ucloud biz 사용자 교육

I. ucloud biz 서비스의 이해

Cloud기술팀 | 2016.1.22

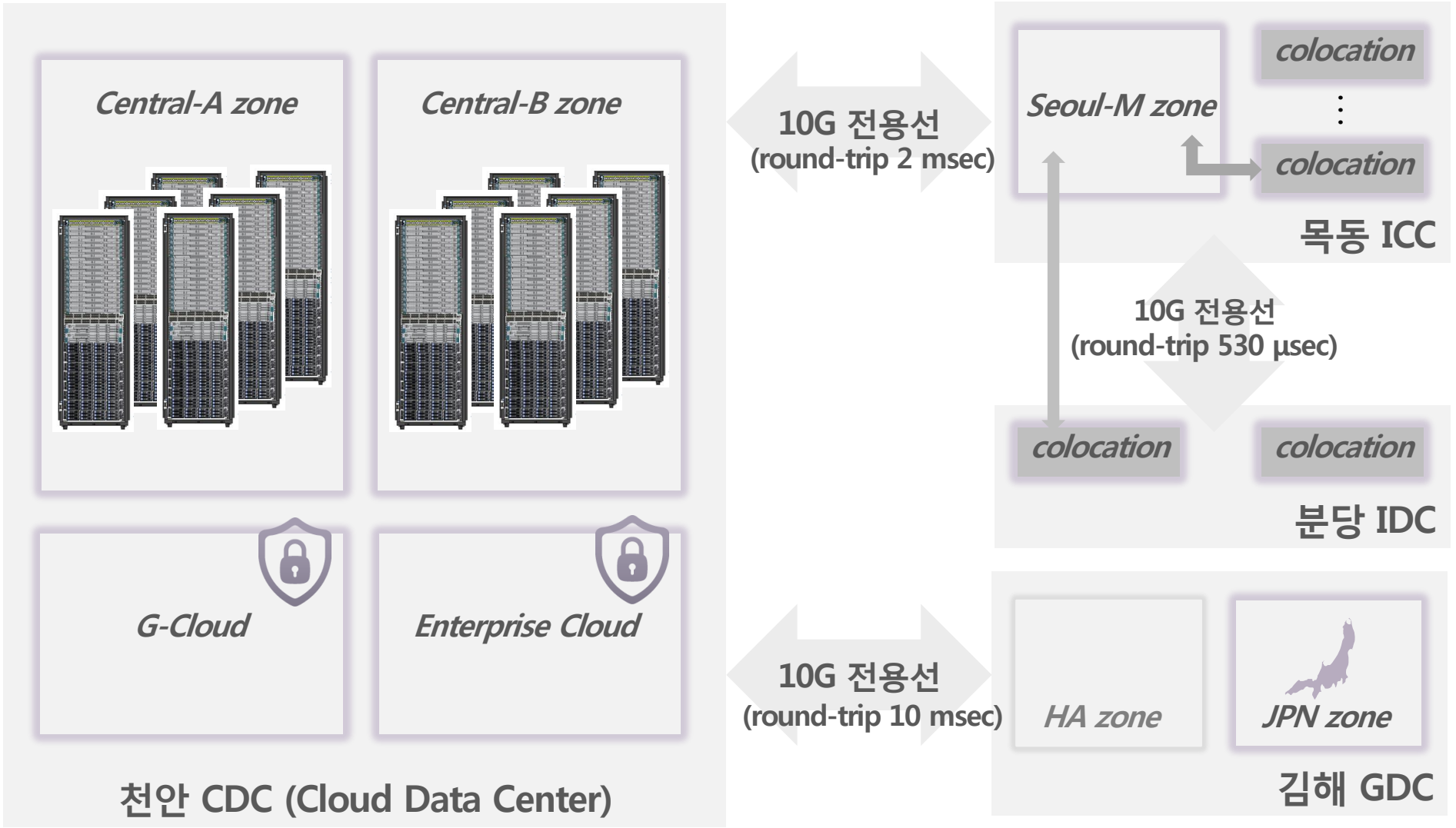
1-1 ucloud biz Data Center

- 변전소 이중화
- UPS N+1 with 발전기
- 분전반 이중화
- 랙 케이블 Power strip 이중화
- 내진설계

- 데이터센터 다중화
- 데이터센터간 10G 전용선

- 철저한 출입통제 (고객사 출입 불가)
- 외부 침입자 탐지 등 철저한 보안 시스템

1-2 Multi-zone



1-3 POD : 이중화/다중화/단순 구성으로 안정성 확보

서버

- 서버 NIC, 로컬 Disk, PSU 이중화
- cloud HA : 서버 failure 시에 VM들은 다른 서버에서 auto-restart
- Live migration : 서버 유지보수 작업 시에는 다른 서버로 무중단 VM 이동

네트워크

- 모든 네트워크 장비 이중화
- 네트워크의 구조와 기능을 최대한 단순화, 랙 내부망도 10G 이상 구성
- 서비스망과 관리망 분리로 보안성 확보

스토리지

- 스토리지 컨트롤러 이중화
- RAID 적용
- 스토리지망 분리 구축

1-4 운용 체계, 프로세스 : certified

SOC-1, SOC-2 :
아웃소싱 업체의 보안성 등과 관련된 독립된 감사인의 인증 보고서
SOC-1 : 국제감사인증위원회
SOC-2 : 미국공인회계사 지침

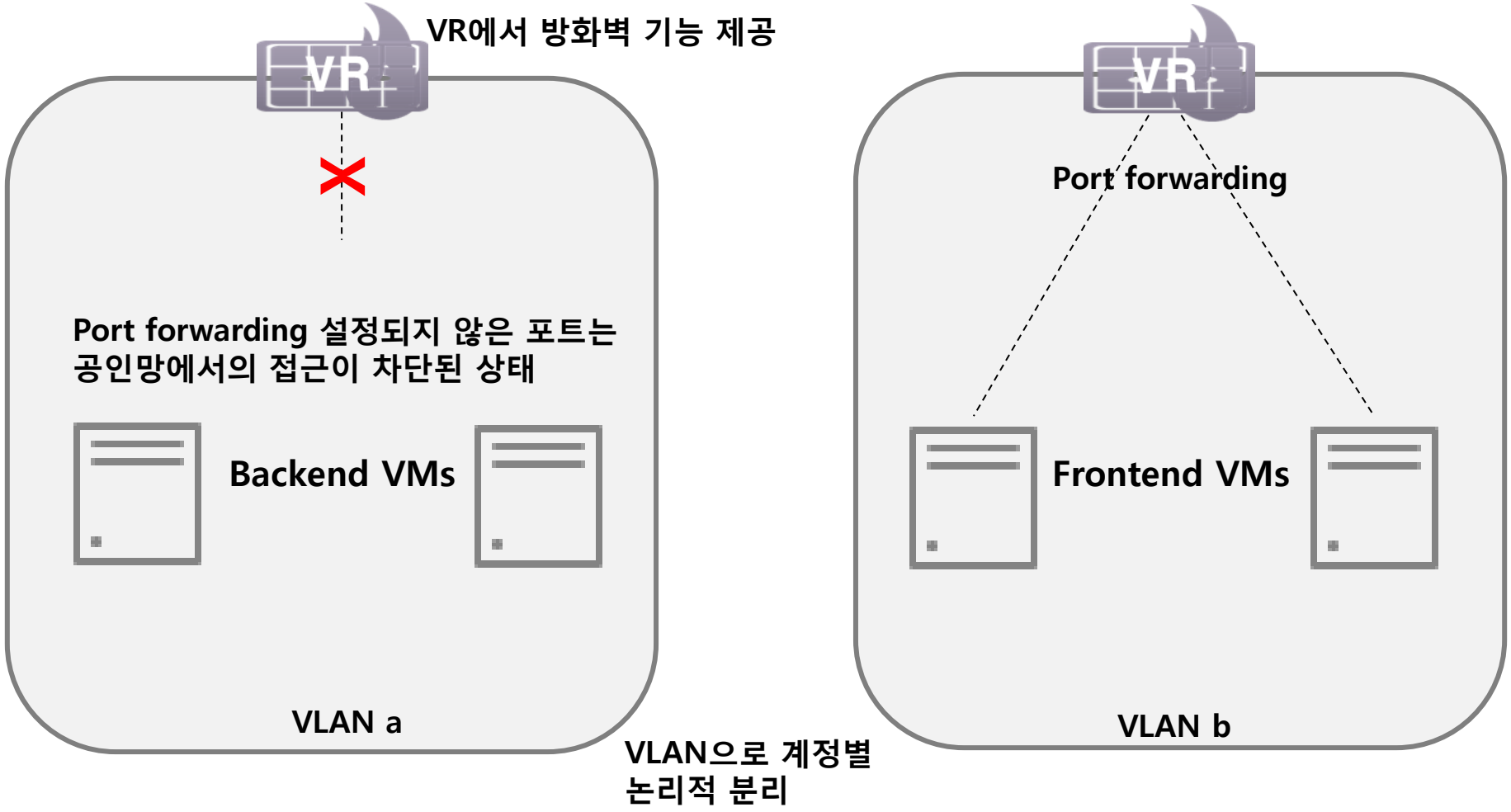
ISMS :
서비스의 안정성 확보를 위한 기술적, 물리적 보호조치 등 종합적인 관리체계에 대한 인증

ISO 27001 :
정보보호 경영시스템에 대한 국제 인증으로 위험관리, 보안정책, 접근통제, 보안사고 대응 등 11개 영역 133개 통제항목에 관한 엄격한 검증을 거쳐, 조직에서 구현한 정보보호 관리체계가 국제 규격에 적합함을 인정

클라우드서비스 우수 SLA :
방송통신위원회가 제정한 국내 클라우드 최우수 인증으로 일반 클라우드 서비스 인증에 가용성과 보안, 손해배상 등의 추가 요건을 만족해야 부여

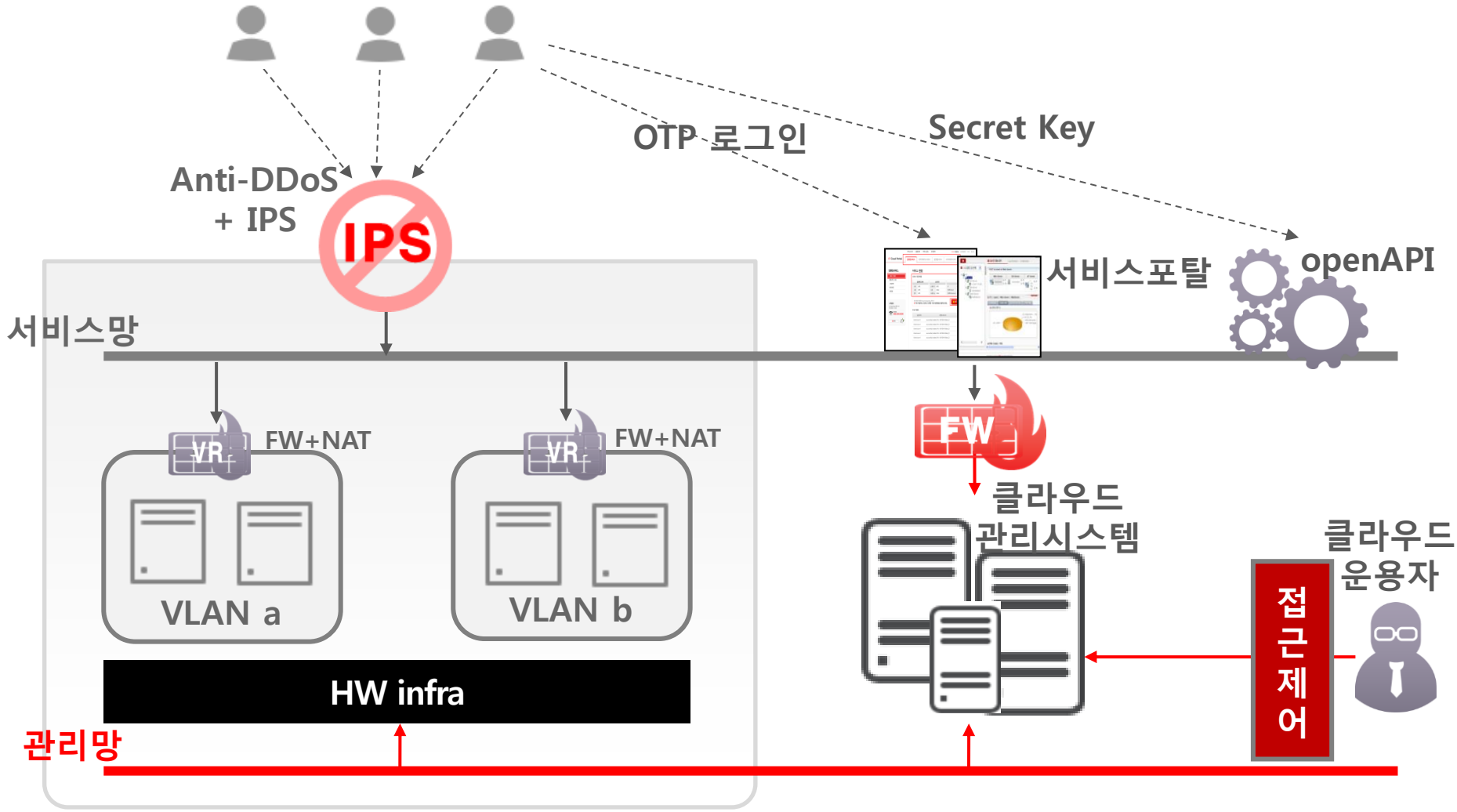
1-5 VLAN & NAT 구조

고객 계정별 VLAN 분리 및 VR (Virtual Router) 방화벽 제공



1-6 ucloud biz security overall

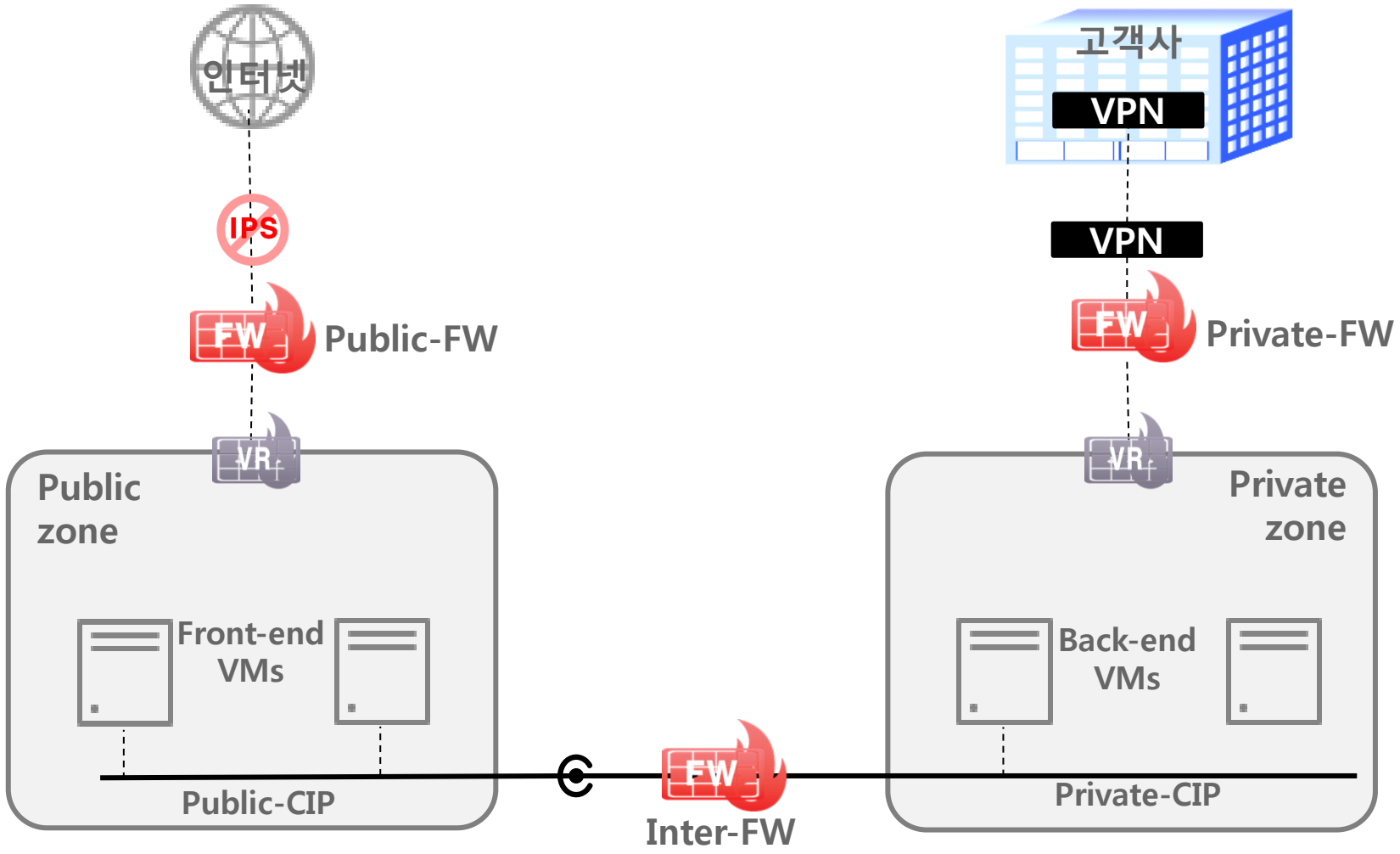
Public 환경에서도 default FW/NAT 활용. WAF 추가 활용 가능



1-7 Enterprise Cloud / G-Cloud

대기업, 정부공공기관의 보안 요구수준을 만족

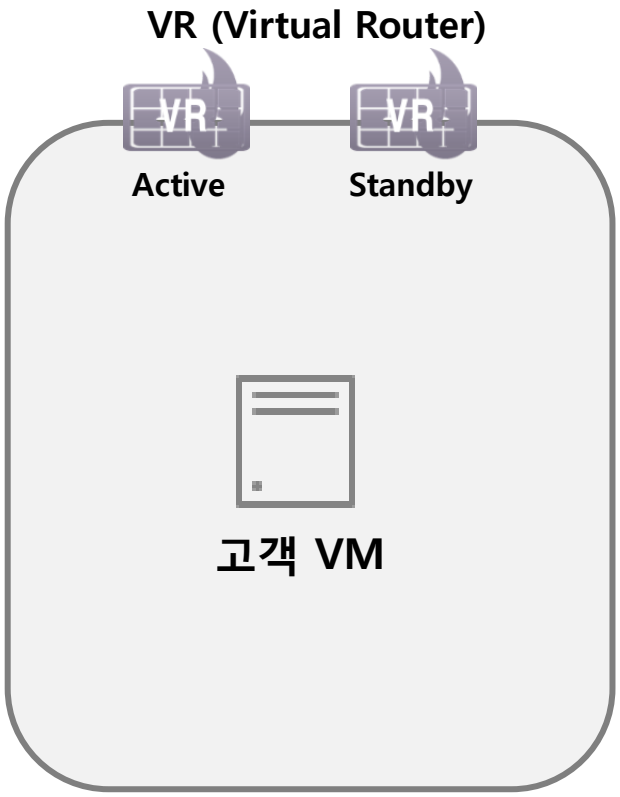
https://ucloudbiz.olleh.com/portal/ktcloudportal.epc.productintro.enterprise3.html



1 ucloud biz infra

2 ucloud biz 기반의 시스템 구조 설계

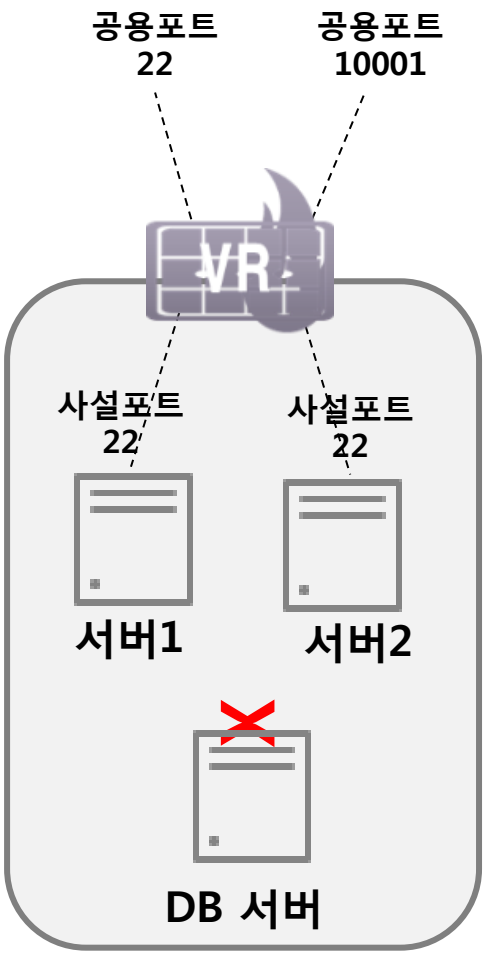
2-1 고객 시스템 환경에 대한 기본적인 이해 (1/2)



VM (Virtual Machine) : 가상서버

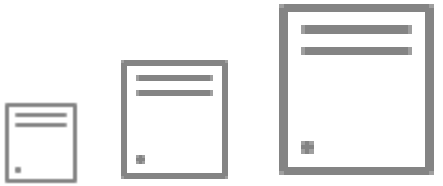
- 각각의 고객 계정은 VLAN으로 분리되어 있다
- VR (Virtual Router) : 고객 VM과 계정 외부와의 통신은 VR이 중개한다. VR은 NAT, 방화벽, DHCP 등의 역할을 담당한다. VR은 Active-Standby 이중화된 리눅스 서버로 구현되어 있다
  - ✓ NAT : 고객 계정 별로 하나의 공인 IP 주소가 할당되며, 필요시 추가할 수 있다. 계정의 모든 공인 IP 주소는 NAT 역할을 하는 VR이 소유한다
  - ✓ 방화벽 : inbound 트래픽의 source IP/port 를 허가할 수 있다
  - ✓ DHCP : 고객 VM에게 사설 IP 주소를 부여한다
- 사설 IP 주소 : 고객 계정별로 하나의 사설망이 할당되며, 고객의 VM은 사설 IP 주소를 부여받는다
  - ✓ 사설 IP 대역 : 172.27.x.x/16
  - ✓ 고객 VM의 사설 IP 주소는 VM이 삭제될 때 까지 변하지 않는다
  - ✓ 당연히, VR도 사설 IP 주소를 갖는다
  - ✓ 고객 VM에 추가 사설 IP 주소를 부여할 수 있다 (추후 설명)
- 계정의 자원 제한 : 고객 실수 등에 의한 자원 오남용을 방지하기 위해 계정별로 이용 가능한 자원의 한도가 있다
  - ✓ 고객 VM 100개 이하, 디스크 300개 이하, 공인 IP 60 개 이하
  - ✓ (일반적으로 권고하진 않음) 더 많은 자원 이용이 필요한 경우, 고객센터에 요청하여 한도를 늘일 수 있다

2-1 고객 시스템 환경에 대한 기본적인 이해 (2/2)

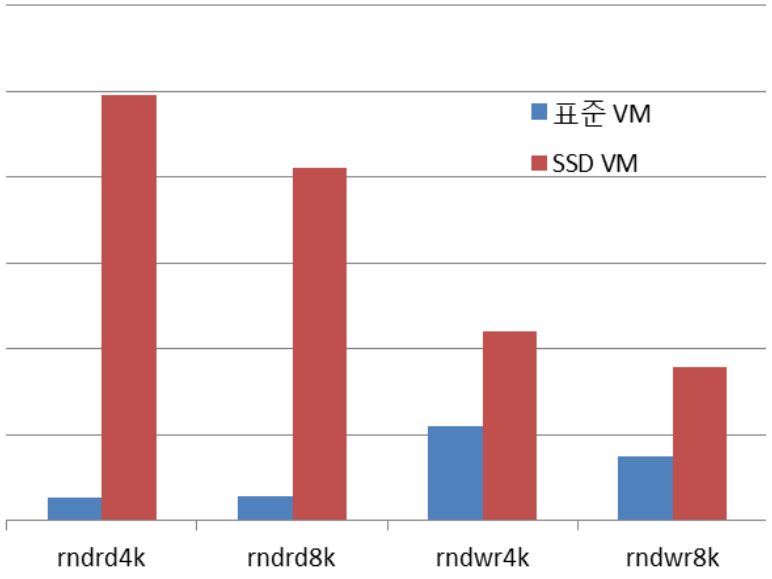


- Port forwarding : 공인망에서 고객 VM을 접근하려면, 접근하고자 하는 포트를 NAT 구성해야 한다
  - ✓ 고객 VM은 공인망으로 부터의 접근이 차단된 상태로 생성된다
  - ✓ 예를 들어, 고객 VM으로 telnet하기 위해서는 22번 포트를 NAT 구성해야 하고, Web 서버는 80 포트를 NAT 구성해야 한다
  - ✓ DB서버와 같이 평상시 공인망 노출이 불필요하고, 보안에 민감한 VM은 port forwarding 구성하지 않는 것이 바람직하다
- 공용포트 선택
  - ✓ Port forwarding 구성에서 고객 VM의 포트를 사설포트, VR에서 NAT되어 공인망에 노출되는 포트를 공용포트라고 한다
  - ✓ 공용포트 번호는 사설포트 번호와 일치하지 않아도 된다
  - ✓ 그림과 같이, 서버1과 서버 2는 모두 22 번 (ssh) 포트를 port fowarding 구성했지만, 서로 다른 공용포트를 사용하고 있다
- 방화벽 관리
  - ✓ VR 방화벽은 inbound 트래픽에 대해 All-deny 상태로 초기 설정되어 있다
  - ✓ Port fowarding 구성하면 자동으로 해당 포트에 대해서 All-allow 된다. 특정 IP대역에 대해서만 접근을 허용하려면 포탈에서 변경하면 된다
- Static NAT : 고객VM과 공인 IP 주소를 1:1 매핑해줄 수도 있다
  - ✓ 포탈에서 추가 공인 IP 주소를 신청하고, 대상 VM과 static NAT 설정하면 된다
  - ✓ Port forwarding 필요 없이, 방화벽만 오픈하면 공인망에서의 접근이 가능하다

2-2 VM 상품 선택



- CPU와 메모리 선택 : ? vcore ? GB
  - ✓ VM은 사용 도중에도 상품변경이 가능하기 때문에, 너무 정밀하게 사이징하지 않아도 된다
  - ✓ 일반적으로, 물리서버와 동일한 수준으로 사이징하면 무난하다
  - ✓ 영상 Transcoder, HPC (High-performance computing) 등 물리서버 환경에서도 CPU 부하율이 매우 높은 서버의 경우에는 물리서버 대비 2배의 코어수를 선택해야 한다



<ucloud의 표준VM vs. SSD VM IOPS 비교>

- (Socket 서버 등) 고성능의 네트워크 IO가 필요한 경우
  - ✓ VM 사양과 네트워크 IO 성능은 정비례하지 않으므로, 적은 수의 고사양 VM 보다는 많은 수의 저사양 VM으로 네트워크 IO를 분산하도록 설계하는 것이 좋다
  - ✓ 물론, VM 내부에서 적절하게 TCP/IP 튜닝도 해야 한다
    http://cafe.naver.com/ucloudbiz/24
- (DB서버 등) 고성능의 디스크 IO가 필요한 경우
  - ✓ 일반 VM은 2,000 IOPS 미만의 디스크 IO 성능을 제공한다
  - ✓ VM에 다수의 디스크를 추가하여 software RAID 구성해도 디스크 IO 성능은 향상되지 않는다
  - ✓ SSD VM 또는 SSD 볼륨은 일반 VM 에 비해 높은 디스크 IO 성능을 제공한다
  - ✓ SSD 특성 상, random read 성능이 탁월한 반면에 write 및 sequential r/w 성능은 일반 VM과 차별성이 크지 않다

2-3 데이터 저장 공간

	VM 디스크	NAS	Zadara	ucloud storage
최대용량	VM당 12개 데이터디스크 (300GB x 12 = 3.6TB)	볼륨당 20TB 이하	NFS, CIFS, I-SCSI를 지원하는 공유형 스토리지 (용량, IOPS, inode 등) 요구사항에 따라 on-demand로 전용 자원 구성 마켓플레이스 상품 https://ucloudbiz.olleh.com/portal/ktcloudportal.epc.productintro.ucloud_server_image.zadara.html	무제한
성능수준	HDD : 2,000 IOPS 미만 SSD : 최대 20,000 IOPS (VM당 최대 2개 볼륨)	2,000 IOPS 미만 Neighbor effect 불가피		업로드 300 Mbps (x N) 다운로드 500 Mbps
가격수준	HDD : 70원 / GB SSD : IOPS 수준별 차등	70원 / GB		구간별 30원 ~ 25원 / GB
파일시스템	OS 파일시스템	NFS, CIFS, I-SCSI		Object storage, RESTful API
기타 특징	데이터디스크가 크면 VM 이동성 저하	공유형 스토리지 자동/수동 확장 가능		기본 3 copy 저장 모든 파일에 static URL CDN 연계 openStack component AWS S3 compatible
적절한 용도	SW 패키지, 자주 변경되는 데이터, 데이터베이스	여러 서버가 공유하는 파일		배포용 대용량 컨텐츠 아카이빙/백업

2-4 Image를 활용한 VM 복제와 증설

원본이 잘생겨야

복제본도 잘생긴다

- 운영중인 VM을 일시정지 → 스냅샷 → 이미지화 한다
- OS 디스크만 이미지화가 가능하다
  - ✓ OS 디스크가 가벼울수록 이미지 생성, 복제 VM 생성이 용이하다
- 웹서버 다중화 등 동일한 VM을 다수 생성해야 하는 경우, 긴급 증설에 대비해야 하는 경우, Autoscaling 설정 등에 활용하면 편리하다
- 스냅샷하기 전에, 데이터디스크 마운트 정보 등 정상적인 VM 부팅을 불가하게 만드는 요소는 제거해야 한다

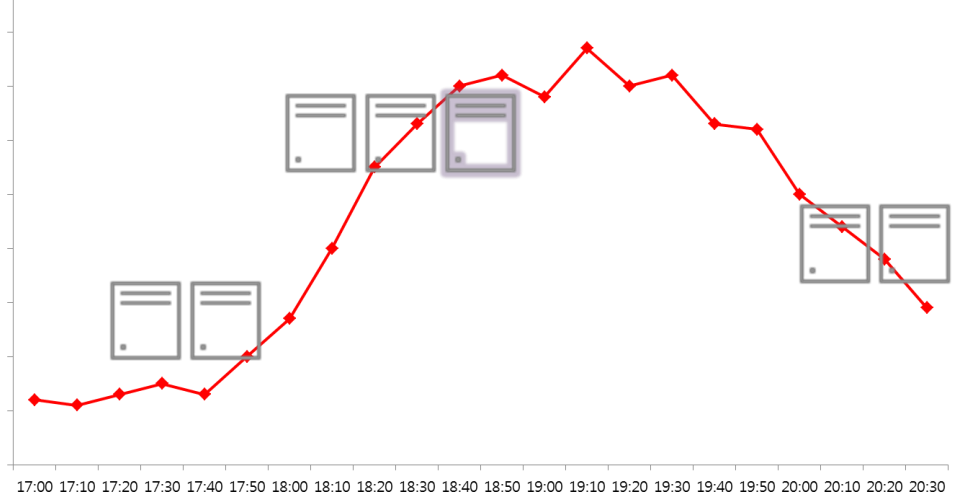
기본이미지에서 불필요한 구성 제거 → 어플리케이션 패키지 설치 → (권고) 로그 서버는 별도로 구성 → 서비스 및 스크립트 구성 → **이미지 생성**

2-5 시스템 부하 변동에 따른 Scaling 정책

- **Scale-up/down vs Scale-in/out**
  - ✓ Scale-up/down은 서버의 spec.을 조절하는 것이고, Scale-in/out은 서버의 수량을 조절하는 것이다
  - ✓ Scale-up/down은 VM을 중지시켜야 하고 (서비스 중단), 조절 가능한 최대 spec.에 제한이 있다
  - ✓ 유료 SW를 사용하는 VM을 Scale-in/out 하려면 비용부담이 있다

- **Autoscaling**
  - ✓ 자동화된 Scale-in/out
  - ✓ 예기치 못한 트래픽 증감에도 유연하게 대처할 수 있다는 장점이 있지만, 급격한 속도의 변동에는 적기 대응하기는 힘들다 (5분 주기 모니터링 → 알람발생 → VM 생성에 소요되는 시간)

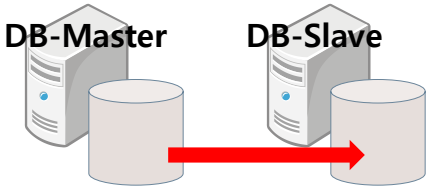
- **Session Clustering** : scale-in이 발생하면 해당 서버에 수용된 세션이 끊어지게 된다. 이를 방지하기 위해 session 정보를 모든 서버들이 공유하게 하는 것이 바람직하다



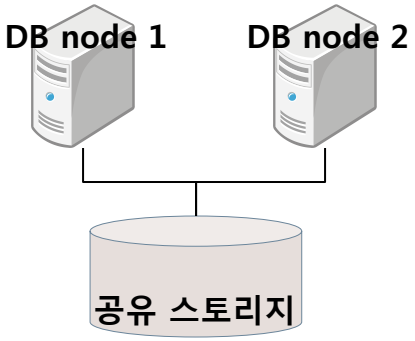
2-6 DB서버의 이중화

- I-SCSI 공유 스토리지 기반의 이중화를 구성할 수 있다
  - ucloud NAS (저성능 DB), Zadara (고성능 DB)
  - MS-SQL clustering
  - 마켓플레이스 상품 MCCS 기반의 이중화 (다양한 RDB 솔루션에 적용 가능)

- VM 디스크로 replication / mirroring 을 구성할 수 있다
  - mySql replication (ucloudDB 서비스)
  - MS-SQL mirroring, mariaDB Galera cluster, PPAS EDB failover manager 등



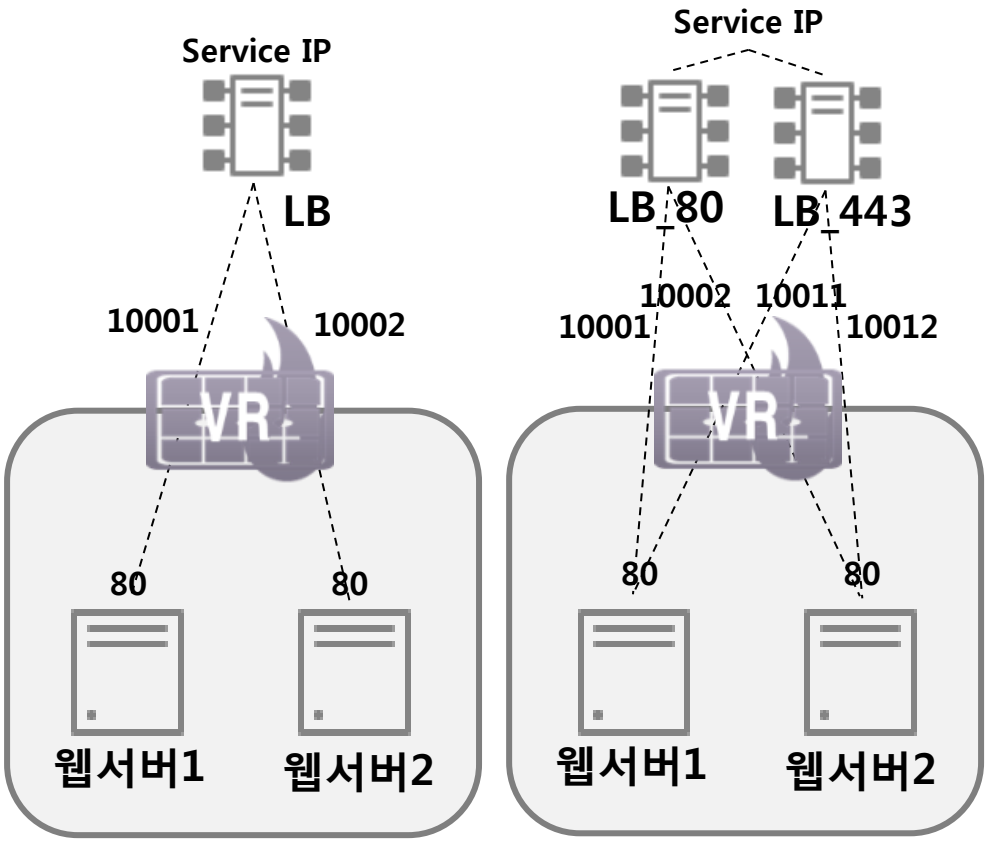
Replication / Mirroring



공유 스토리지 기반의 Clustering

2-7 LB (Load balancer) 사용

- LB는 계정 외부에 proxy 형태로 존재한다
  - ✓ 로드밸런싱해야 하는 포트를 port forwarding 하고, 공용포트를 대상으로 LB 구성한다
  - ✓ 계정 내부 연동에서의 로드밸런싱에는 적합하지 않다



- 패킷이 LB를 통과하면서 source IP가 LB의 SNIP로 변경되므로, 웹서버 로그 등에 Client의 IP주소를 기록하고 싶다면 X-Forwarded-For 헤더를 확인해야 한다
  http://cafe.naver.com/ucloudbiz/56
- Session stickyness
  - ✓ LB에서는 session 정보를 관리하지 않는다
  - ✓ LB 알고리즘을 Source IP hash (+port) 로 설정하면, client IP 주소(+포트)별 항상 동일한 서버로 패킷을 보내준다
  - ✓ 또는, 서버에서 session clustering을 구성해도 session stickyness를 구현할 수 있다
- HTTPS 트래픽
  - ✓ LB는 포트별로 별도 생성해야 하지만, 포트가 다르면 동일한 service IP로 묶을 수 있다
  - ✓ LB 프로토콜을 HTTPS로 선택하고 인증서를 등록하면 HTTPS 트래픽을 복호화하여 평문 트래픽으로 서버에 전달할 수 있다

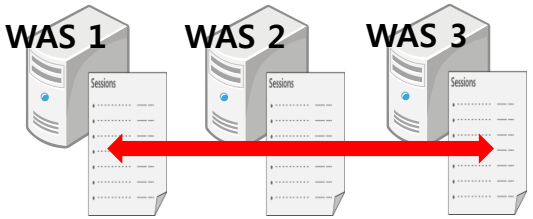
※ DNS나 GSLB를 로드밸런서로 활용하는 것은 권고하지 않음

2-8 session clustering

다중화된 모든 서버들이 모든 session 정보를 공유할 수 있으면

- ✓ LB 알고리즘에 무관하게 session stickyness가 보장될 뿐 더러,
- ✓ 일부 서버의 장애 또는 scale-in이 발생해도 해당 서버에 수용된 세션이 끊어지지 않는다

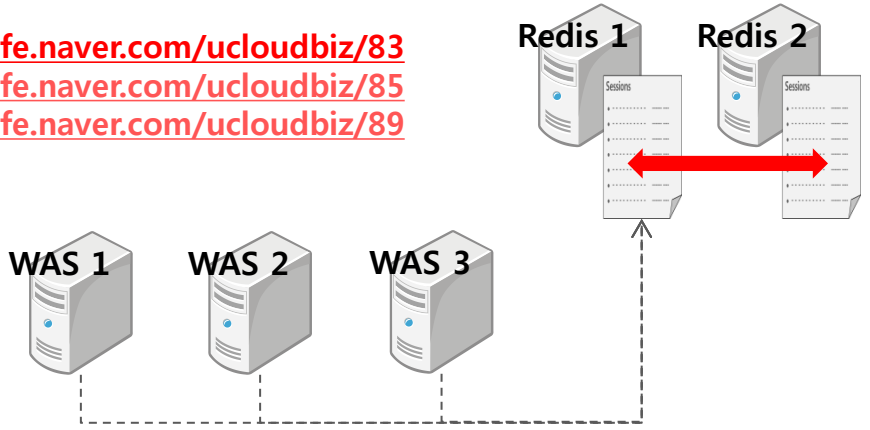
- Tomcat/JBOSS Session Clustering
  - ✓ Web/WAS 솔루션들은 대개 session clustering 기능을 제공한다
  - ✓ Web/WAS 서버간 세션 정보를 공유함으로써 일부 장애 또는 scale-in에 대처



http://cafe.naver.com/ucloudbiz/155

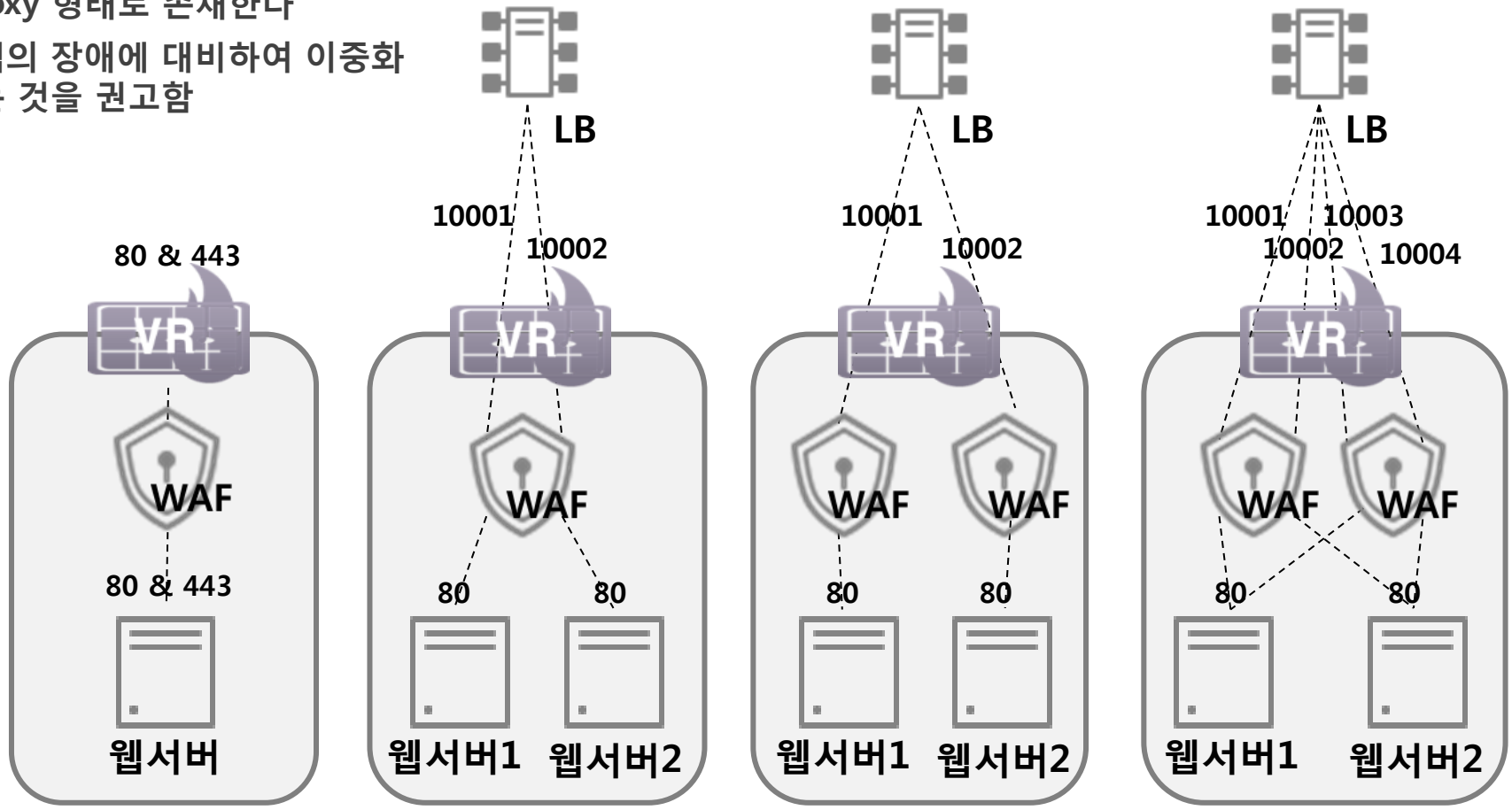
- Redis Session Manager
  - ✓ In-memory DB 솔루션인 Redis 활용한다
  - ✓ Redis 에서 세션 정보를 별도로 관리

http://cafe.naver.com/ucloudbiz/83
http://cafe.naver.com/ucloudbiz/85
http://cafe.naver.com/ucloudbiz/89



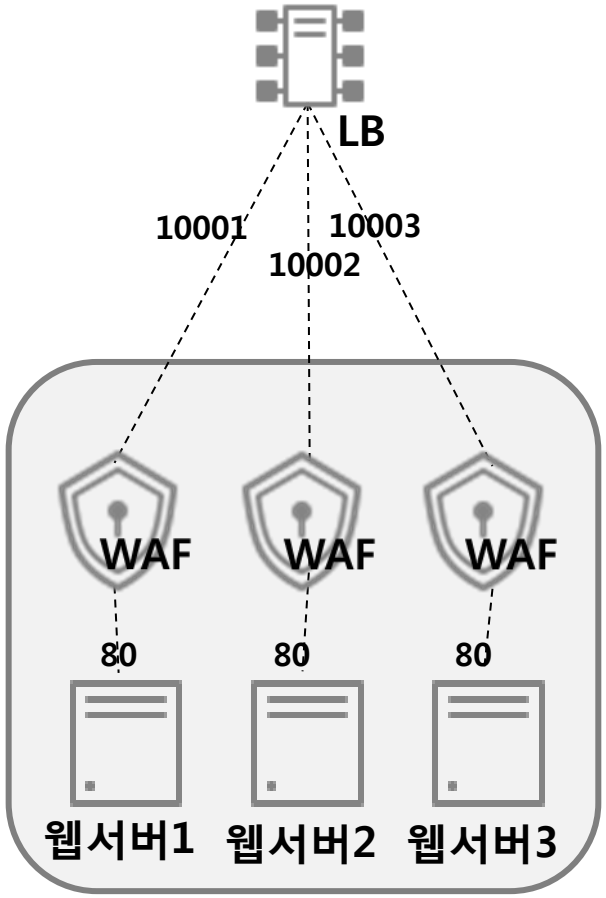
2-9 웹방화벽 사용 (1/2)

- 웹방화벽은 펜타시큐리티의 WAPPLES 와 모니터랩의 WIWAF-VE 상품 중에서 선택이 가능하다
- 웹방화벽은 일종의 VM으로, 계정 내부에 proxy 형태로 존재한다
- 웹방화벽의 장애에 대비하여 이중화 구성하는 것을 권고함

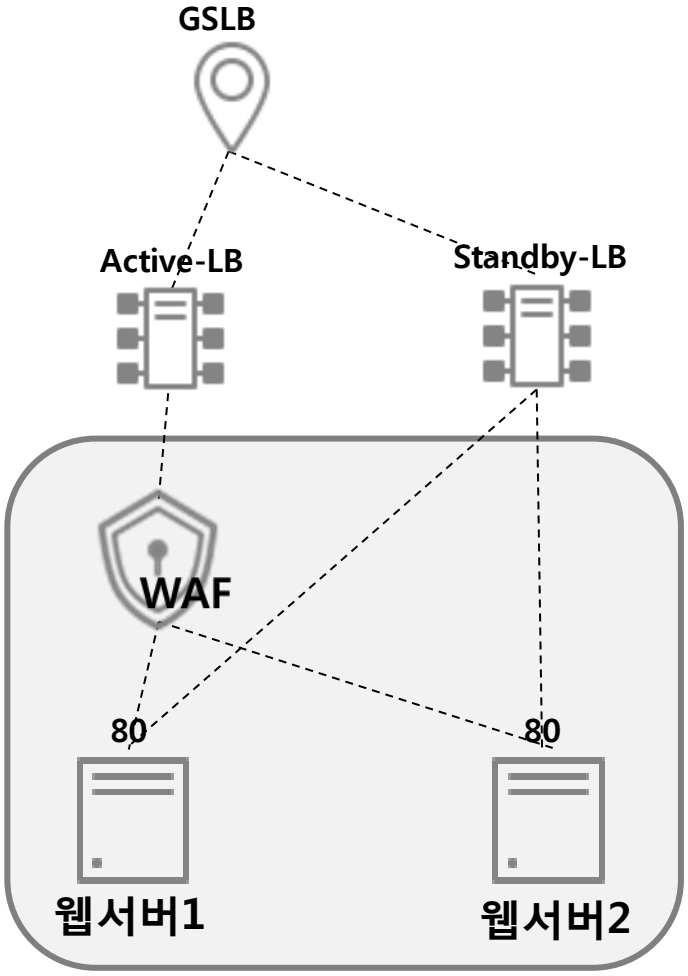


2-9 웹방화벽 사용 (2/2)

- 일시적인 트래픽 폭주에 대비 : 웹방화벽은 scale-up/down 되지 않으므로, scale-in/out으로 대처한다

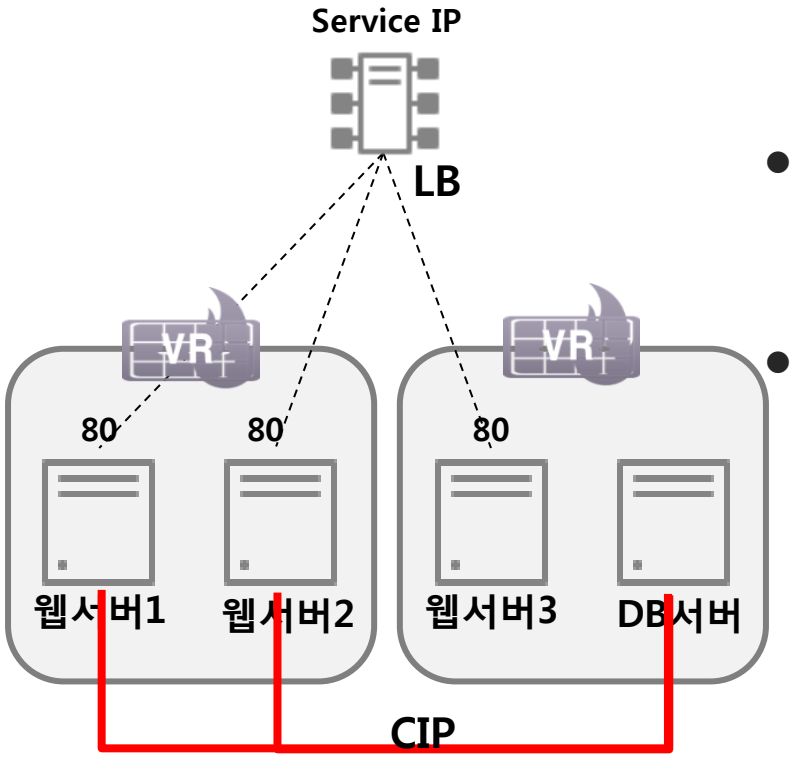


- 웹방화벽을 이중화 구성하지 않을 경우, 웹방화벽 장애에 대비하여 트래픽 우회 방안을 마련해야 한다



http://cafe.naver.com/ucloudbiz/141

2-10 대형 시스템 구성을 위한 그룹계정 및 CIP 기능



- VR의 한계
  - ✓ 50만 conntrack, in+out 1 Gbps 미만. VR scale-up 하더라도 30 % 내외 개선 효과 (scale-up은 고객센터에 별도 신청)
  - ✓ 2015.2월 부터 신규 생성된 계정의 VR은 in+out 3 Gbps 가능하며, VR scale-up 하면 최대 500만 conntrack 까지 가능하다 (Seoul-M, Central-A, Central-B only)
  - ✓ conntrack time-out : 3,600 초
- 그룹계정 : 다수의 계정을 하나의 그룹으로 묶어서 사용할 수 있다
  - ✓ Single-Sign-On, 통합과금, 이미지 공유 (그룹공개 이미지)
  - ✓ 하나의 LB로 그룹계정 전체를 로드밸런싱 할 수 있다
- CIP (Cloud Internal Path)
  - ✓ 계정별 또는 그룹계정별 CIP라는 추가 네트워크를 사용할 수 있다. CIP를 생성하면 추가 VR도 생기게 되지만, DHCP 역할만 담당한다
  - ✓ CIP는 모든 VM에 일괄 적용되지 않고, 선택적으로 적용된다
  - ✓ 그룹CIP는 그룹계정 전체에 적용되어, 계정간 내부망 역할을 제공한다
  - ✓ CIP는 NAS, VPN, 전용회선, 베어메탈서버 등 비가상화 장비와의 연동 역할도 겸한다

2-11 CIP를 활용한 비가상화 장비 또는 외부 연동

- 목동ICC 고객은 층간 패치로 Hybrid Cloud 구성

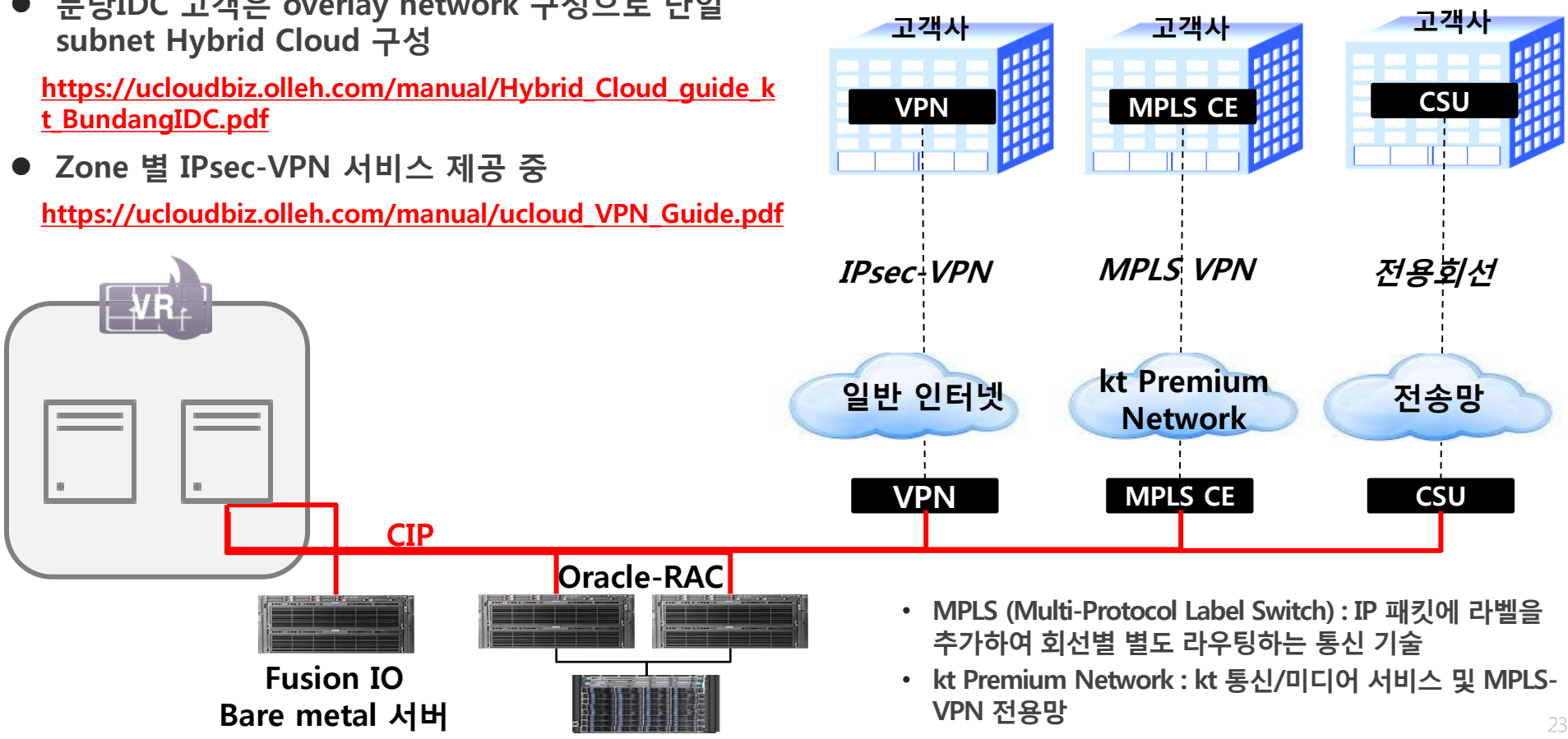
  https://ucloudbiz.olleh.com/manual/Hybrid_Cloud_guide_kt_mokdongIDC.pdf

- 분당IDC 고객은 overlay network 구성으로 단일 subnet Hybrid Cloud 구성

  https://ucloudbiz.olleh.com/manual/Hybrid_Cloud_guide_kt_BundangIDC.pdf

- Zone 별 IPsec-VPN 서비스 제공 중

  https://ucloudbiz.olleh.com/manual/ucloud_VPN_Guide.pdf

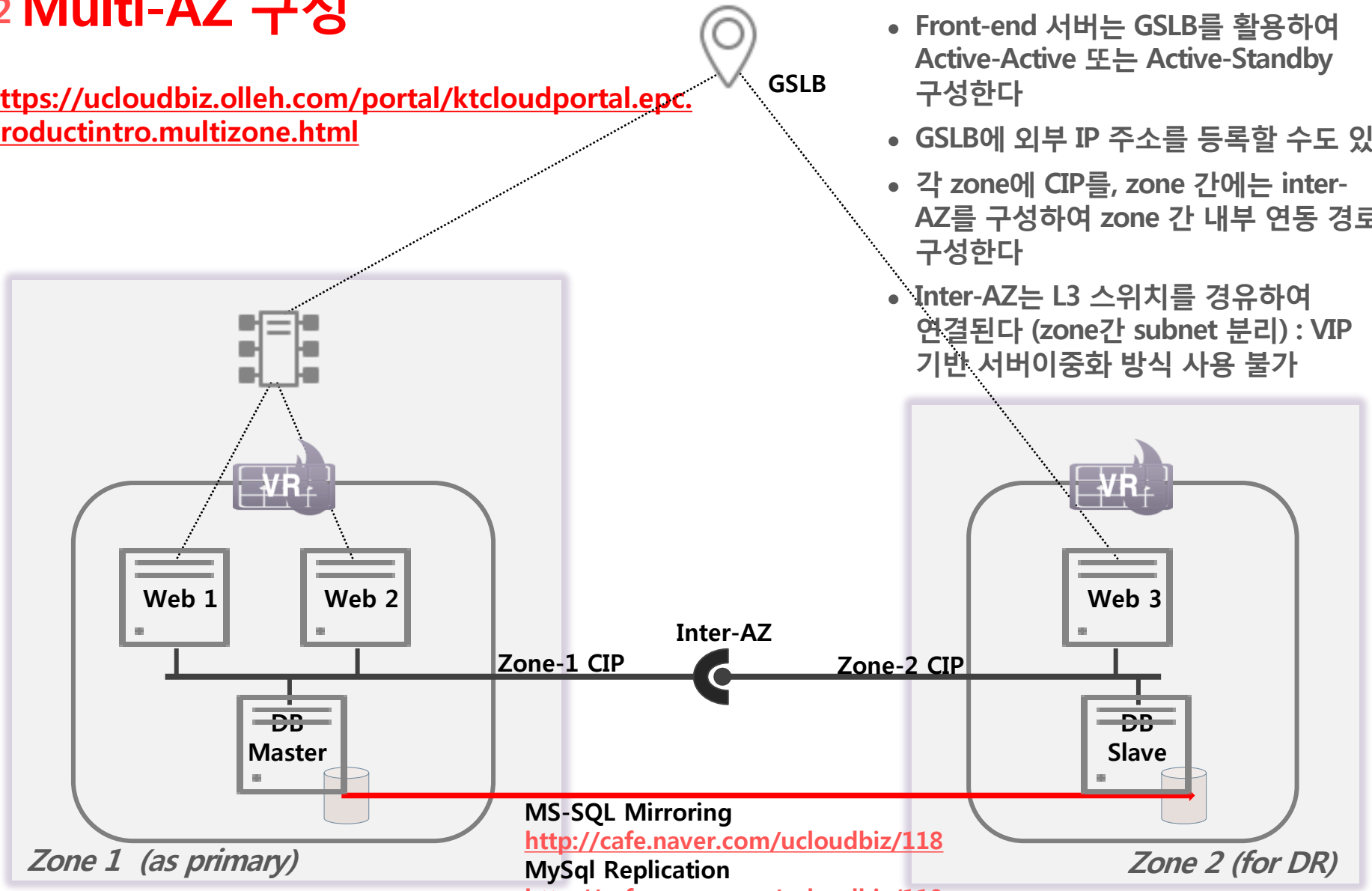


- MPLS (Multi-Protocol Label Switch) : IP 패킷에 라벨을 추가하여 회선별 별도 라우팅하는 통신 기술
- kt Premium Network : kt 통신/미디어 서비스 및 MPLS-VPN 전용망

2-12 Multi-AZ 구성

https://ucloudbiz.olleh.com/portal/ktcloudportal.epc.productintro.multizone.html

- Front-end 서버는 GSLB를 활용하여 Active-Active 또는 Active-Standby 구성한다
- GSLB에 외부 IP 주소를 등록할 수도 있다
- 각 zone에 CIP를, zone 간에는 inter-AZ를 구성하여 zone 간 내부 연동 경로를 구성한다
- Inter-AZ는 L3 스위치를 경유하여 연결된다 (zone간 subnet 분리) : VIP 기반 서버이중화 방식 사용 불가



Thank you