



앞서가는 금융기관을 위한 새로운 서비스 아키텍처 디자인

F5 Networks
이진원 부장
JW.LEE@f5.com

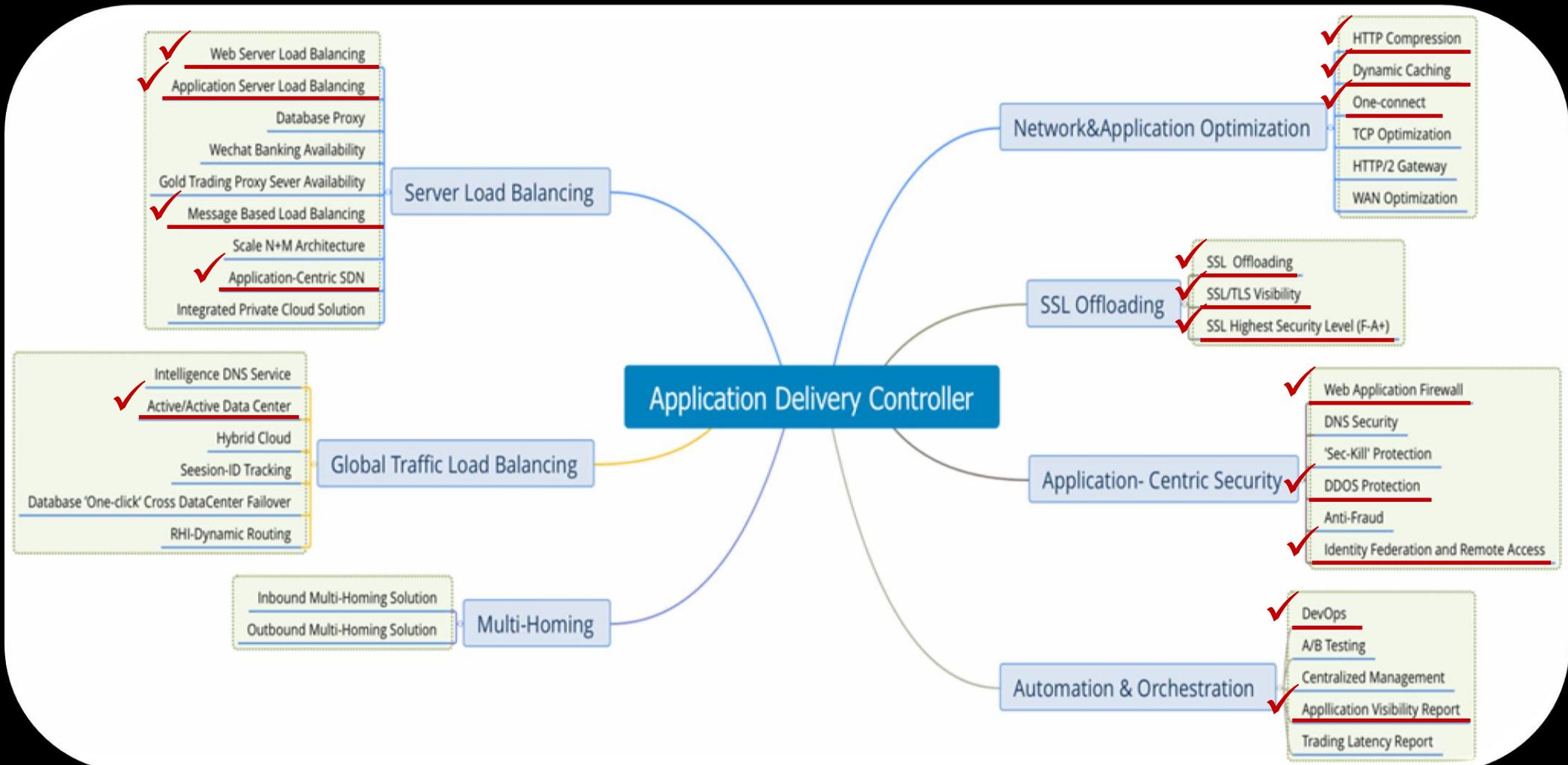
어플리케이션에 대한 향상이 필요합니다.



F5는 어플리케이션을 이해합니다.

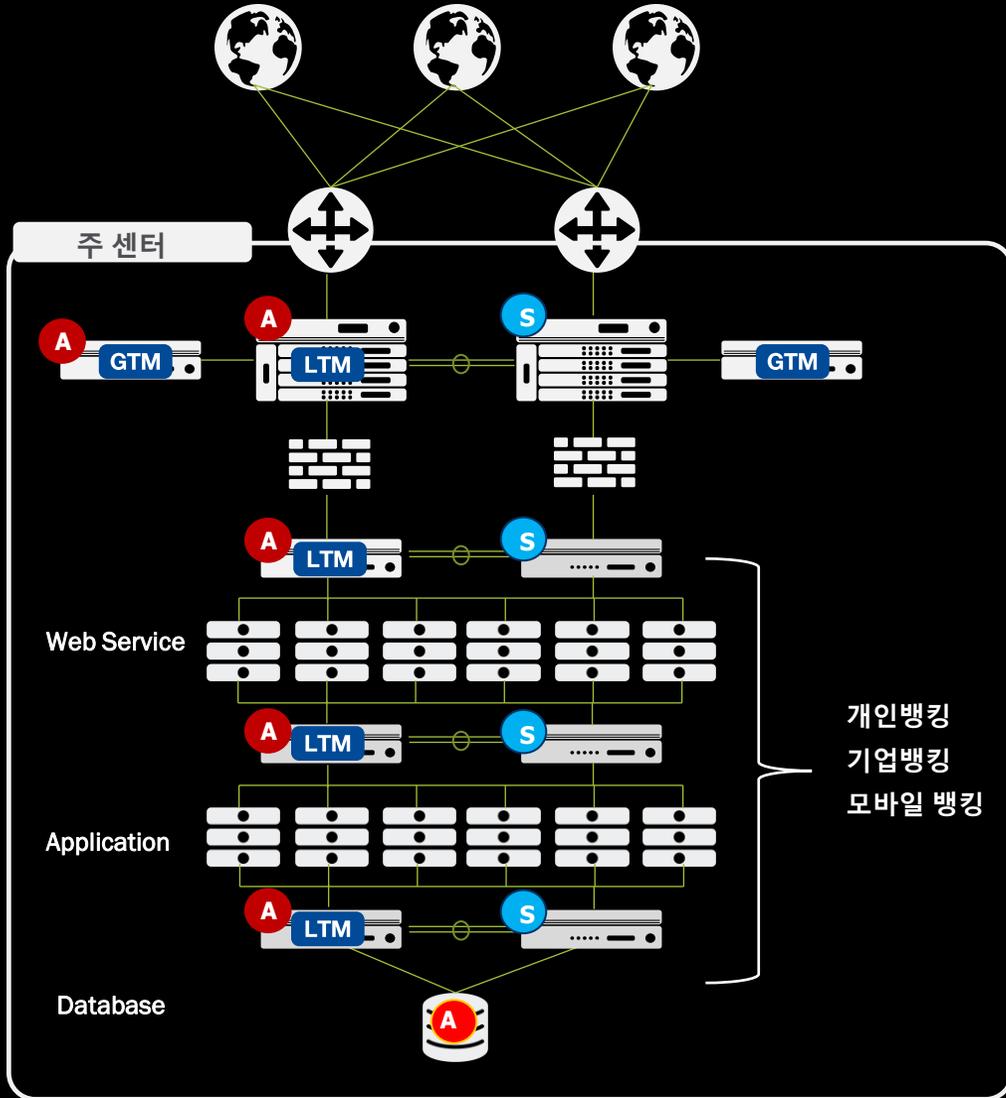


국내 금융기관은 F5를 다음 용도로 사용하고 있습니다.





현 금융기관 서비스 아키텍처

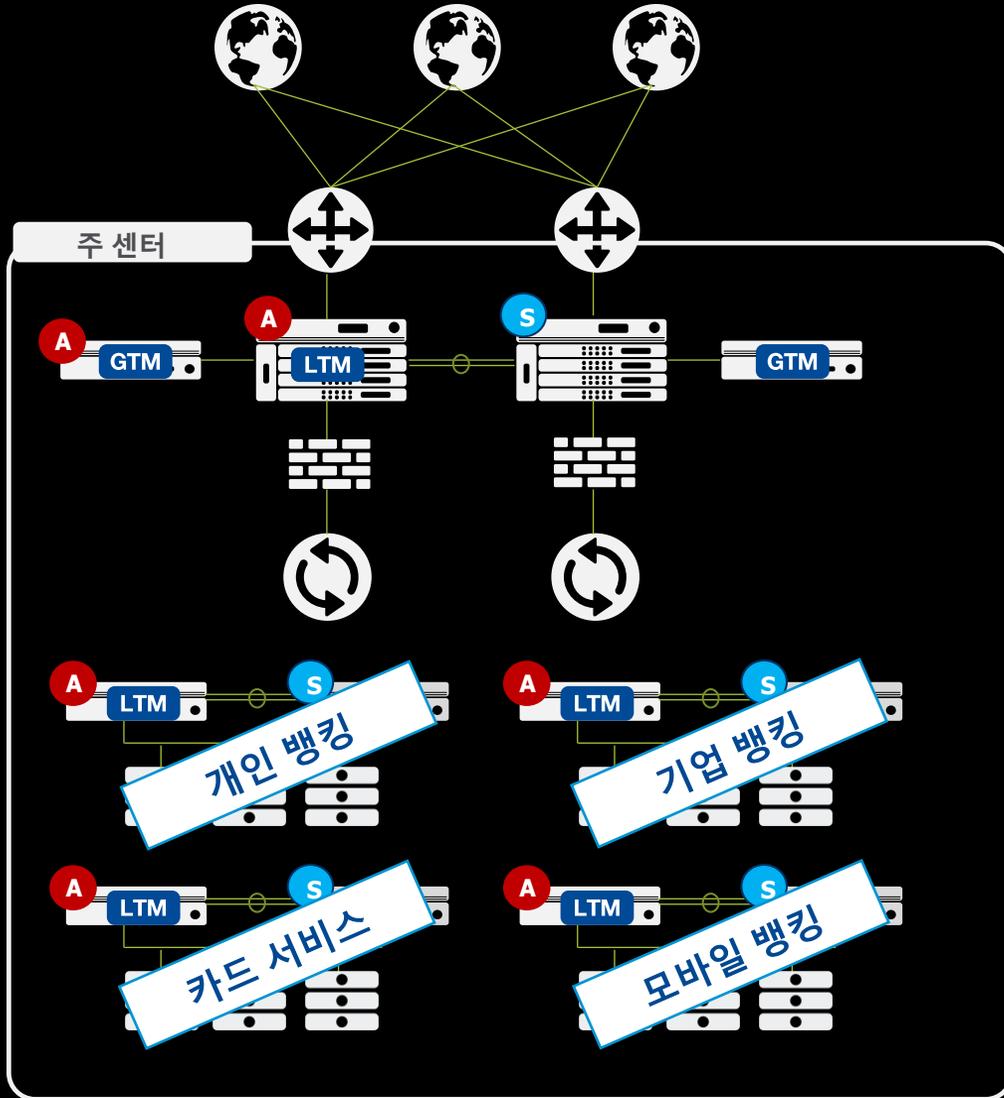


- 중요 서비스를 하나의 ADC에서 수행

- ADC 서비스 장애 시 다른 서비스에 영향

- Active-Active DC 구축 - 주센터/DR센터

금융기관 서비스 아키텍처 구성 사례



- 업무 시스템별 별도 구성(장애 영향 최소화)

- 압축, 캐싱, One-connection L7 고급 기능

- 오픈뱅킹 서비스에 대한 SSL 암복호화 수행

- 업무팀별 관리 업무 분담

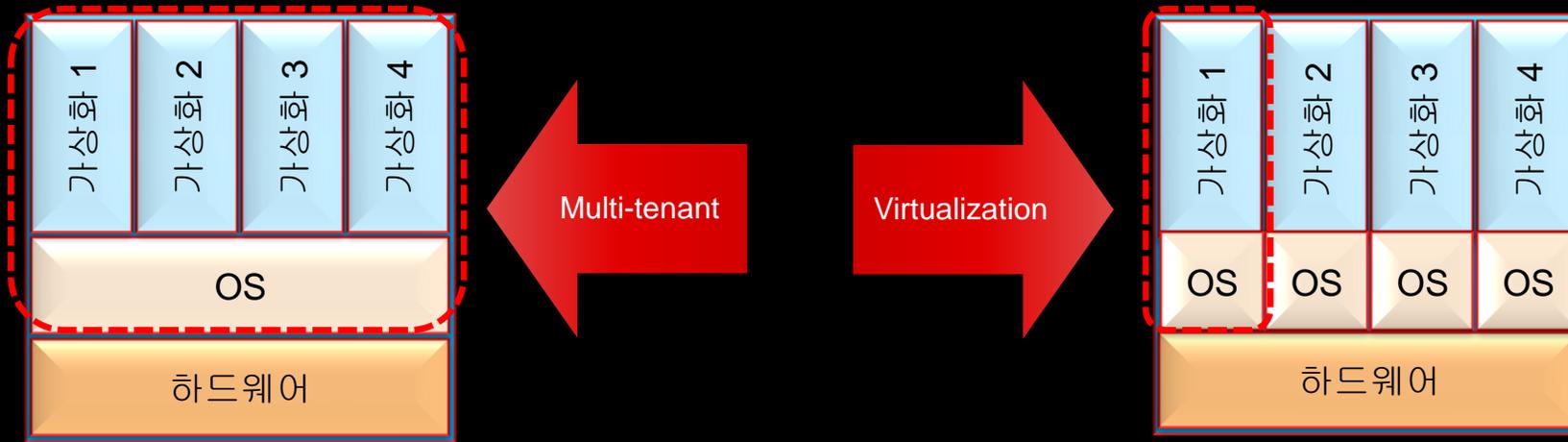
SLA 극대화 서비스 아키텍처

논리적 가상화와 물리적 가상화 차이점

- 고객 요구사항에 따른 가상화 방안

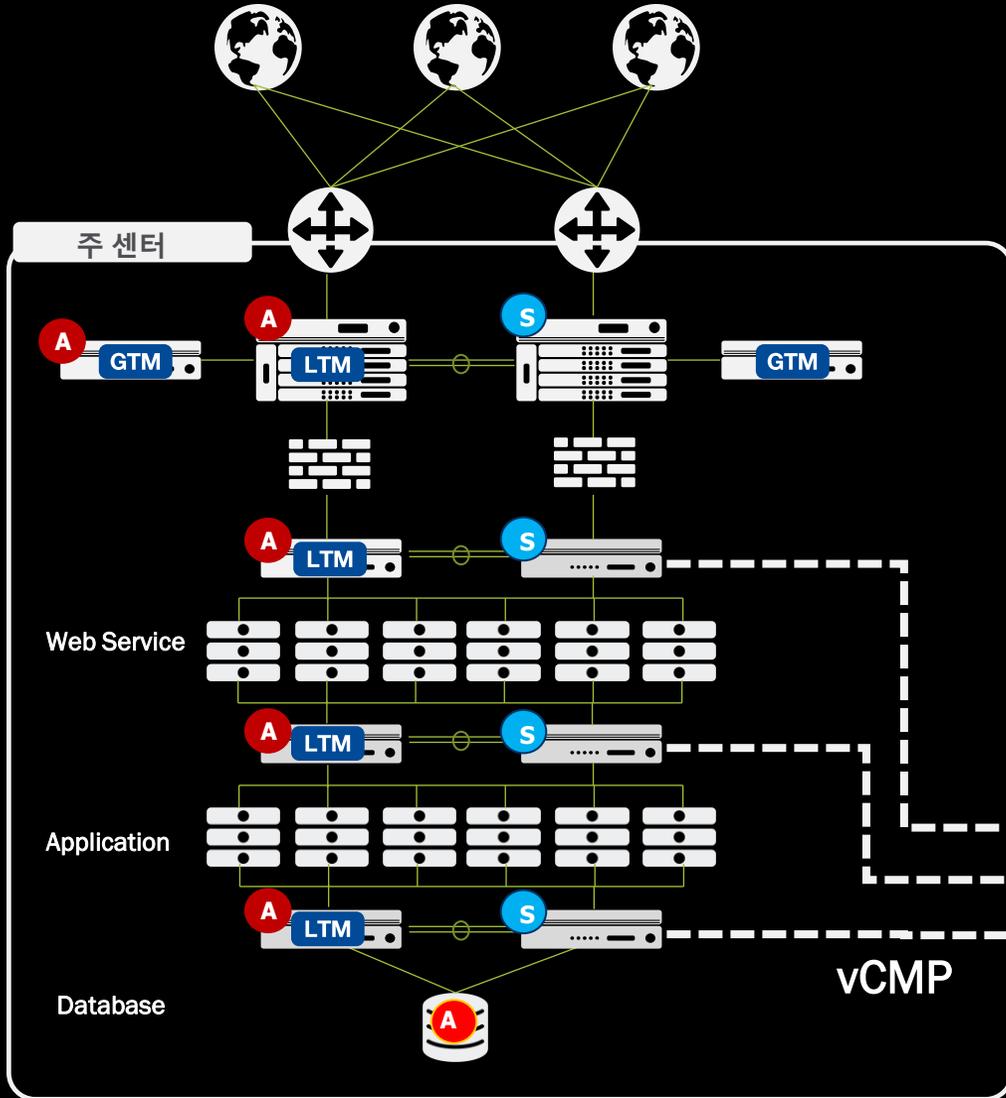
• 공유되어 있는 인프라 통합

• 리소스 사용률 개선



논리적 가상화	멀티 테넌트	물리적 가상화
리소스 공유	유연한 리소스 할당	리소스 할당
OS 기반 가상화	도메인	호스트 별 가상화

SLA 극대화 서비스 아키텍처 방안 1 - 웹 서비스

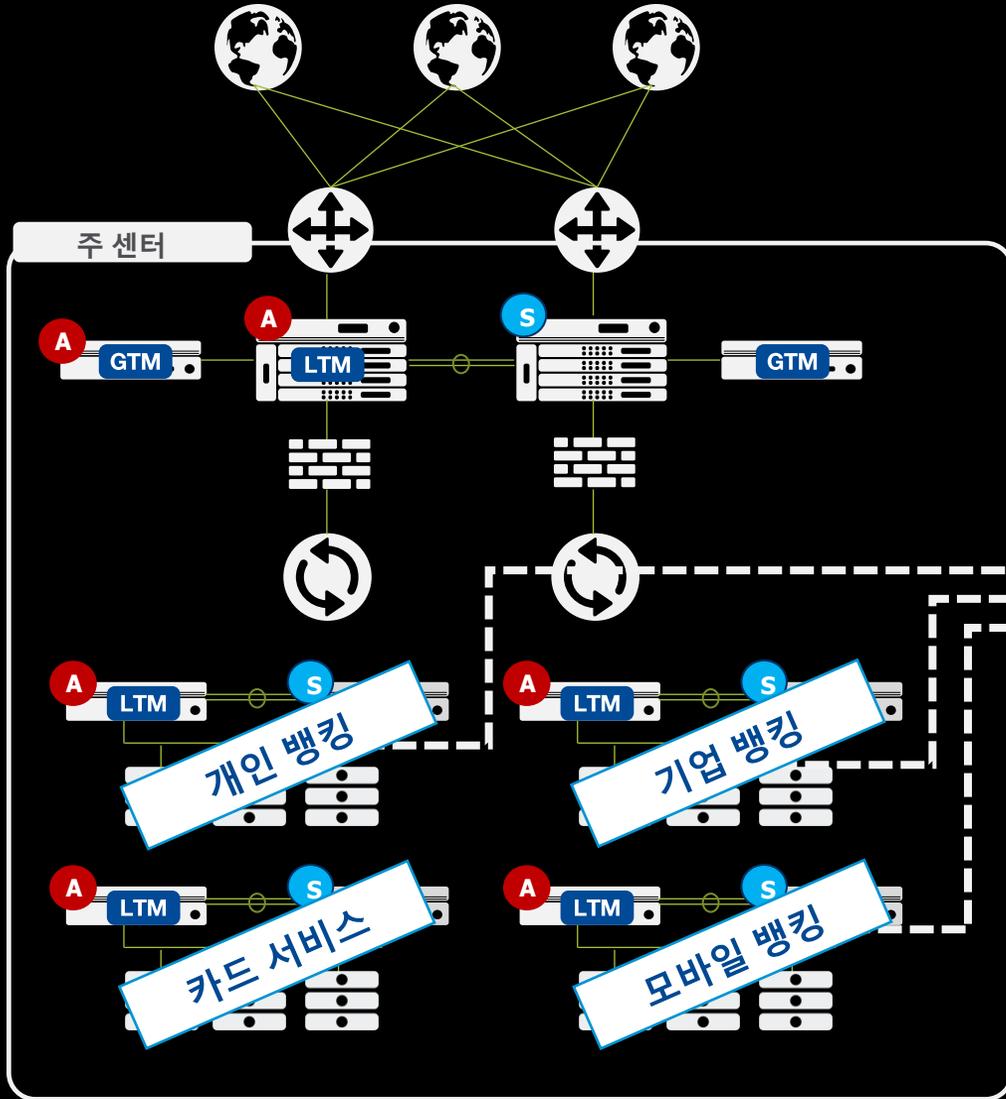


- 완벽한 가상화 호스트 분리
- 물리적 가상화와 논리적 가상화 동시 지원
- DNS 기반 서비스 대상 센터간 이중화 구성



virtual Clustered Multi-Processing

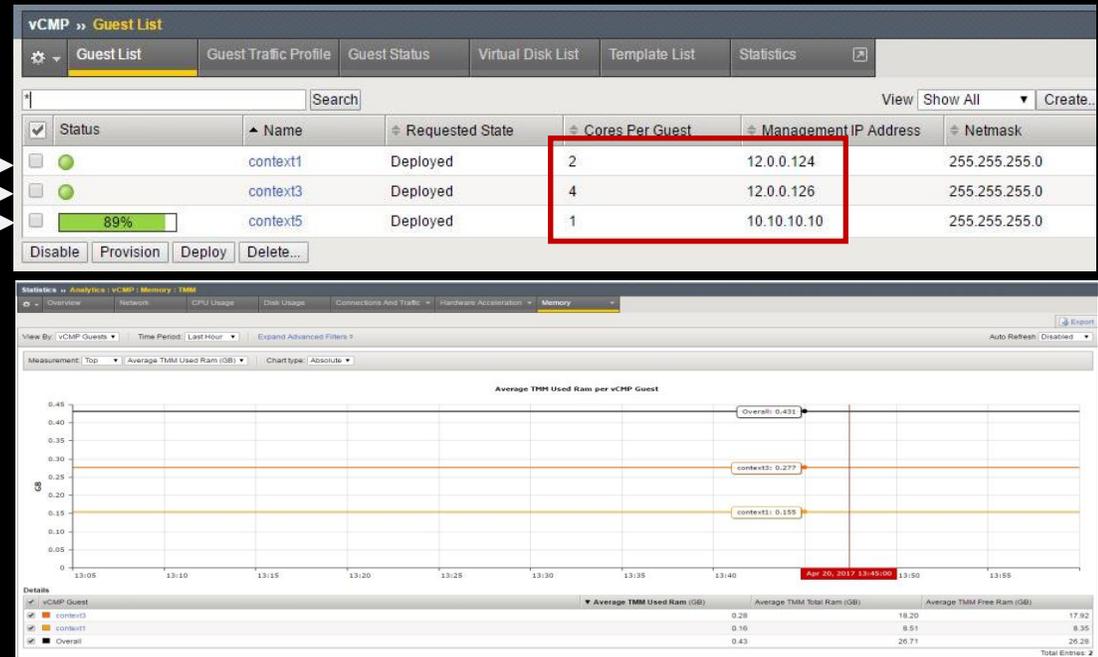
SLA 극대화 서비스 아키텍처 방안 1 – 웹 서비스



- 투자 비용 절감 및 운용 편리성 극대화

- 장비별 별도 OS 운영 및 관리

- 가상 ADC별 리소스 독립적인 운영 보장

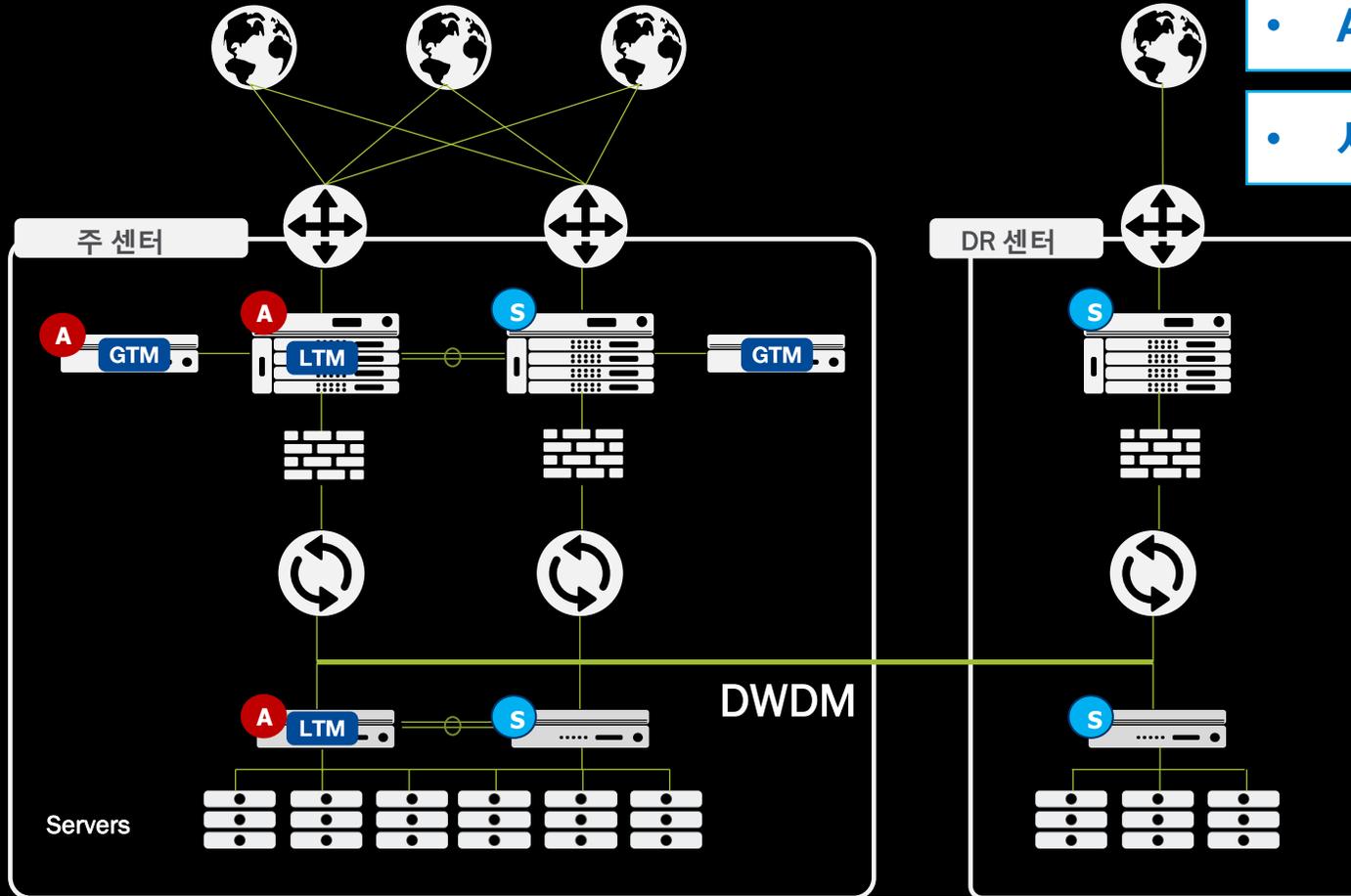


가상 ADC별 리소스 모니터링

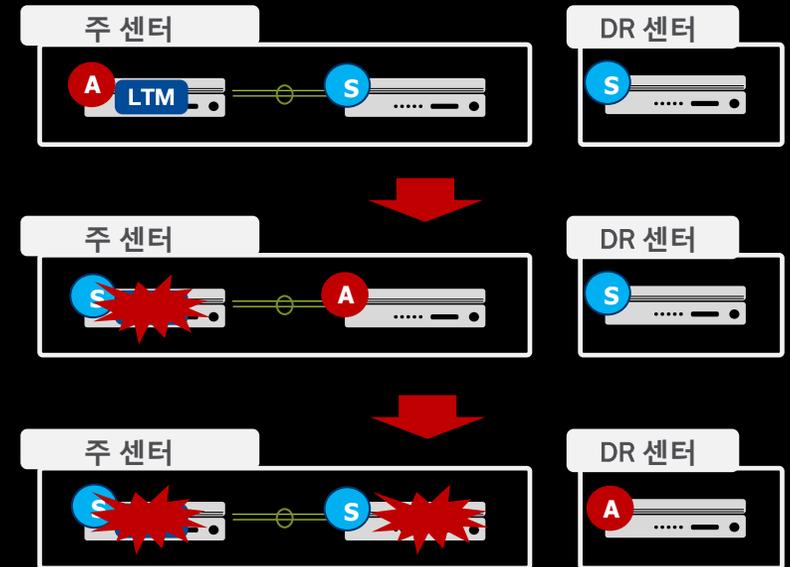
SLA 극대화 서비스 아키텍처 방안 2 - TCP 서비스

- 금융기관 대표적인 TCP 기반 서비스
 - ✓ 계정계, ATM, 단말기, 대외계 서비스

- 다중 클러스터 서비스망 구축
- Active-Standby-Standby 다중화
- 세션 동기화로 서비스 연속성 보장



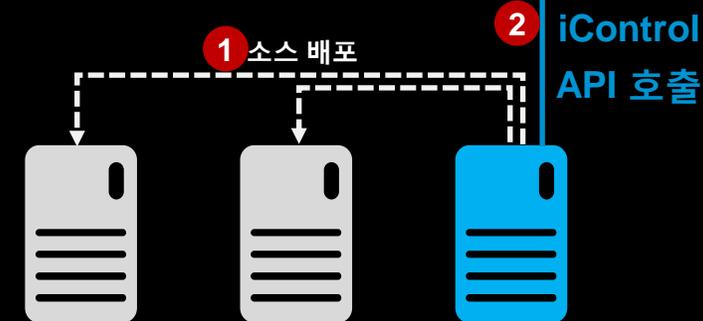
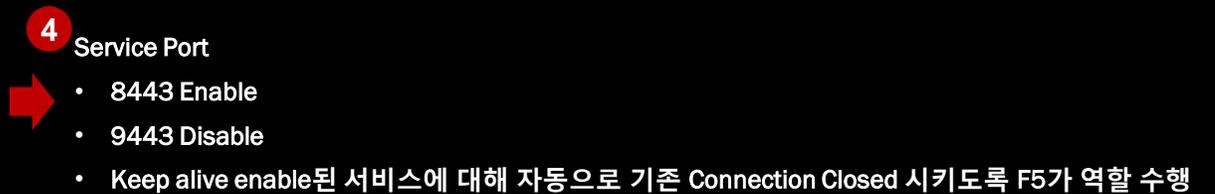
다중 클러스터 서비스 페일오버 순서



F5 API를 활용한 서비스 오케스트레이션 아키텍처

iControl API를 활용한 서비스 단절없이 실시간 서버 소스 배포 및 적용

- 소스적용 - WAS에 대한 로직 변경 작업
- 서비스 중단 없이 빠른 소스 배포 및 적용(API를 이용한 적용 서비스 확인 기능 탑재)
- 수동 적용보다 빠른 적용 - GAP 차이 극복(수동 vs 자동)
- 업무분담 - 서버 담당자가 ADC 장비에 접속 없이 바로 소스 적용



- 1 Main Server가 다른 서버에 소스 배포
- 2 Main Server가 F5 장비에 API 호출
- 3 소스 업데이트 Port Enable – 소스 적용 정상 여부 확인
- 4 기존 서비스 Port Disable
 - ✓ Keep alive가 disable인 서비스인 경우 - 즉시 반영
 - ✓ Keep alive가 enable된 서비스인 경우 - F5 장비가 기존 Connection을 Closed 하여 소스가 즉시 반영되도록 함

	인스턴스#1	인스턴스#2	Service Port
인스턴스#1	• 8443	• 8443	• 8443
인스턴스#2	• 9443	• 9443	• 9443

Main Server
소스 배포 서버



GO

SMARTER



GO

SAFER



GO

BETTER

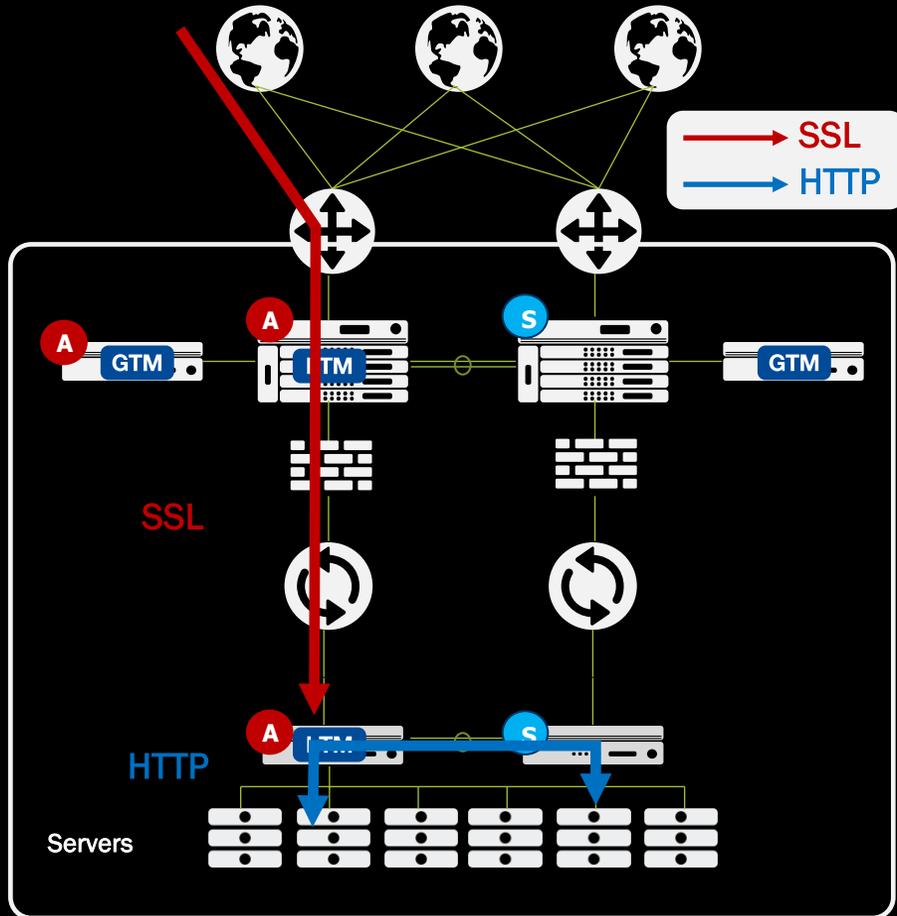


GO

FASTER

현 SSL 서비스 아키텍처

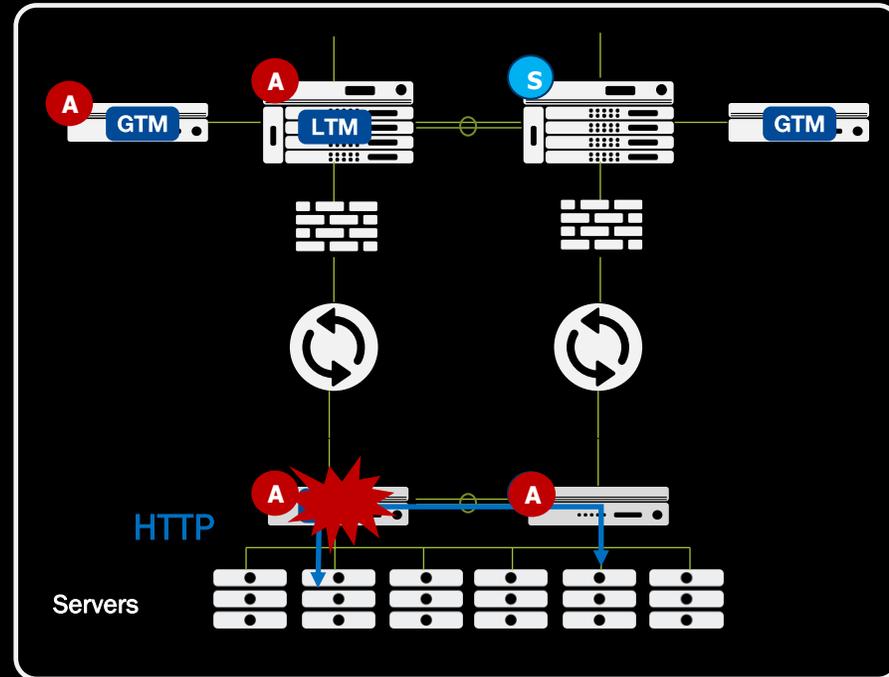
- SSL 가속 서비스 트래픽 Flow 현황



- ADC 장비에서 SSL Offloading 기능 수행

- ADC 장비에서 Client Side만 SSL 암호화

- 페일오버 발생 시 연결된 SSL 서비스 단절



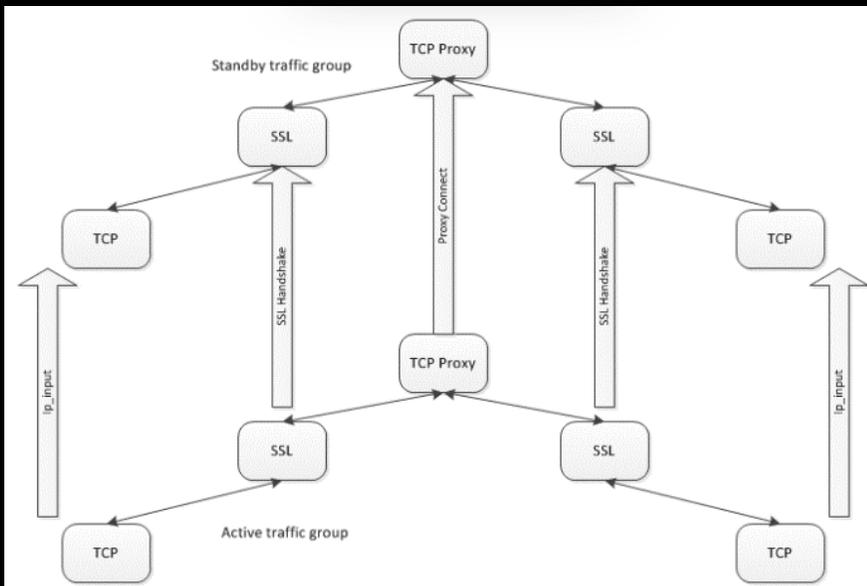
SSL 서비스 아키텍처 - SSL 암호화 Connection 미리 기능



ADC 업계 최초 SSL 암호화 미리링 지원

- ATM 서비스
- SSL 기반 연결 지향 데이터 통신 서비스

• **페일오버 발생 후에도 SSL 서비스 연속성 보장**



Standby



Active



오후 5:54:27 192.168.1.240:53456 Requested GET /favicon.ico
 오후 5:54:30 192.168.1.240:53456 Requested GET /BIGIP-11.6.0.0.0.401.iso

IP	Filename	Status	Speed	Time left	%
192.168.1.240:53455		idle 2		-	
192.168.1.240:53456	BIGIP-11.6.0.0.0.401.iso	28,158,760 / 1,95...	459.11 KB/s	1:10:11	1%

오후 5:54:27 192.168.1.240:53456 Requested GET /favicon.ico
 오후 5:54:30 192.168.1.240:53456 Requested GET /BIGIP-11.6.0.0.0.401.iso

IP	Filename	Status	Speed	Time left	%
192.168.1.240:53455		idle 2		-	
192.168.1.240:53456	BIGIP-11.6.0.0.0.401.iso	66,508,760 / 1,95...	458.03 KB/s	1:10:16	3%

SSL 서비스 아키텍처 - SSL 인증기반 DDoS 방어 기능

SSL기반 L7 DDoS 공격 방어를 누가 해야 할까요?

- HTTP/HTTPS flood
- Syn/Syn-Ack Flood
- Slowloris (GET DDoS)
- Slow POST (POST DDoS)
- Rudy attacks

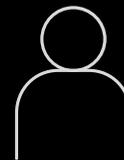
국내 은행 7곳에 디도스 공격 협박장... '비트코인 내나라'

발행일 : 2017.06.21

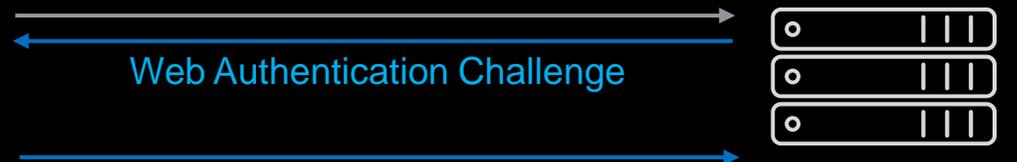


국내 시중은행 7곳에 분산서비스거부(디도스) 공격 협박장이 날아들었다. 비트코인을 지불하지 않으면 인터넷뱅킹 등 금융 서비스에 장애를 일으키겠다고 경고했다. 웹호스팅 기업 인터넷나야나가 랜섬웨어 공격에 몸값을 지불하자 해커그룹이 한국으로 물리는 정황이다.

21일 금융업계는 해킹그룹 아르마다 콜렉티브(Armada Collective)로부터 디도스 공격 위협 이메일을 받고 긴급 대응에 들어갔다. 해킹그룹이 공격을 명시한 날은 26일 월요일이다.

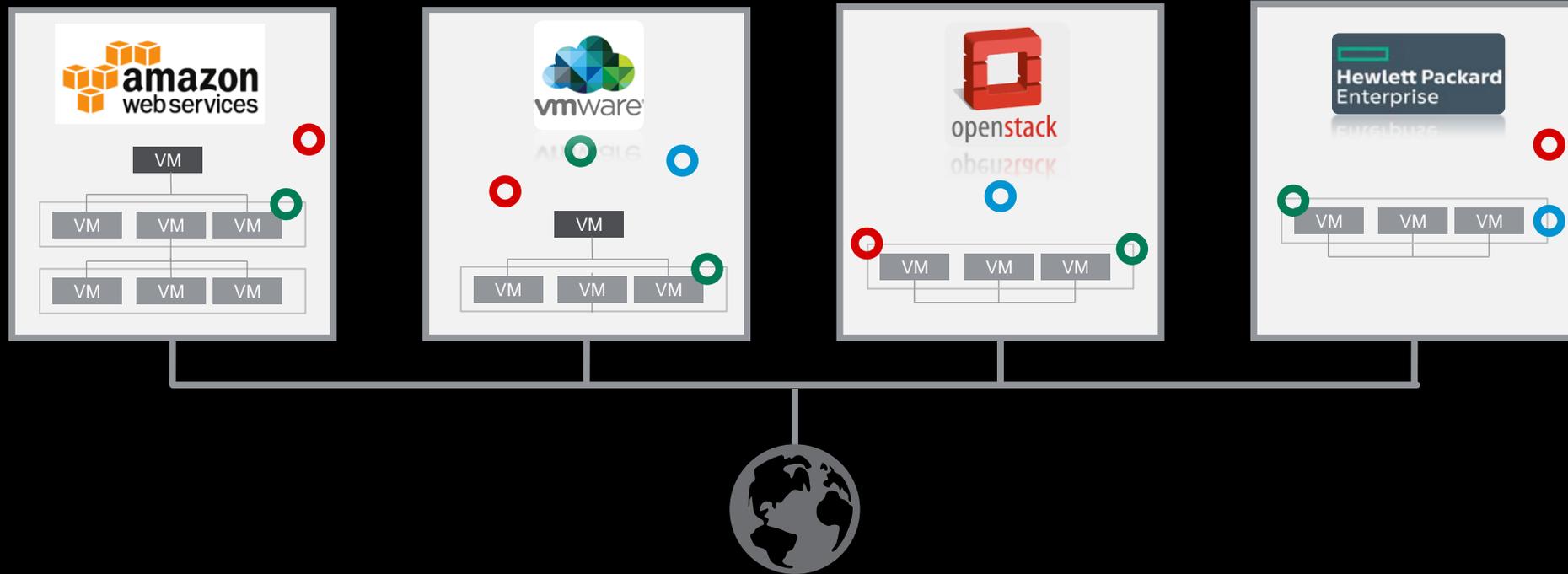


Web Authentication Challenge



Web Authentication Success!!

Hybrid 클라우드 SSL 서비스 아키텍처 - SSL is everywhere

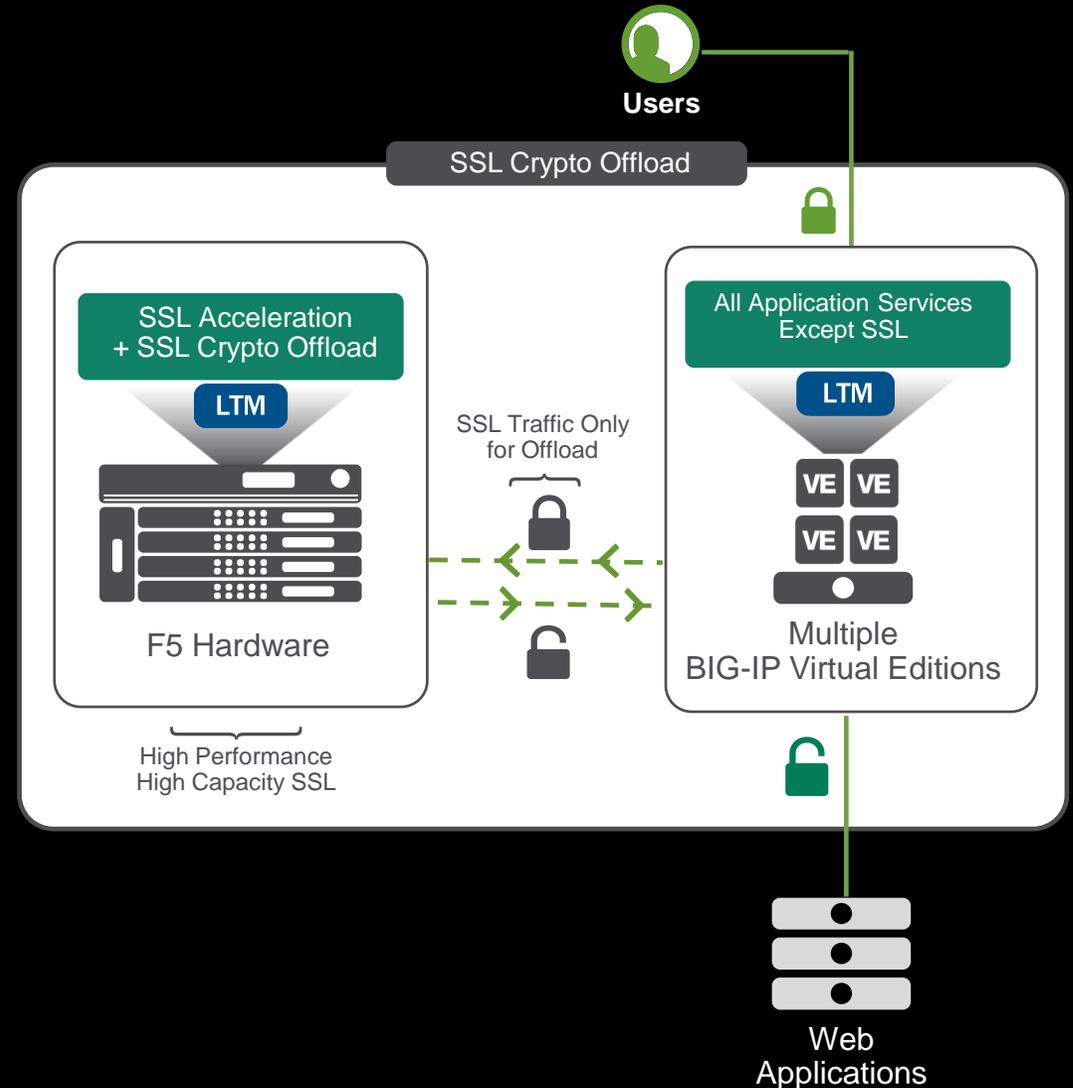


SSL 은 어느 곳이나 존재합니다. 클라우드도 마찬가지 입니다.

SSL Crypto Offload 기능

Hybrid Deployments을 위한 SSL Crypto Offload 기능 제공

- NFV L4 의 SSL 트래픽을 하드웨어 장비로 Offload 할수 있는 기능 지원
- SSL 트래픽만을 전용 하드웨어 장비로 운영함에 따른 SSL 기능 적용의 제약점 극복
- 소프트웨어 L4의 CPU 처리 부하 제거



SSL Crypto Offload 성능



SSL Performance



vCPU Utilization



VE Stand-Alone

1,500
TPS

100%



5,700
TPS

34%

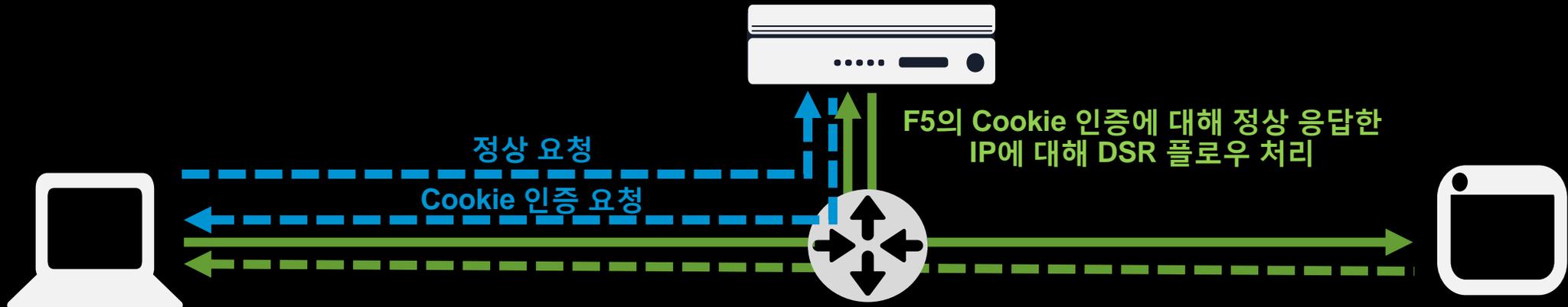
DSR 서비스 아키텍처에서 L4-L7 DDoS 차단 ?

Asymmetric

DSR 서비스 아키텍처에서 L4-L7 DDoS 차단 기능

동작 방식

- DSR 환경은 사용자에게 유입되는 트래픽만 F5 를 통과
- F5는 암호화된 Cookie 삽입 후 리다이렉션 요청
- 암호화된 Cookie 로 다시 접속하는 사용자는 DSR로 동작



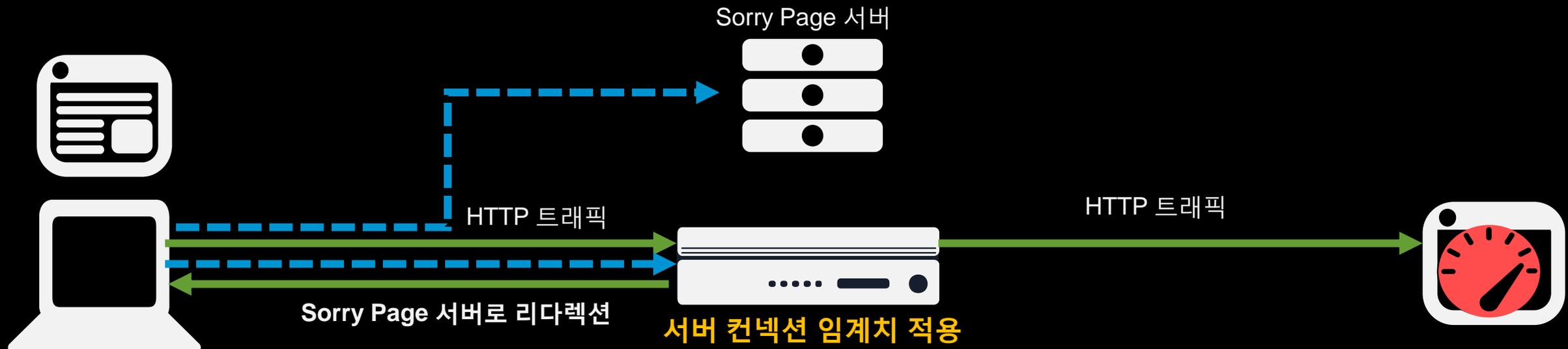
지능화된 서비스 아키텍처 - 세션 제어 솔루션

현재 ADC 에서 Redirection 동작 방식

- 특정 Sorry Page 서버로 전달

• Sorry Page 서버 성능

• 먼저 접속한 사용자에게 대한 우선순위 불가능



지능화된 서비스 아키텍처 - 세션 제어 솔루션

F5 세션 제어 솔루션 동작 방식

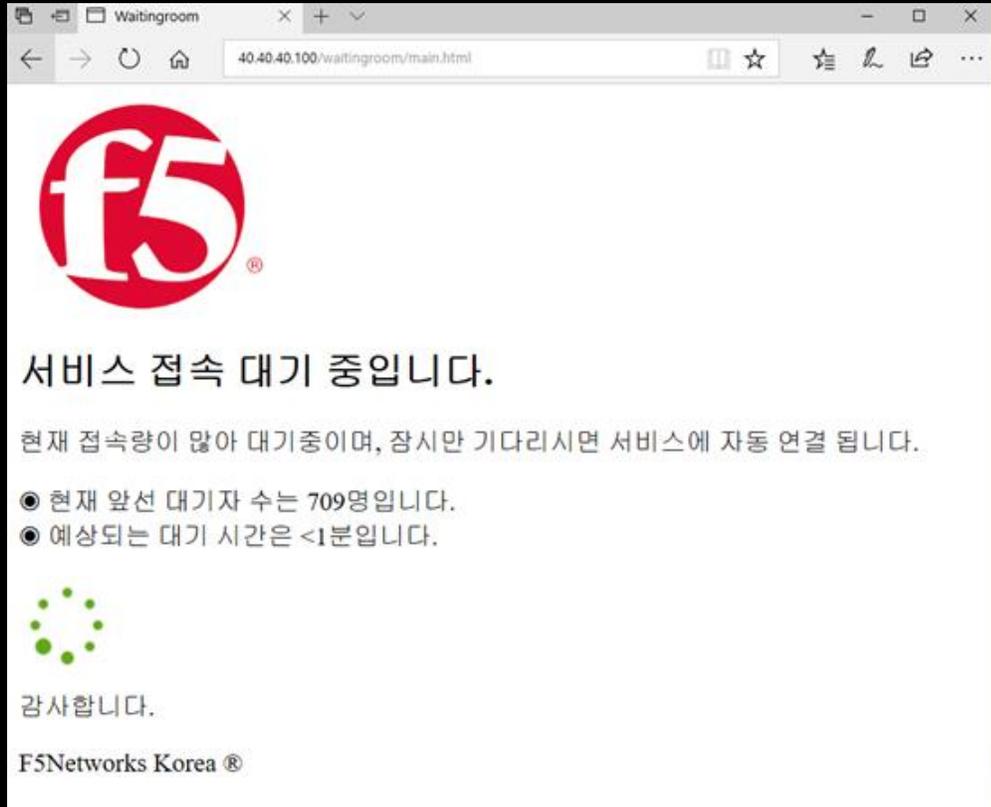
- 사용자화면에 대기 페이지 전달
- 세션 기반 트래픽 처리 제공

• 먼저 접속한 사용자에게 우선적으로 허용

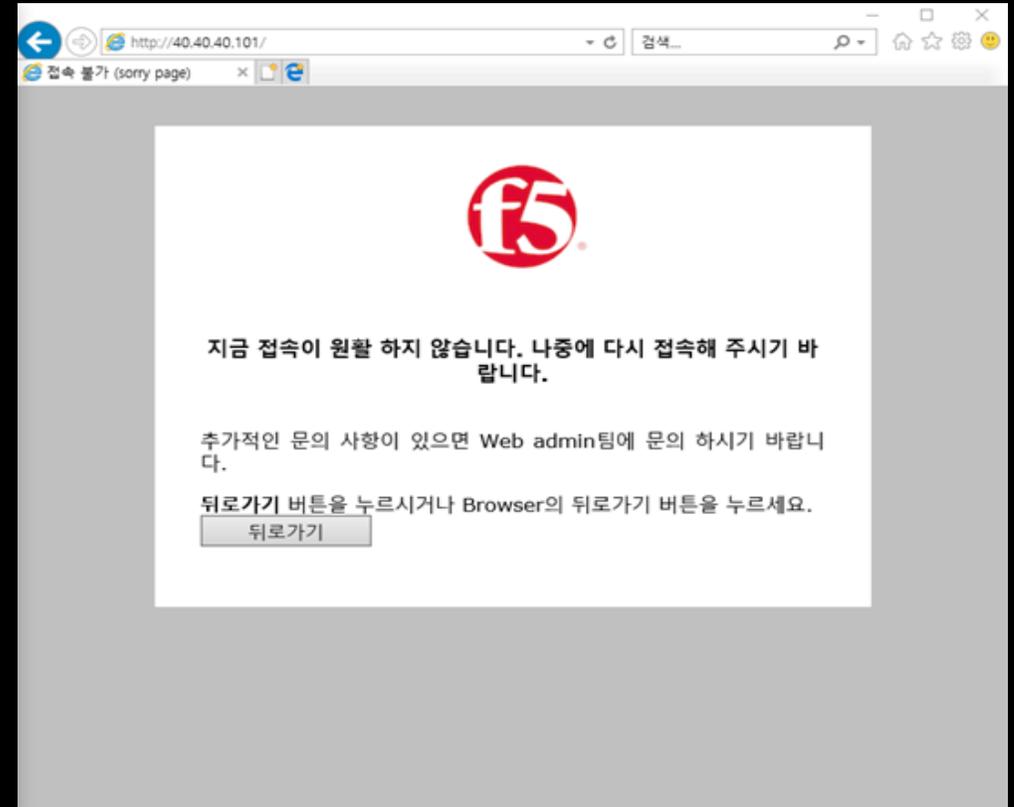
• 서버 Down시 ADC에서 직접 Sorry Page 전달



지능화된 서비스 아키텍처 - 세션 제어 솔루션



사용자단 안내 페이지 화면



서버 Down 시 Sorry Page 화면



WE MAKE APPS GO

SMARTER | SAFER | BETTER

감사합니다