

네트워크 가상화를 통한 망분리 고도화

임관수 / Senior Systems Engineer

vmware®

© 2014 VMware Inc. All rights reserved.

#VDI (Virtual Desktop Infrastructure)

#SDDC (Software Defined Data Center)

데스크톱 가상화(VDI) 고려사항

Capex

(구축비용)

Opex

(운영비용)

Security

(보안)

CAPEX(구축비용)

**가상화
솔루션**

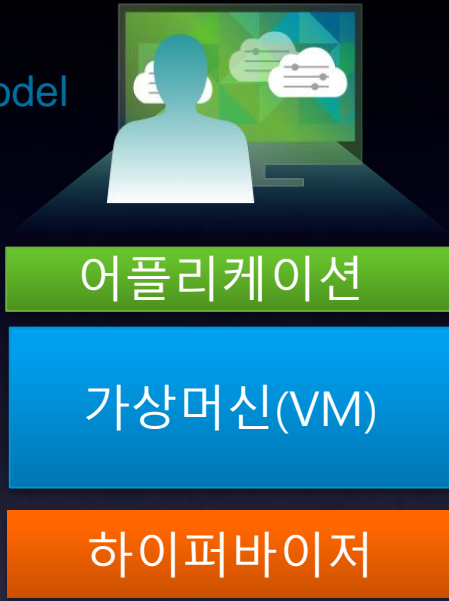
(Hypervisor + VDI Solution)

하드웨어
(Server & Storage)

네트워크
(Network Infra)

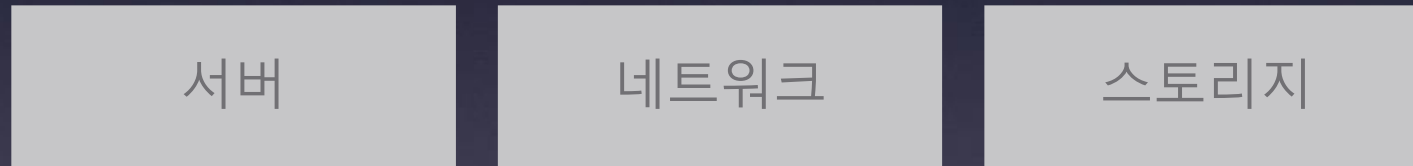
소프트웨어 정의 데이터 센터 접근 방식 (SDDC)

Automated Operational Model



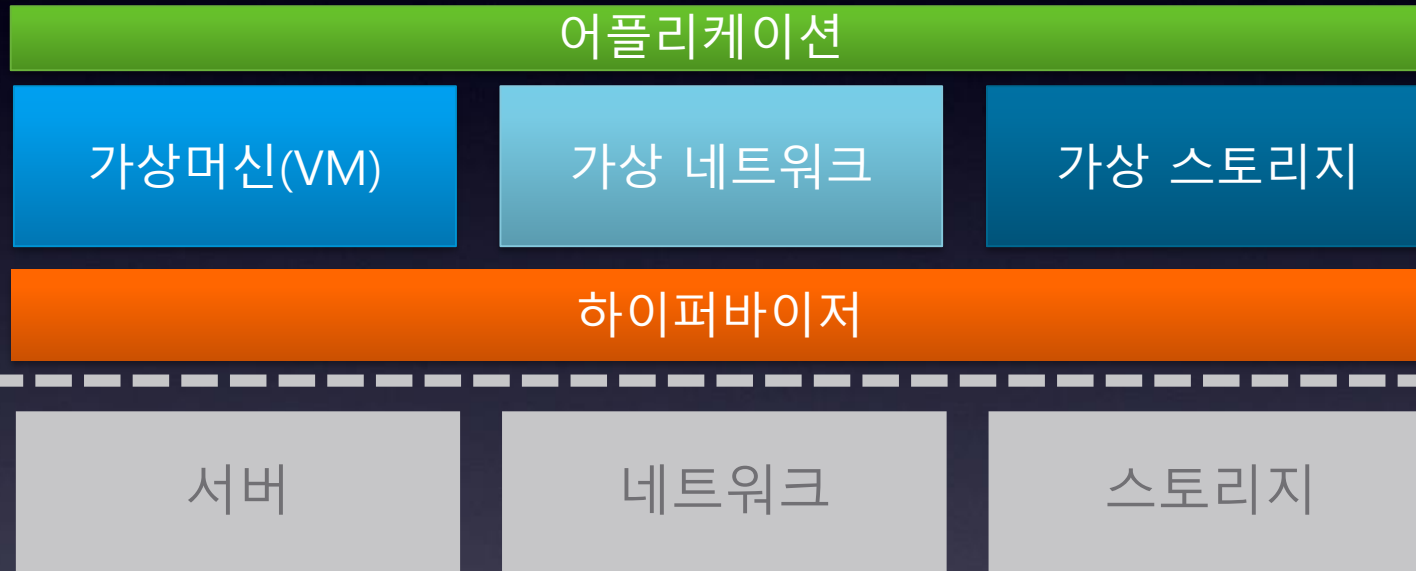
Software

Hardware



소프트웨어 정의 데이터 센터 접근 방식 (SDDC)

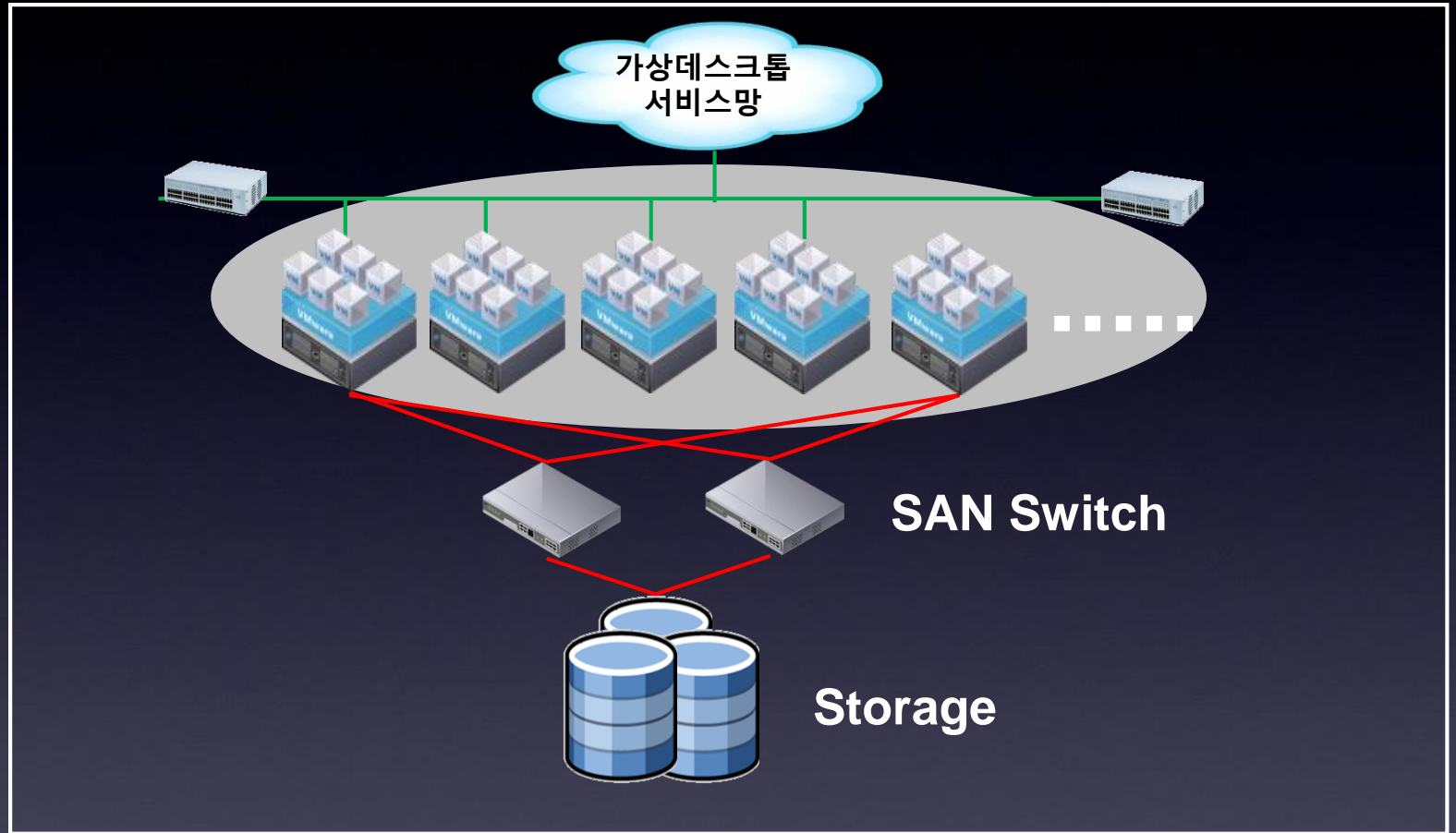
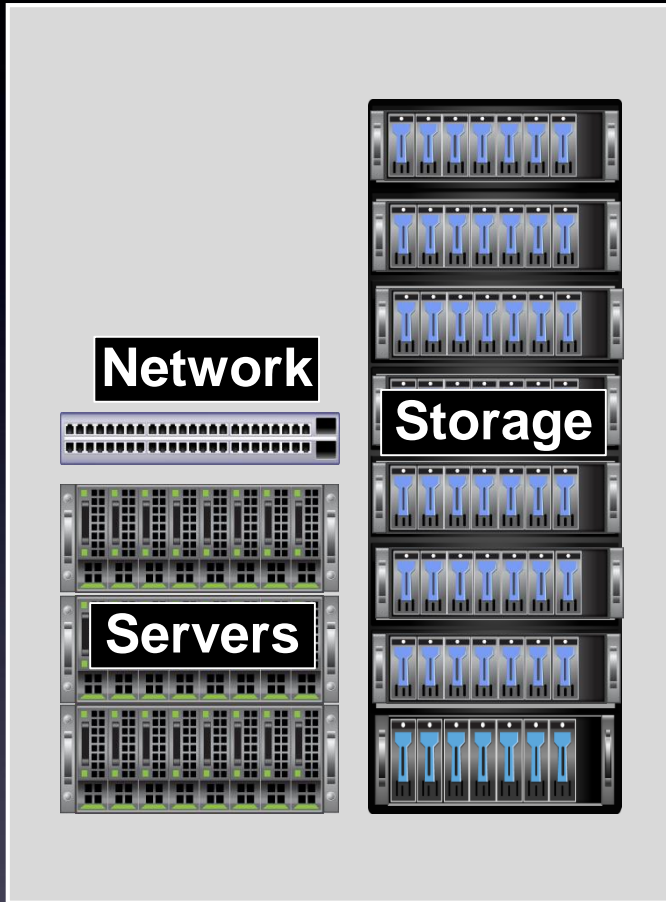
Automated Operational Model



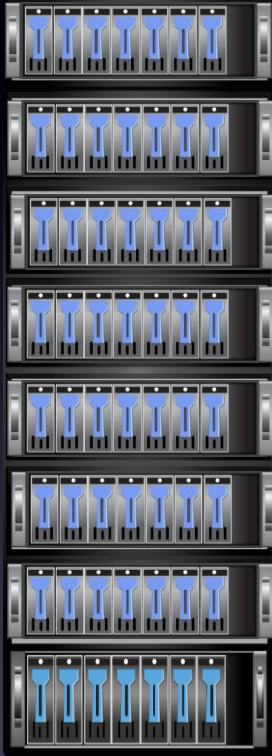
Software

Hardware



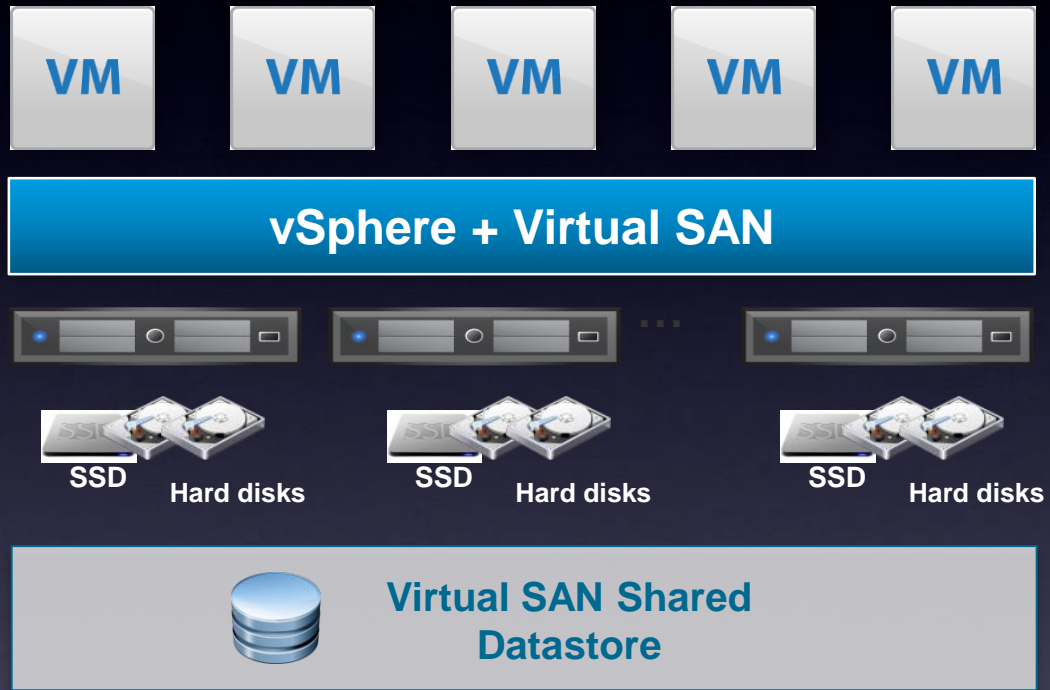


Storage



- 초기 과투자 (Over Sizing & Spending)
- 벤더 종속성 (Vendor Lock-in)
- Bottle-Neck
- Opex

스토리지 가상화 (Virtual SAN)

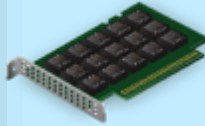


- 표준 x86 서버 & 내장 디스크
- 10만 IOPS per host / 6백만 IOPS per cluster
- 데이터 가용성 보장
- VM 단위 스토리지 정책 (QoS, FTT 등)
- 확장성 (Scale-Out)
- vSphere 내장(Built-in) 기술

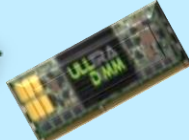
Virtual
SAN



SSD



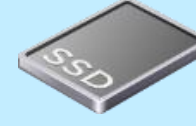
PCIe



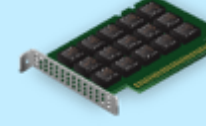
Ultra DIMM

Read and Write Cache

Caching



SSD



PCIe



Ultra DIMM

Writes cached first, Reads go direct to capacity tier



SAS/NL SAS/SATA/Direct-attached JBOD



Capacity Tier



Data Persistence



SSD



SSD



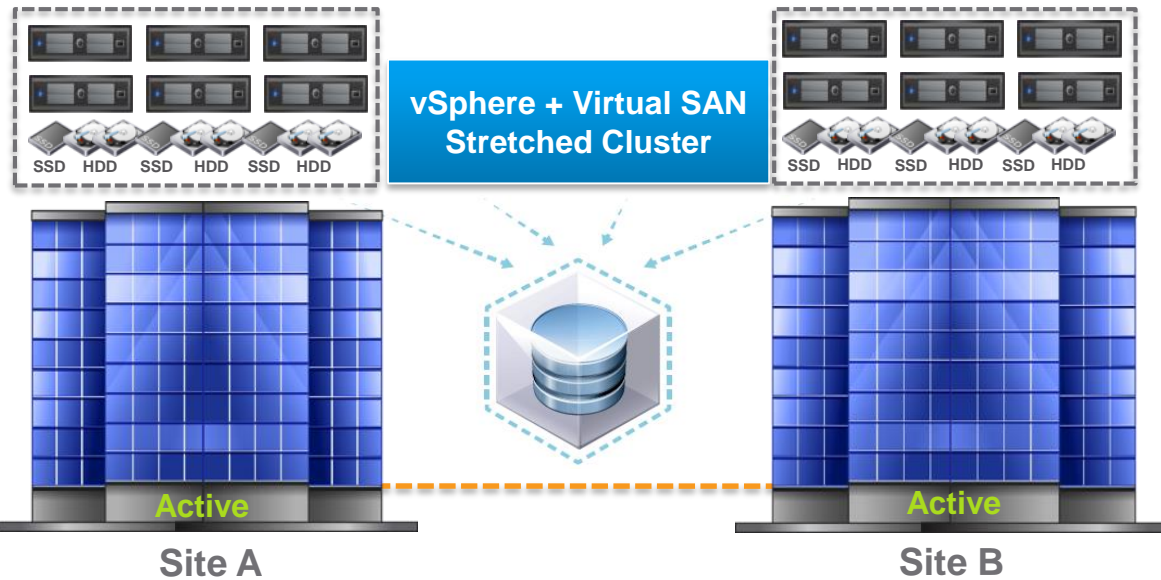
SSD

Capacity Tier
Flash Devices
Reads go directly to capacity tier

All-Flash 방식 VSAN의 특징

- SSD는 캐싱(Caching)뿐 아니라 데이터저장 기능으로 사용됨
- 호스트당 최대 100K IOPS 제공 / 클러스터 600만 IOPS 최대
- 2 Tier All-Flash 모델
 - Write-Intensive SSD로 100% 구성
 - Write-Intensive SSD와 Read-Intensive SSD 혼합구성 (비용절감시)

VSAN 확장클러스터



- Active-Active 또는 Active-DR
- Site간 데이터 복제
- 무손실, 무중단, RPO=0
- vCenter 통합관리

Performance (사례)

2분 21초

- 100VM 동시부팅

46분 45초

- 200VM 동시 백신 수동검사

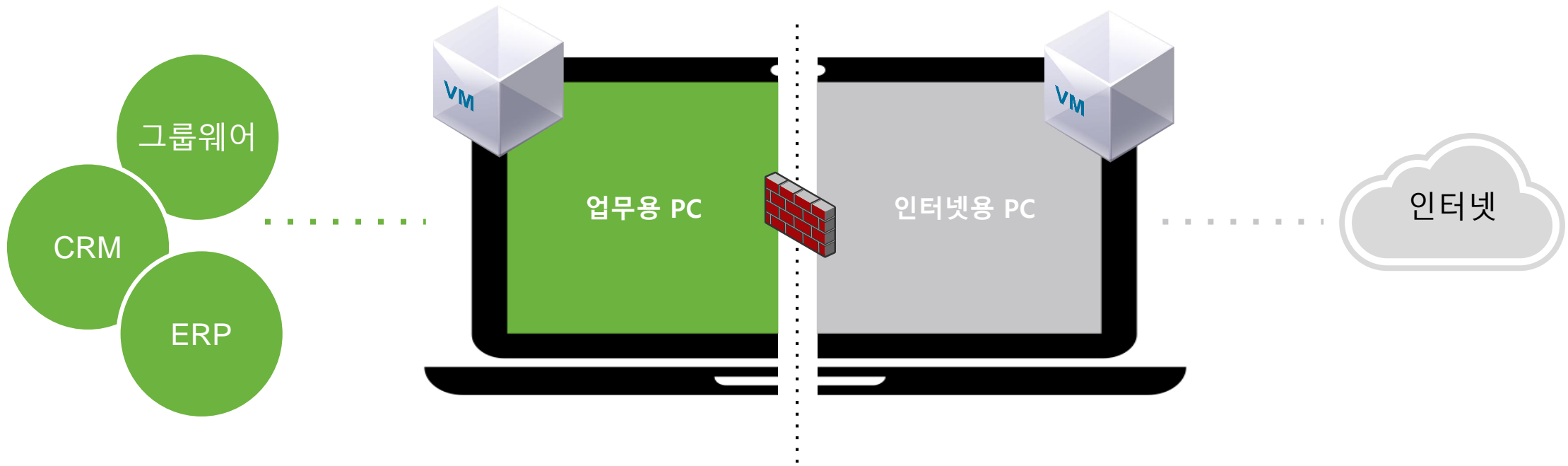
23초

- 무중단 마이그레이션 (vMotion)

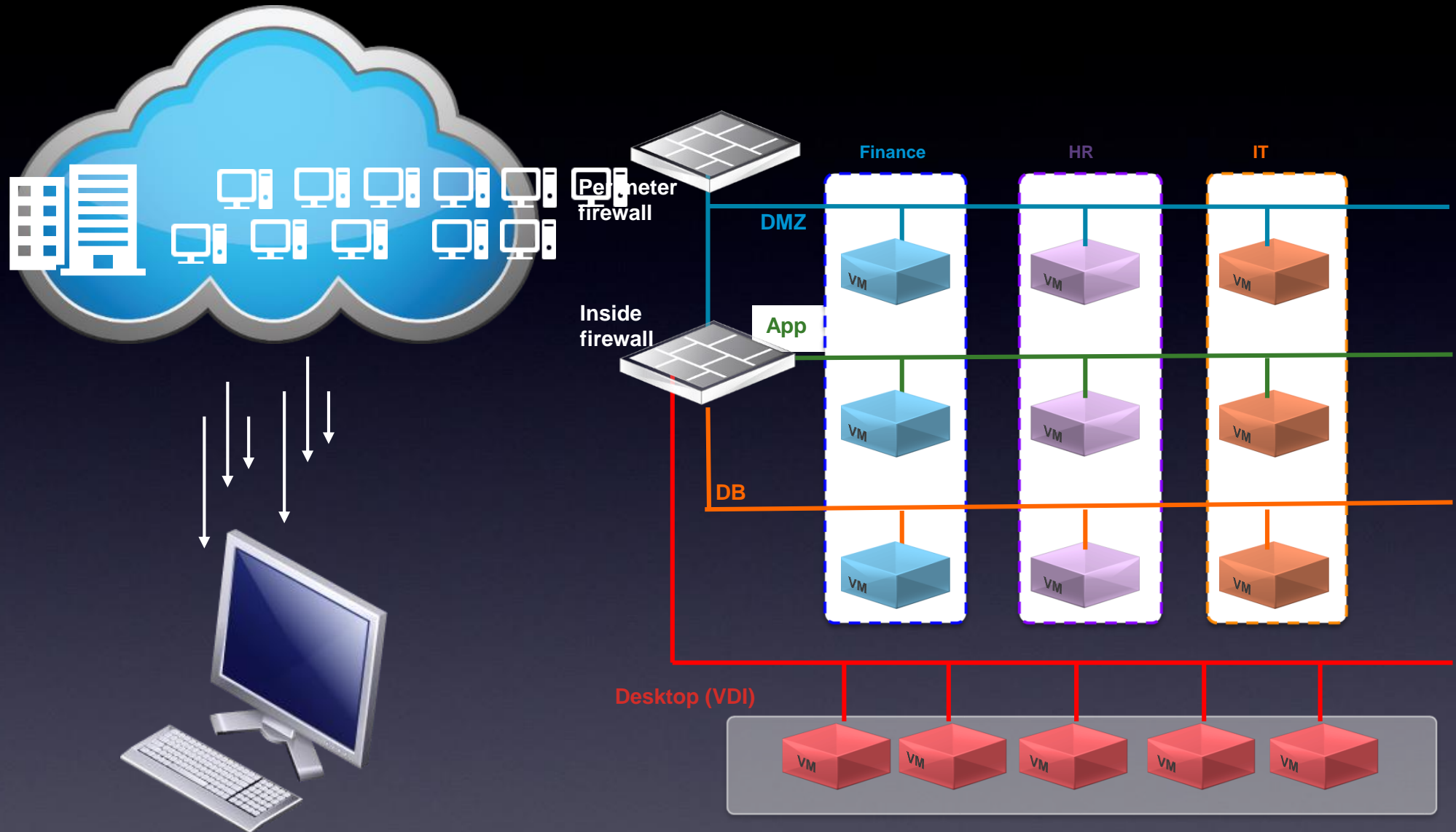
1분 21초

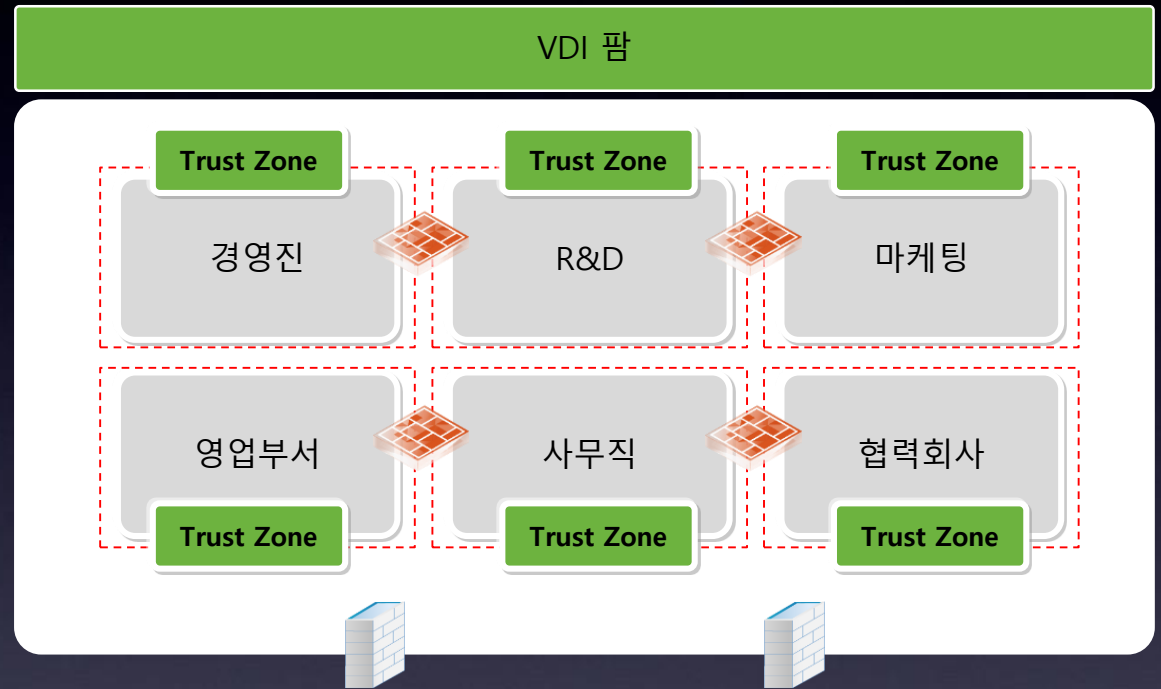
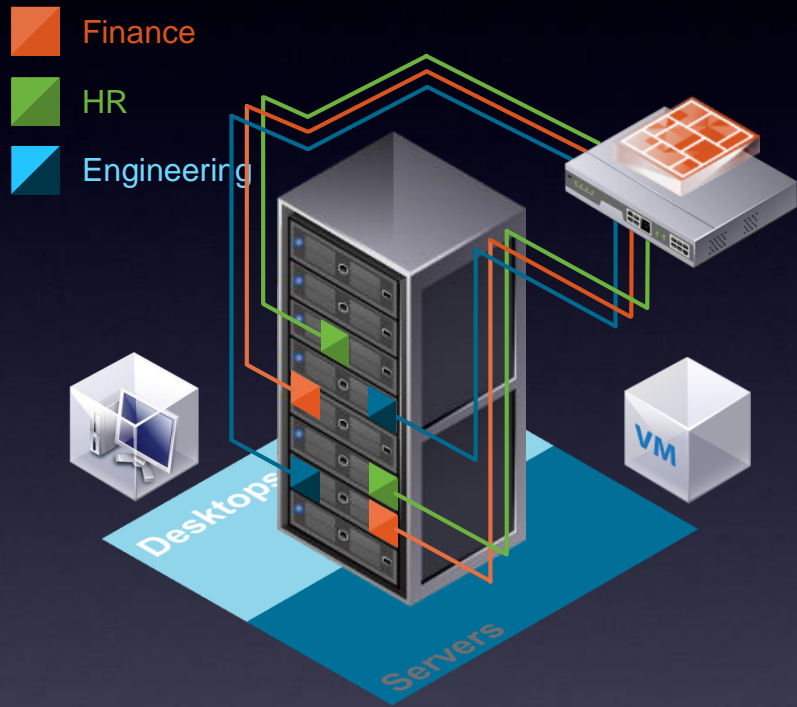
- 용량확장 (노드추가)

Security

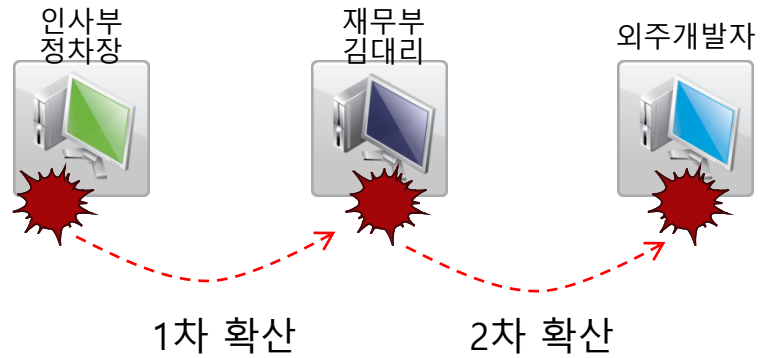


1. 보안은 충분한가?
2. 성능 향상 방법?





기존 VDI Farm



Secure VDI Farm

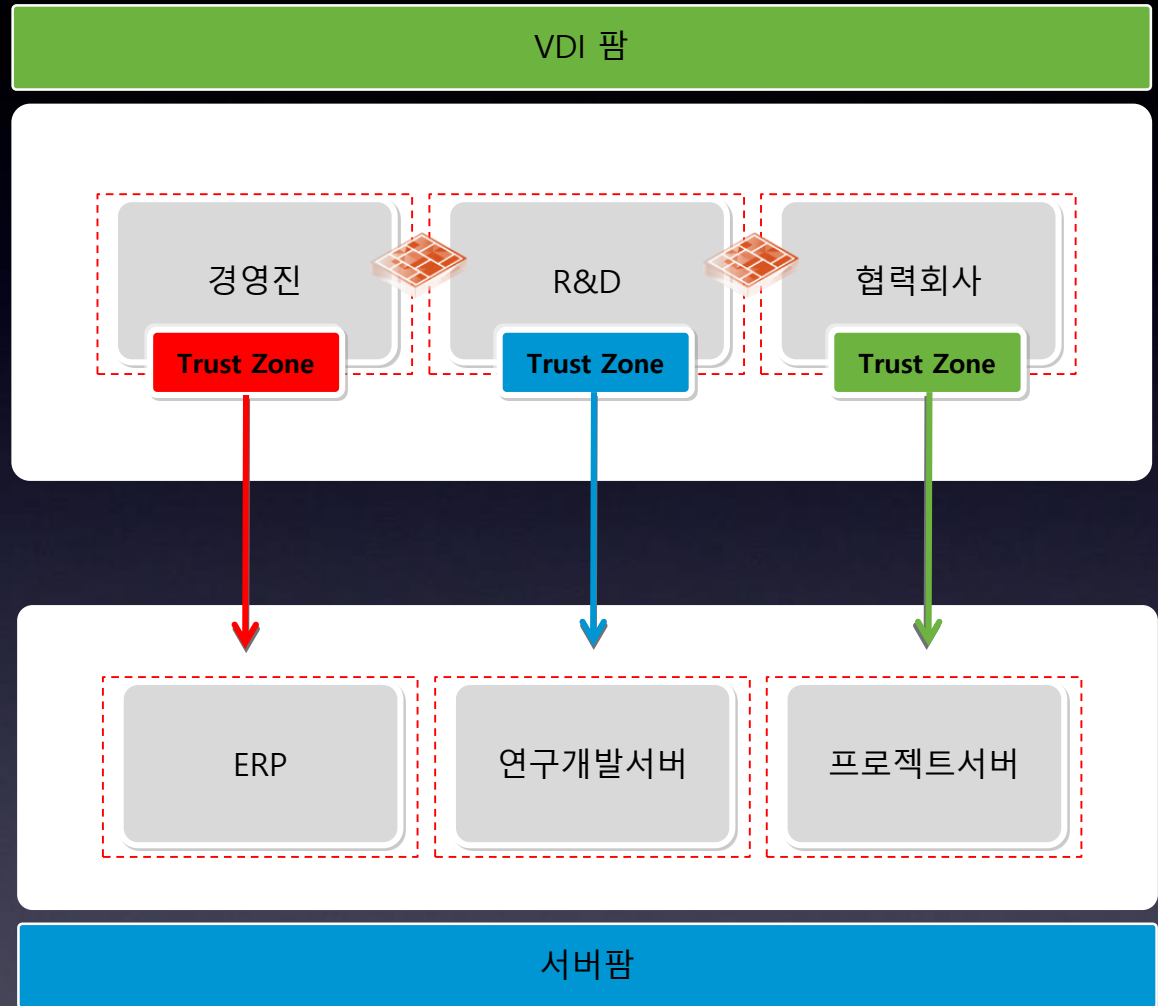
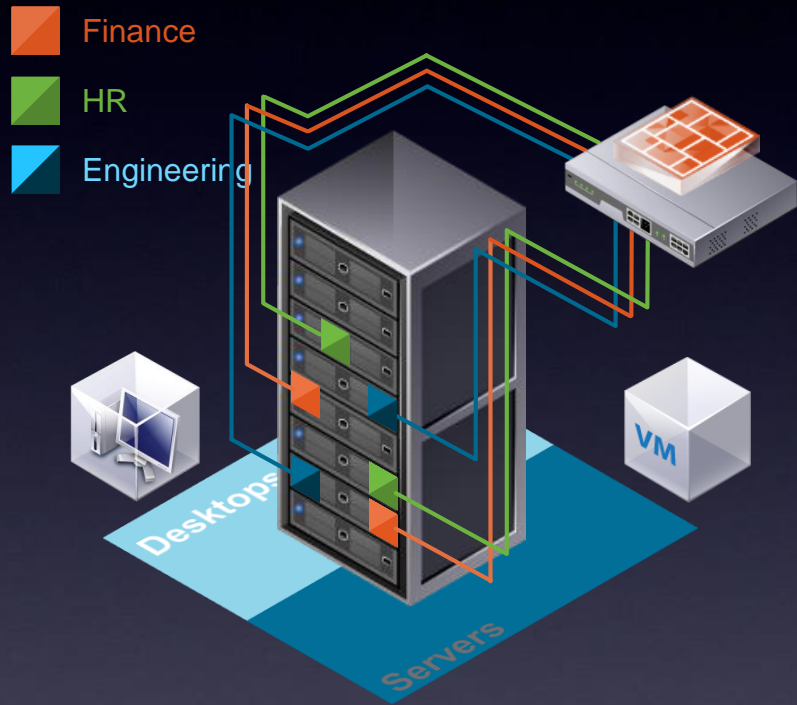


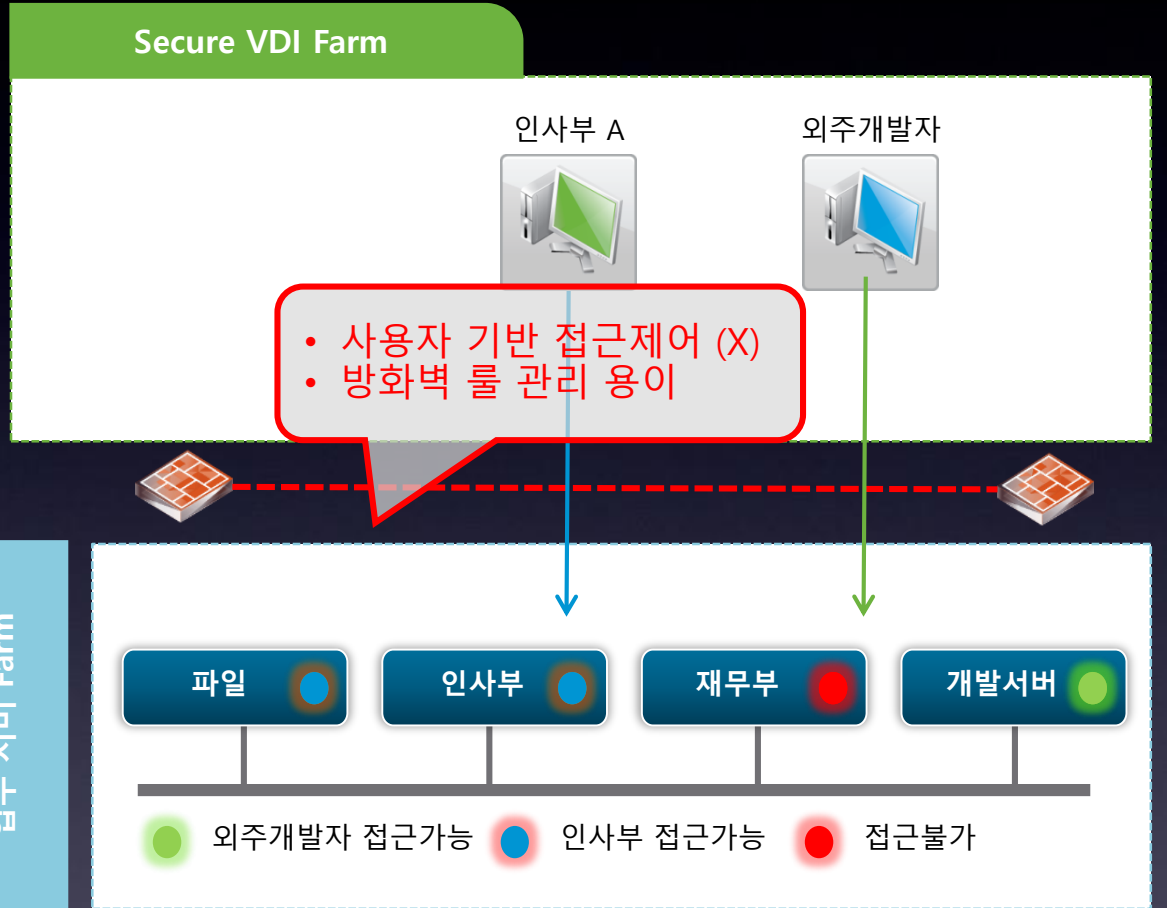
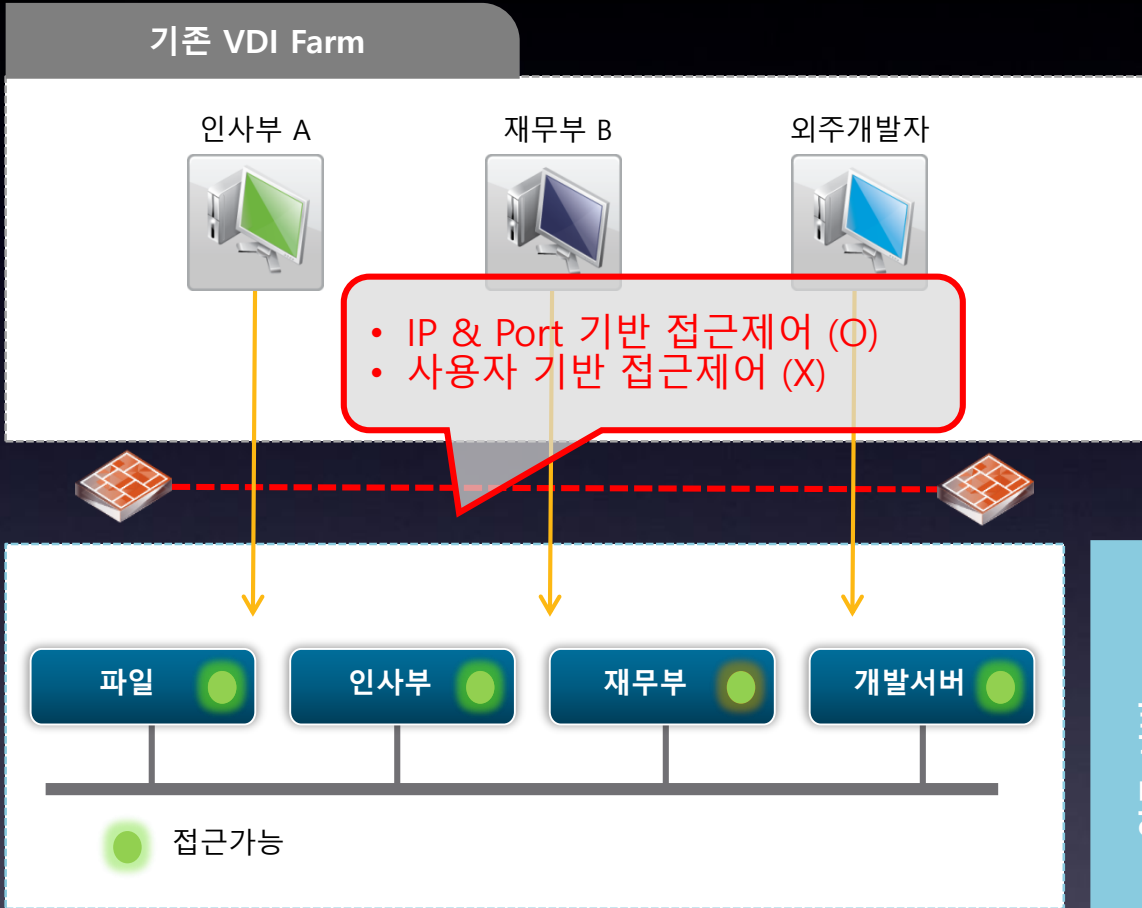
AS-IS

- VDI팜내 악성코드 유입시 확산방지 불가능
- VDI팜내 트래픽에 대한 이상감지 불가능
- VM별 백신SW에 절대적 의존

TO-BE

- 차세대 방화벽 및 백신SW 연동을 통해 VM간 트래픽 감시
- Agentless 백신SW 연동을 통해 VM간 악성코드 전이 감시
- 감염 의심 VM에 대한 자동격리



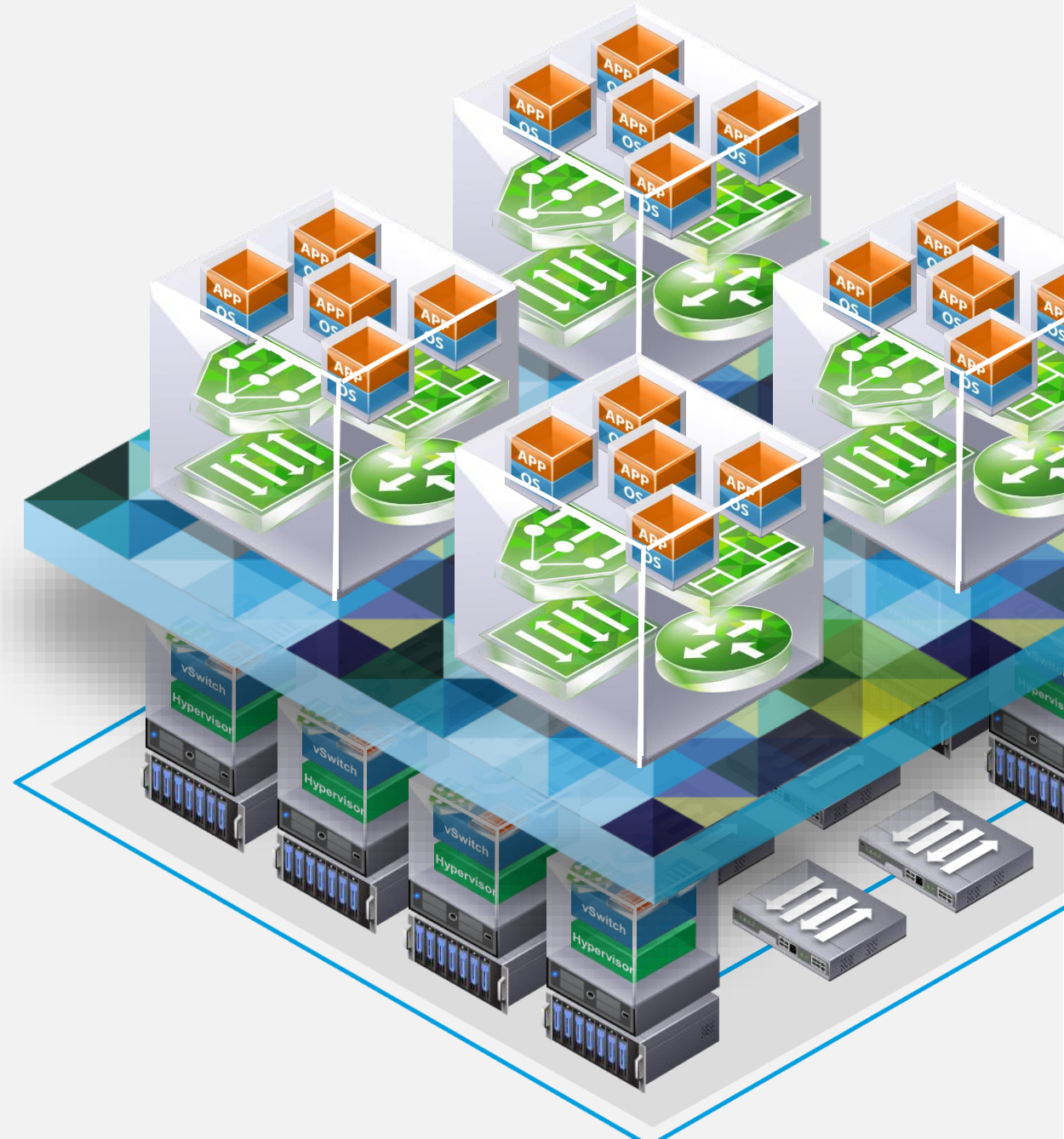


업무 서버 Farm

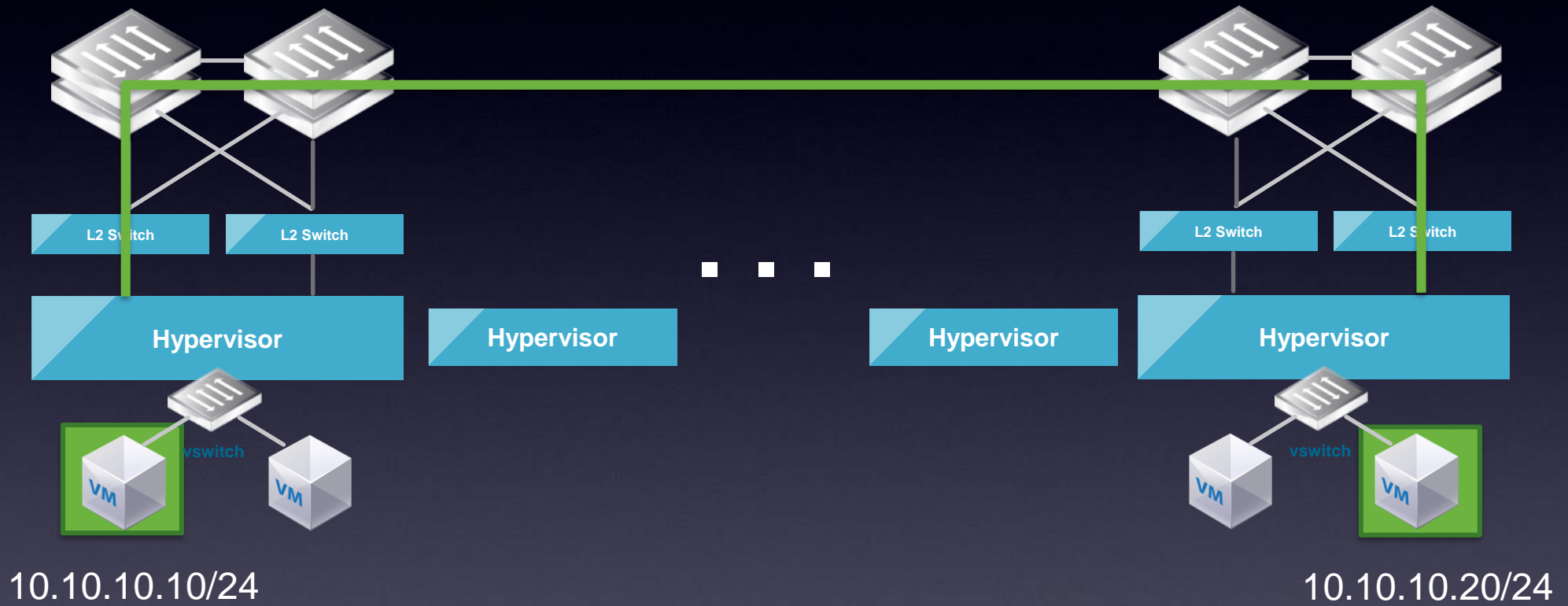
VMware NSX

네트워크 가상화

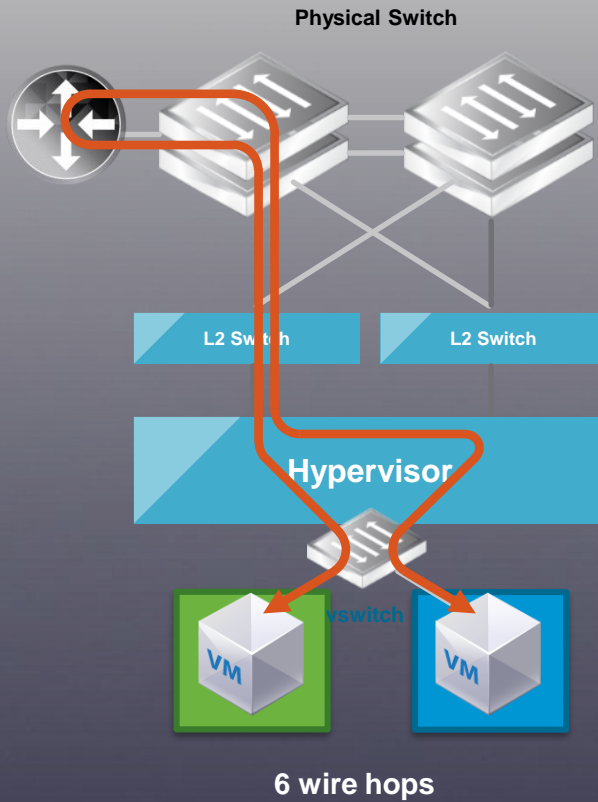
- ▶ “네트워크 하이퍼바이저”
- ▶ 논리적 스위치, 라우터
- ▶ Edge 방화벽, 분산 방화벽
- ▶ L4 로드밸런서, VPN 등



Before NSX

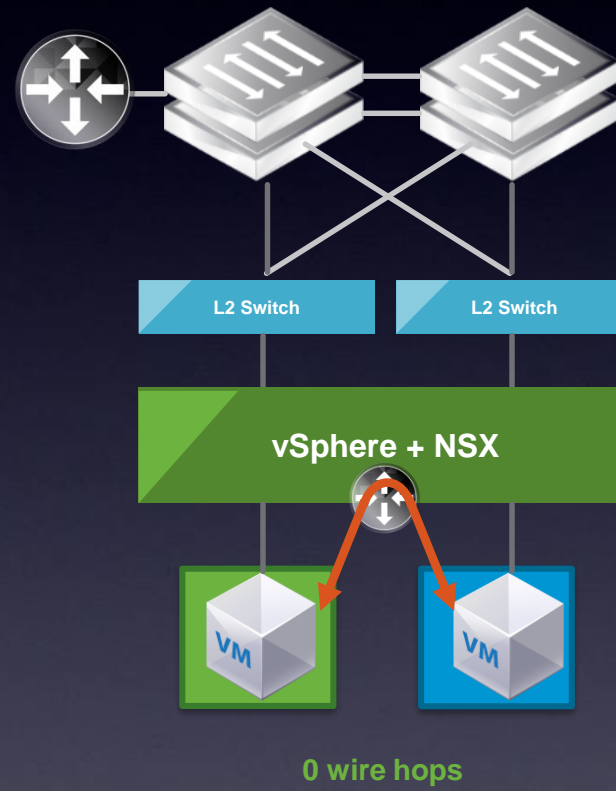


Before NSX

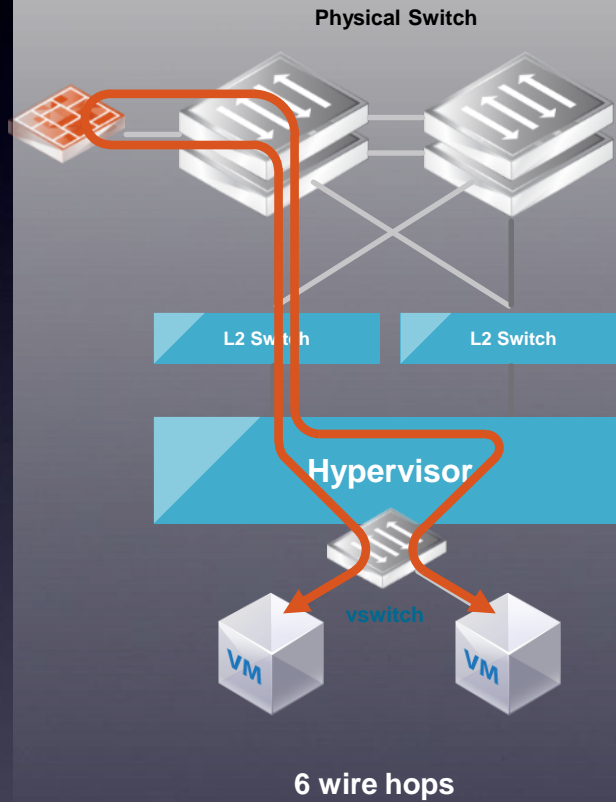


With NSX

Distributed Virtual Firewall

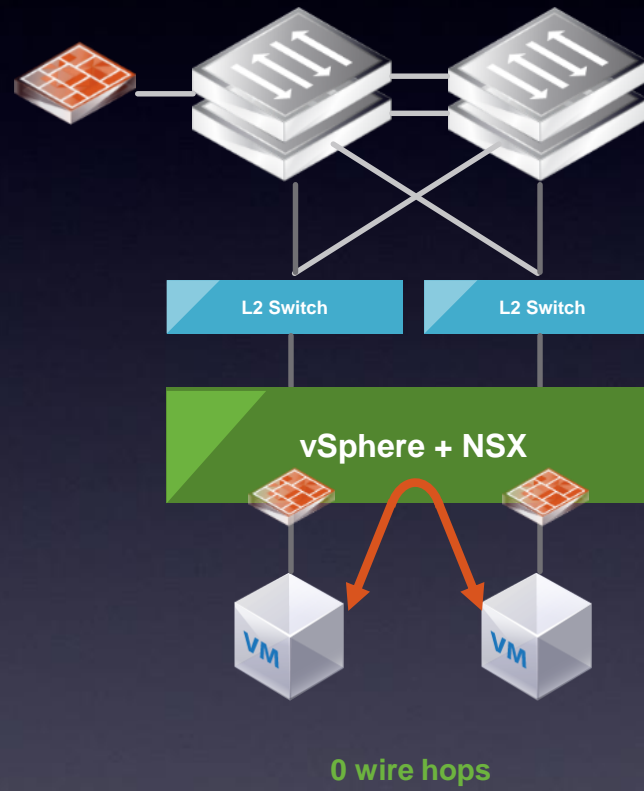


Before NSX



With NSX

Distributed Virtual Firewall



Before NSX



Hypervisor



With NSX



Hypervisor



Summary

Capex

(구축비용)

Opex

(운영비용)

Security

(보안)