로, 실제 서버 정보를 알 수 없음 (보안 강화)
- Load Balancing 또는 서버 확장에 유리
- ADC(Application Delivery Controller)라고 불리는 대부분의 장비는 Reverse Proxy로 동작

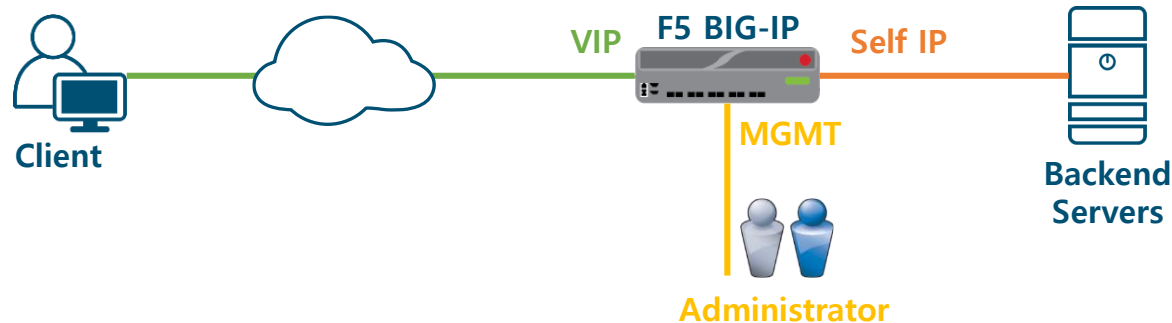
SLB에 필요한 정보

Citrix와 F5 BIP-IP 비교

citrix

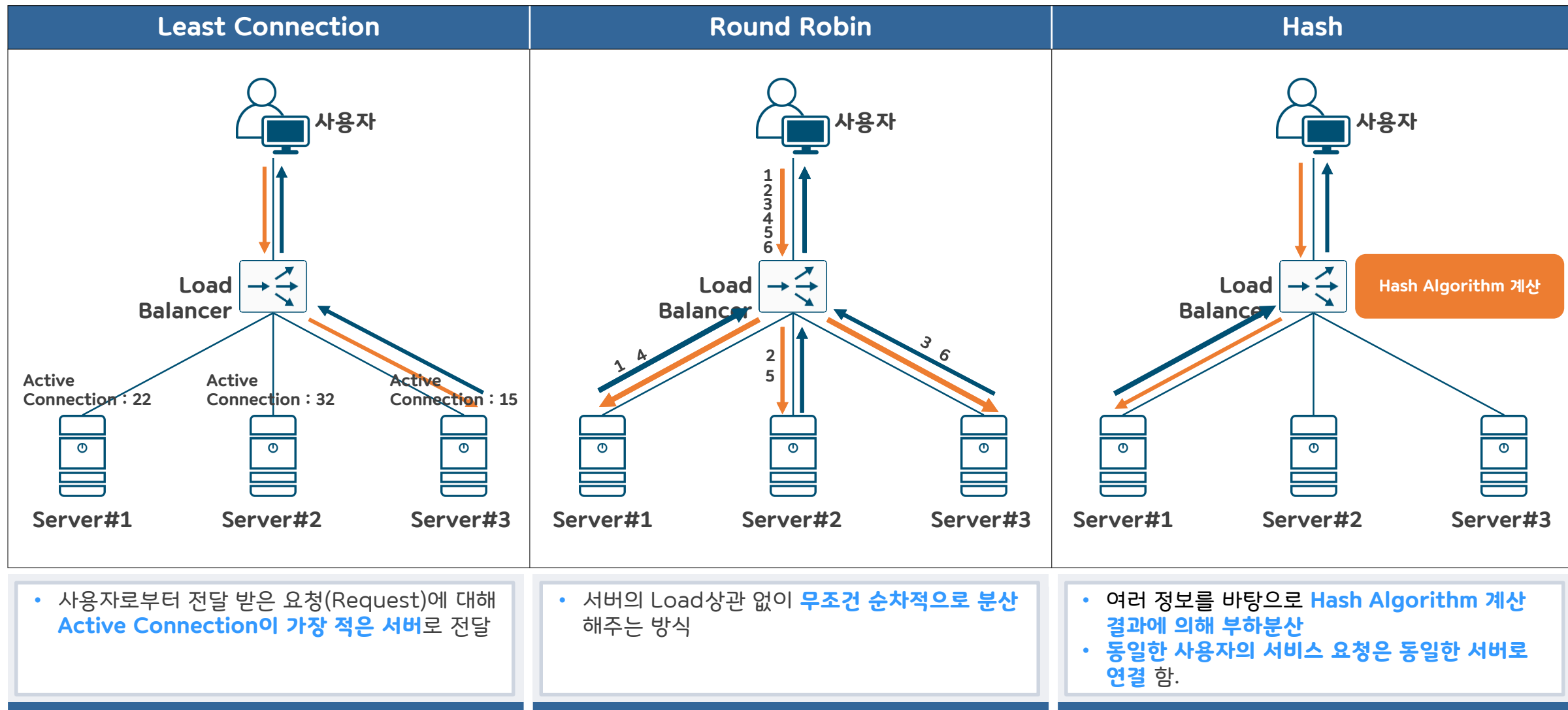


- NSIP(Netscaler IP) : 운영자가 접속하기 위한 IP로 사용
 - VIP(Virtual IP) : Service를 대표하는 IP / Client가 접속하는 IP
 - SNIP(Subnet IP) : Backend Server와 통신을 위해 사용되는 IP
- ※Citrix ADC Lab1 : LoadBalancing <https://youtu.be/wROeNkSZ7cM>



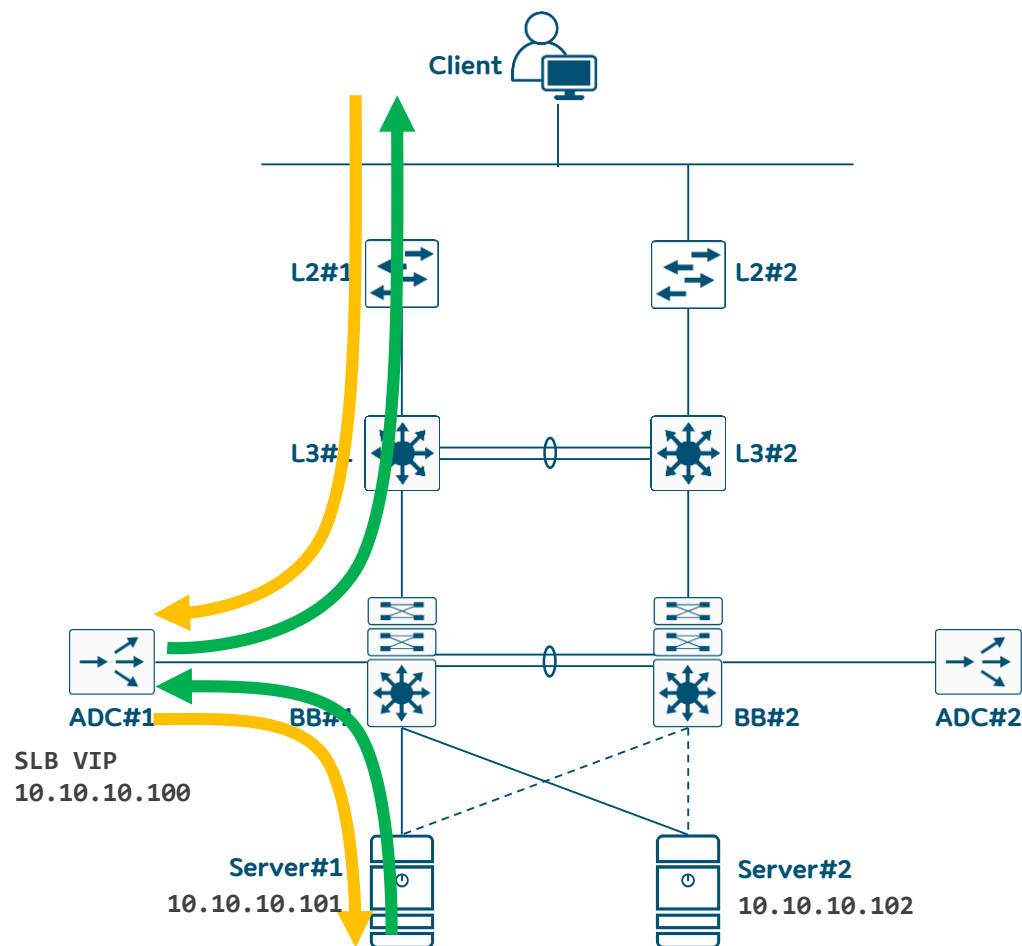
- MGMT : 운영자가 접속하기 위한 IP로 사용
 - VIP : Service를 대표하는 IP / Client가 접속하는 IP
 - Self IP : Backend Server와 통신을 위해 사용되는 IP
- ※ Quick deployment A one armed load balancing configuration (<https://youtu.be/ViC8BL4FbkM>)

부하분산 방식 (LB Method)



One-Arm? In-Line?

One-Arm Mode(Proxy)



장점

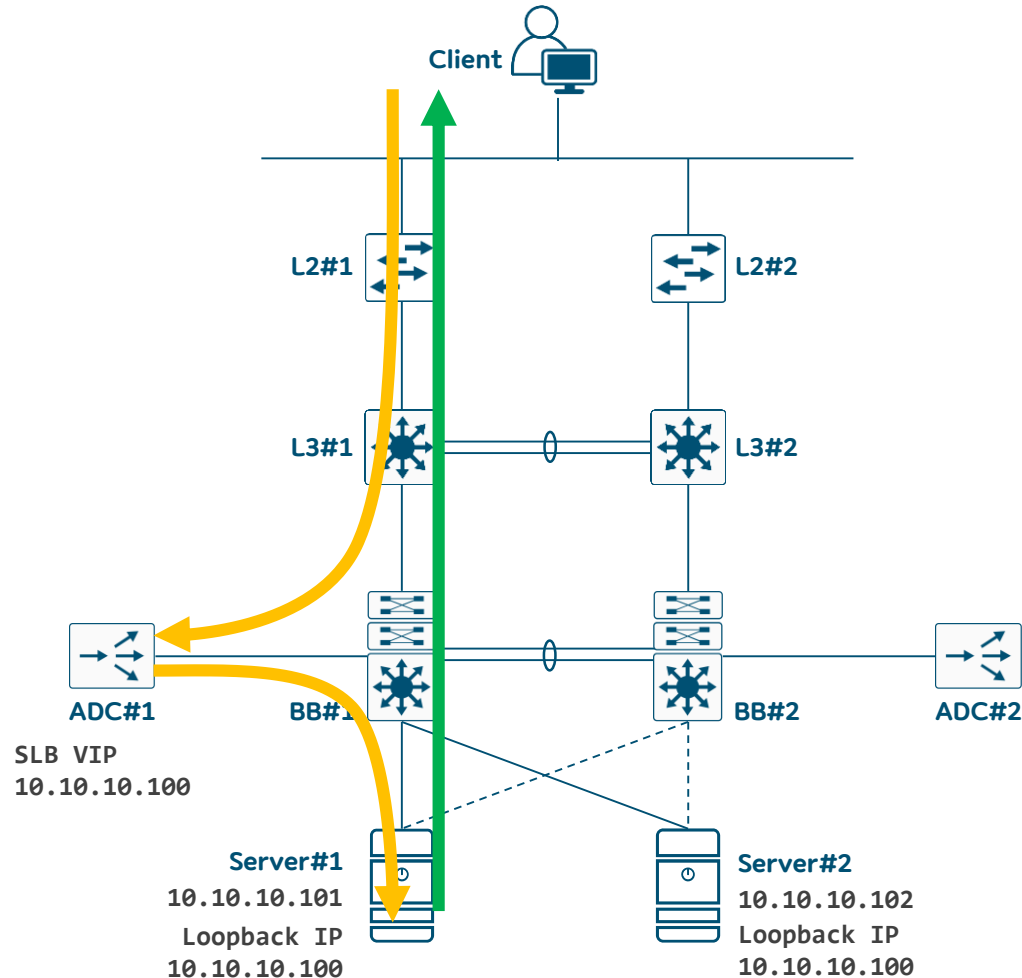
- ✓ TCP Offloading, SSL Offloading 구현 가능
- ✓ Multiplexing 구현 가능
- ✓ Traffic Throughput, Connection등에 대한 상태 정보 확인 가능
- ✓ L7기능 지원 가능

단점

- ✓ TCP Protocol에 대한 Client IP추출 불가능
- ✓ HTTP Protocol의 Client IP 추출 시 HTTP Header 참조 필요

One-Arm? In-Line?

One-Arm Mode(DSR)



장점

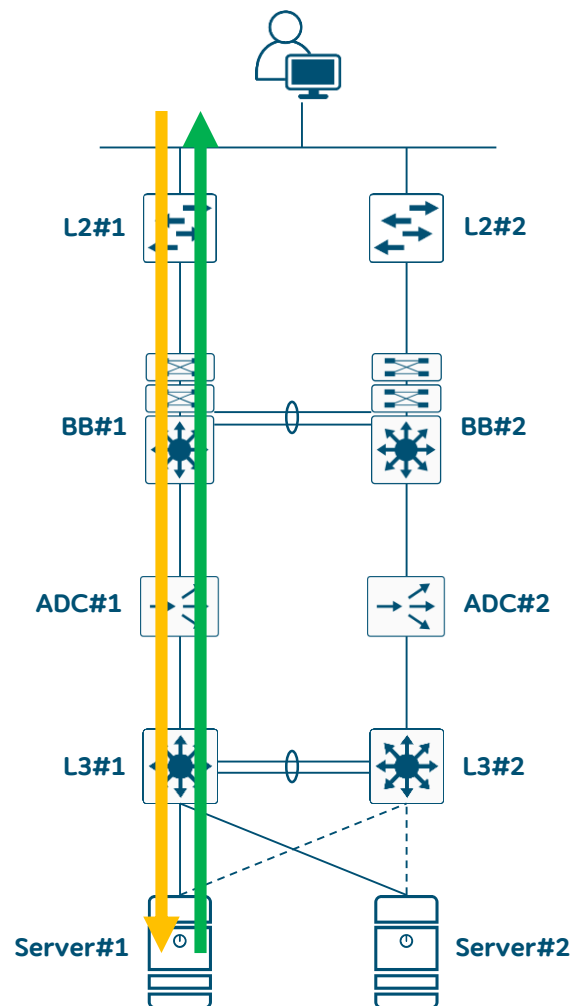
- ✓ TCP Protocol에 대한 Client IP 추출 가능
- ✓ 요청 트래픽(Request)만 Load Balancer로 유입 및 서버에게 전달
- ✓ 스트리밍 서비스처럼 많은 양의 Response가 발생하는 서비스에 유리

단점

- ✓ TCP Offloading, SSL Offloading 구현 불가
- ✓ Multiplexing 구현 불가
- ✓ L7기능 구현 불가
- ✓ Load Balancer에 생성된 VIP의 개수 만큼 서버에서 Loopback Interface를 생성해야 함

One-Arm? In-Line?

In-Line Mode



장점

- ✓ TCP Offloading, SSL Offloading 구현 가능
- ✓ Multiplexing 구현 가능
- ✓ Traffic Throughput, Connection등에 대한 상태 정보 확인 가능
- ✓ TCP Protocol에 대한 Client IP추출 가능

단점

- ✓ Load Balancing의 VIP로 유입되는 트래픽이 아닌 Packet에 대해서도 로드밸런서 장비를 거치므로 트래픽 부하 발생
- ✓ Server와 Load Balancer간 케이블 직결을 권장하지 않으므로, 스위치(L2/L3)가 추가로 필요 (서버가 증설되는 경우, 확장의 어려움)

Load Balancer의 사용 범위

Cloud벤더에서 제공하는 Load Balancer



- Network Load Balancer(NLB)
- Application Load Balancer(ALB)
- Gateway Load Balancer
- Classic Load Balancer



- Application Gateway
- Frontdoor
- Load Balancer
- Traffic Management

K8S, Docker 등의 Modern APP(Micro Service)환경을 위해 제공하는 Load Balancer Component



MetalLB



감사합니다

네트워크 전문가 따라잡기 - 29회 - N.EX.T 정기세미나(2021)
<https://cafe.naver.com/neteg>