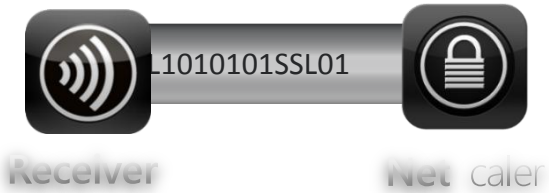
데스크탑 가상화를 활용한 망분리 방안

김준철 부장
Sales Engineer
Citrix Korea

Citrix = 토탈 클라우드 서비스

매끄러운
사용자 경험

안전한 접근



클라우드 솔루션

CITRIX

목 차

- 망분리 사업 전망
- 금융전산 망분리 가이드라인
- 표준 데스크탑 방안
- VDI 망분리 종류와 장단점
- 시트릭스 망분리 가이드
- M생명 구축 사례
- VDI 망분리 고려 사항

CITRIX®

최근 보안 사고 특징 및 망분리 사업 전망

CITRIX®

컵

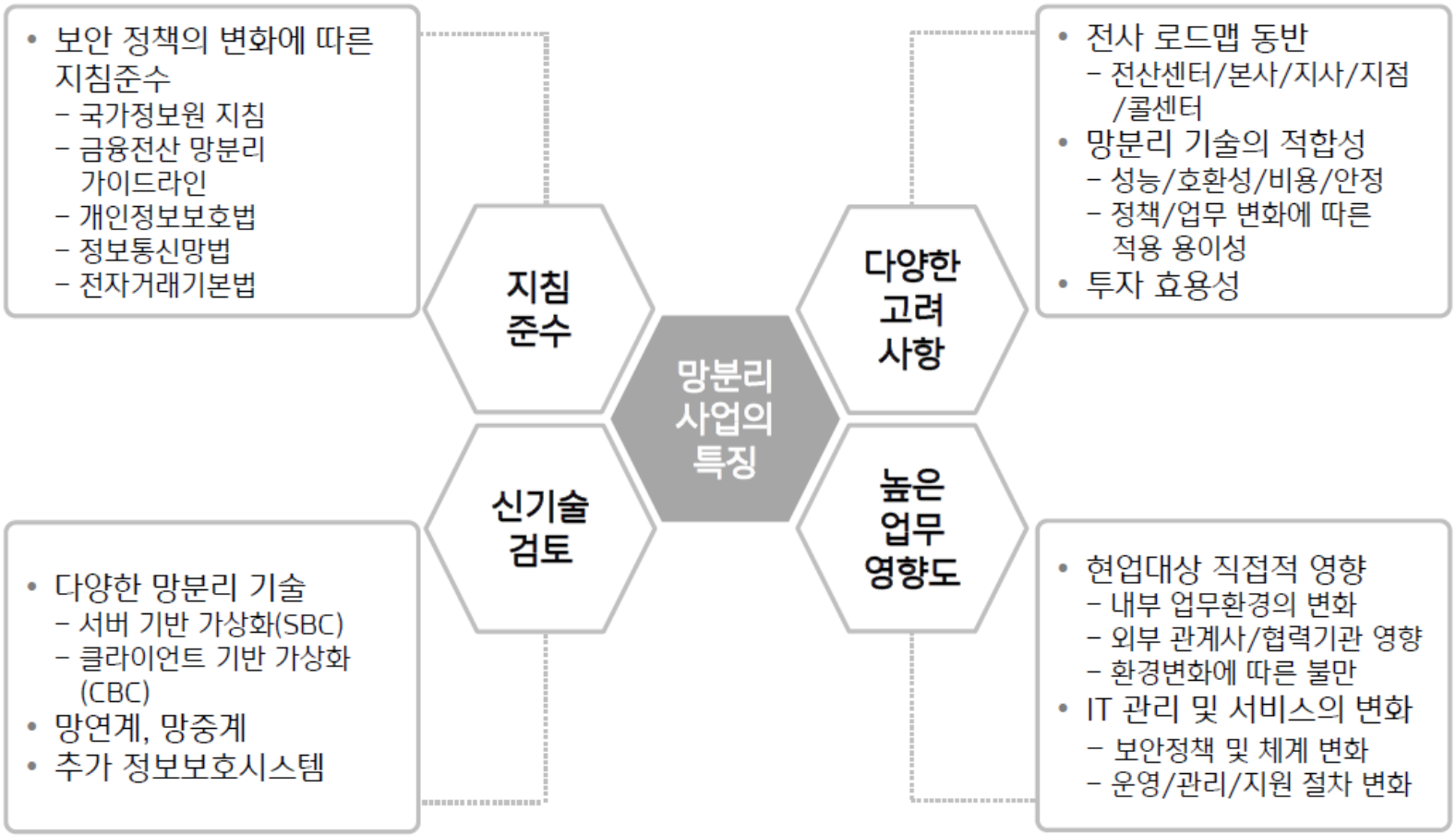
박스

최근 금융사고 형태

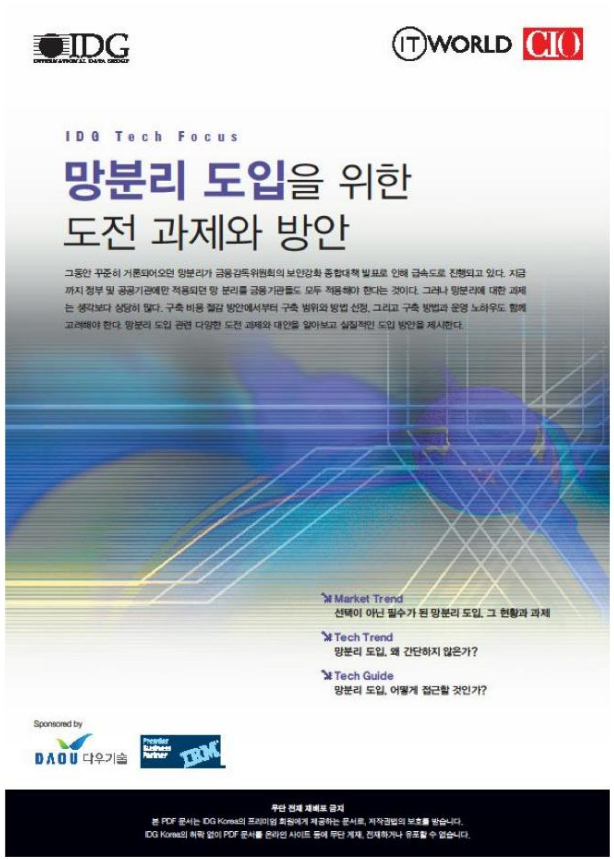
	3.20 사이버공격	카드사 고객정보유출
정의	✓APT 공격으로 인한 업무 무력화	✓내부접근자로부터의 정보유출
공격경로	✓직원PC악성코드 감염 -> PMS서버 감염 -> 악성코드배포	✓USB를 이용한 정보유출
가이드 라인	✓망분리 ✓인터넷 차단	✓망분리? ✓DRM? ✓ECM?

CITRIX®

망분리 사업의 특징


• 보안 정책의 변화에 따른 지침준수
– 국가정보원 지침
– 금융전산 망분리 가이드라인
– 개인정보보호법
– 정보통신망법
– 전자거래기본법
지침 준수
• 전사 로드맵 동반
– 전산센터/본사/지사/지점/콜센터
• 망분리 기술의 적합성
– 성능/호환성/비용/안정
– 정책/업무 변화에 따른 적용 용이성
• 투자 효용성
다양한 고려 사항
망분리 사업의 특징
• 다양한 망분리 기술
– 서버 기반 가상화(SBC)
– 클라이언트 기반 가상화 (CBC)
• 망연계, 망중계
• 추가 정보보호시스템
신기술 검토
• 현업대상 직접적 영향
– 내부 업무환경의 변화
– 외부 관계사/협력기관 영향
– 환경변화에 따른 불만
• IT 관리 및 서비스의 변화
– 보안정책 및 체계 변화
– 운영/관리/지원 절차 변화
높은 업무 영향도

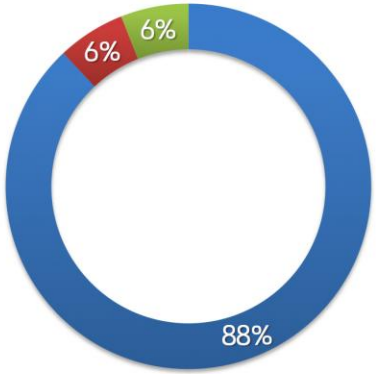
2014 망분리 시장 전망



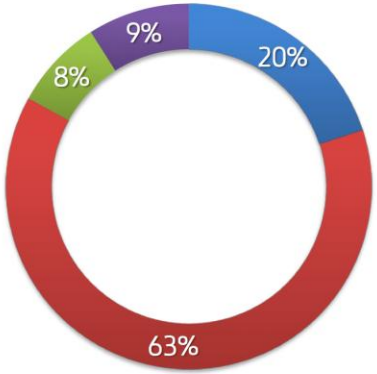
2013~2014 금융분야 망분리 도입 추이

- 망분리 도입 및 고려 (88%)
- 도입 시기 : 6개월 ~ 1년 이내 (83%)

도입 및 고려



도입 시기



- 2013년 : 성공사례 주시 및 관망 (데이터센터 망분리에 촛점)
- 2014년 : 카드 3사 개인정보 유출사고에 따른 빠른 계획 수립 및 추진 (전사적 망분리 고려)

CITRIX

Voice of Customer

- 발표된 가이드라인이 구체적이지 않아 **해석이 모호하다**
- 어떠한 지침과 법규를 준수하여야 하는지...

- 우리 기업에 가장 **효율적 망분리 방안(인터넷, 업무)**은 무엇인가?
- 기존 정보보호시스템(보안소프트웨어)과 **중복투자**되지 않는지...

- 다양한 **신기술 출현**에 따른 측정 기준 및 방법에 대한 **확신이 없다**
- 전문가 도움없이 **객관적이고 합리적 평가**가 어렵다

- IT기획, 서버, 네트워크, 보안, IT지원 등 **복잡한 이해관계**를...
- 협의체(TFT)를 구성하였으나 **결론 도출에 어려움**이 있다

- 망분리 도입 **범위와 대상**은 적절한가?
- 불법 접근과 내부 정보유출 차단에 대한 대응은 완벽한가?

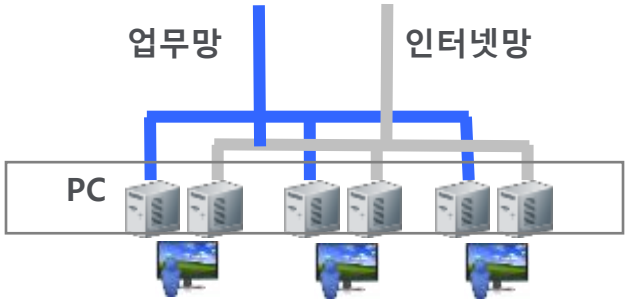
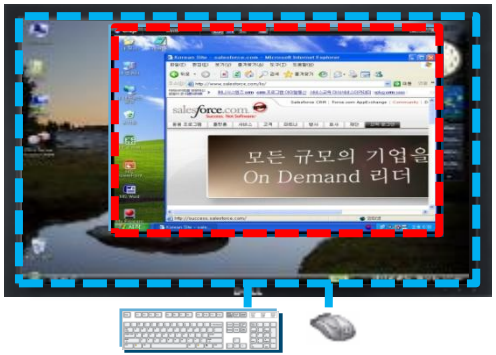
- 망분리 후 데이터 및 메일 전송에 대한 **편의성 확보**는 어떻게 할 것인가?
- 성능, 호환성 등에 대한 **사용자 불만**을 제거할 수 있는가?

CITRIX

금융전산 망분리 가이드라인

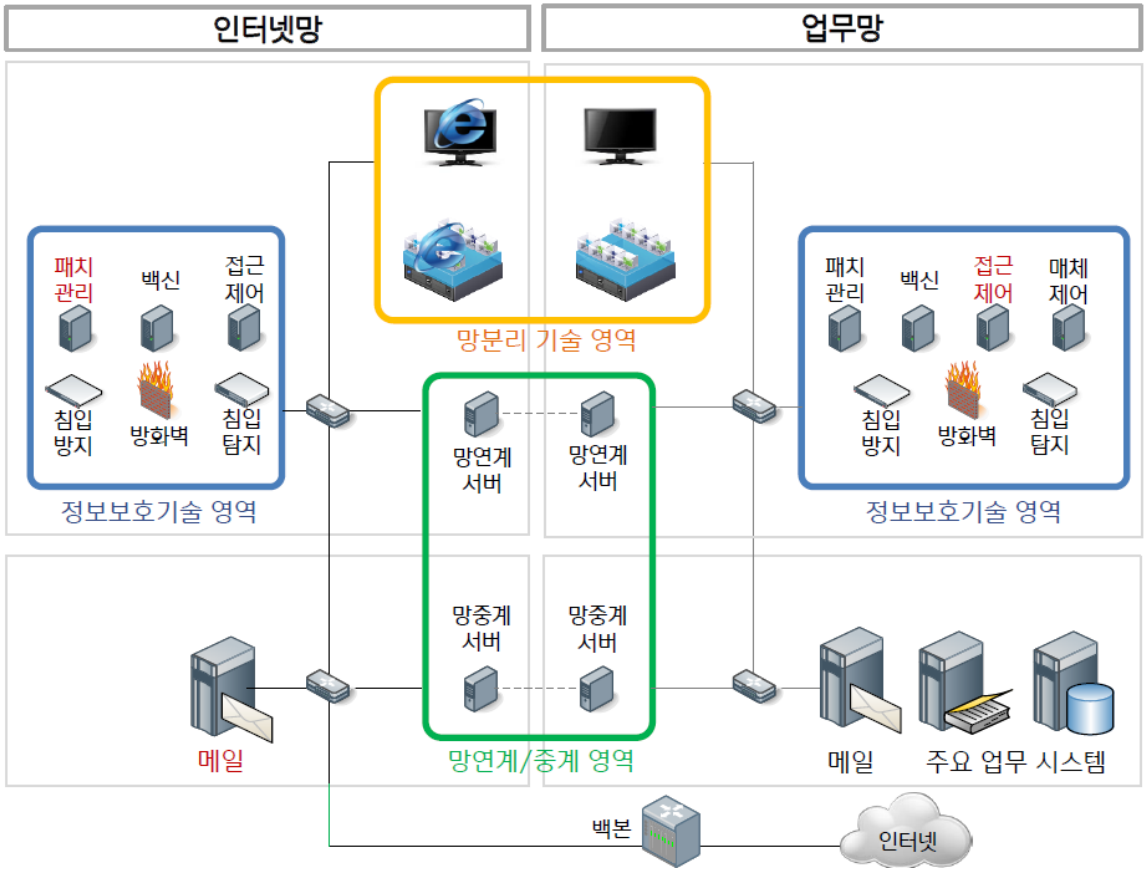
CITRIX®

금융전산 망분리 가이드라인

	물리적 망분리	논리적 망분리
정의	✓통신망을 물리적으로 업무용과 인터넷용으로 분리하고 별도PC 사용	✓통신망을S/W적으로업무용과인터넷용으로분리하고논리적으로분리된PC사용
대상	✓전산센터	✓본점, 영업점
구성안	 1인당 2개 PC	 1인당 1 PC

CITRIX

금융전산 망분리 가이드라인(전체)



주요 이슈

- 전산센터 물리적 망분리
  - 망분리 이후 메일 및 패치 서버 운영 방안
  - 주요시스템 IT담당자 접속 시 Two-Factor 인증
- 사용자 영역 망분리
  - 망분리 기술 선정
  - 망분리 이후 빈번한 파일 전송 시 업무 불편 해소

Key Success Factor

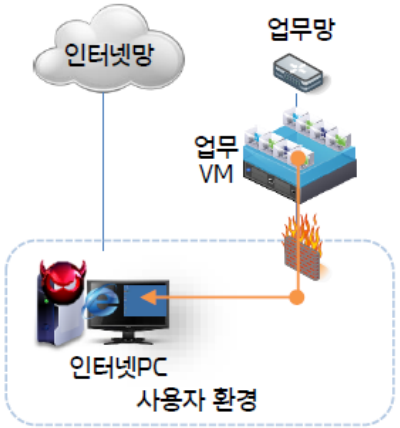
- 메일 및 패치서버 분리
  - 망연계/중계 구현
- 안전한 전송 구현
  - 단방향 암호화 통신
  - 전송 시 악성코드/위변조 검사, 승인절차
- 망분리에 따른 기존 정보보호시스템 중복투자 제거
- 메시지, OTP 등 효율적 인증 방식 선정

CITRIX

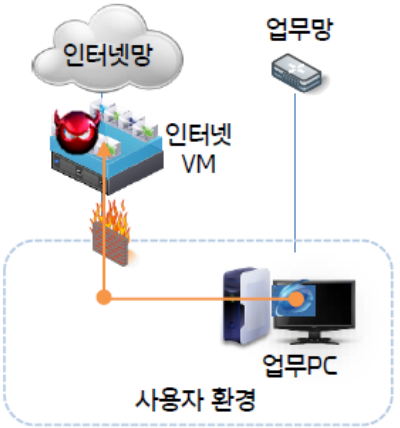
금융전산 망분리 솔루션 종류

물리적 망분리

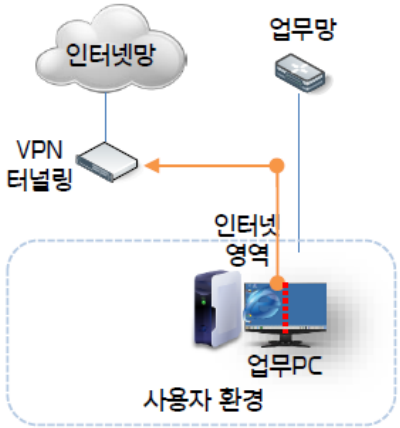
VDI 업무 망분리



VDI 인터넷 망분리



CBC 인터넷 망분리



유형별 특징

- 전산센터 물리적 망분리에 적용
- 100유저 이하의 소규모 사업장 도입 사례 많음
- 대규모 사업장의 경우 일부 영역 적용

- 높은 망분리 도입 비용을 스마트워크 환경 활용으로 인한 비용효율 확보
- 동시 다발적 업무유형 분석이 중요함

- 업무 영역 VDI 기술 적용 대비 낮은 도입비용
- 인터넷 영역 감염시 빠른 복구 이점

- 1대 PC를 논리적으로 격리 후 VPN 터널링을 통한 인터넷 사용
- 적은 비용으로 IE만 격리 시 적합
- 인터넷 영역 SW 사용 제약 검증 및 업무 영역 SW 호환성 검증

표준 데스크탑 방안

CITRIX®

이제는 사용자 PC 관리 변화가 필요한 때!

KBS·MBC·YTN 정보전산망 완전 마비

KBS, MBC, YTN, 신한은행, 농협 정보 전산망 완전 마비

경찰, 사이버 테러 여부 수사

(SBS 뉴미디어부)

"뚫릴 때까지 공격한다…'APT 공격'대응 방안 없나?"

보안 전문가 5인이 말하는 APT 대처 방법

2013년 05월 02일 (목) 17:52:46 최승호 기자 midas@itdaily.kr

지능형지속위협(APT : Advanced Persistent Threat) 공격에 대한 관심이 다시 높아지고 있다. KBS, MBC, YTN, 농협 등 전산망을 무너뜨렸던 3.20 사이버 대란이 APT 공격으로 밝혀졌기 때문이다.

APT 공격은 어제 오늘 발생한 일이 아니다. 2011년 SK커뮤니케이션즈 3500만명과 넥슨 1320만명의 개인정보유출, 농협 전산망 마비 등 사이버 사건이 모두 APT 공격으로 발생한 일이다.

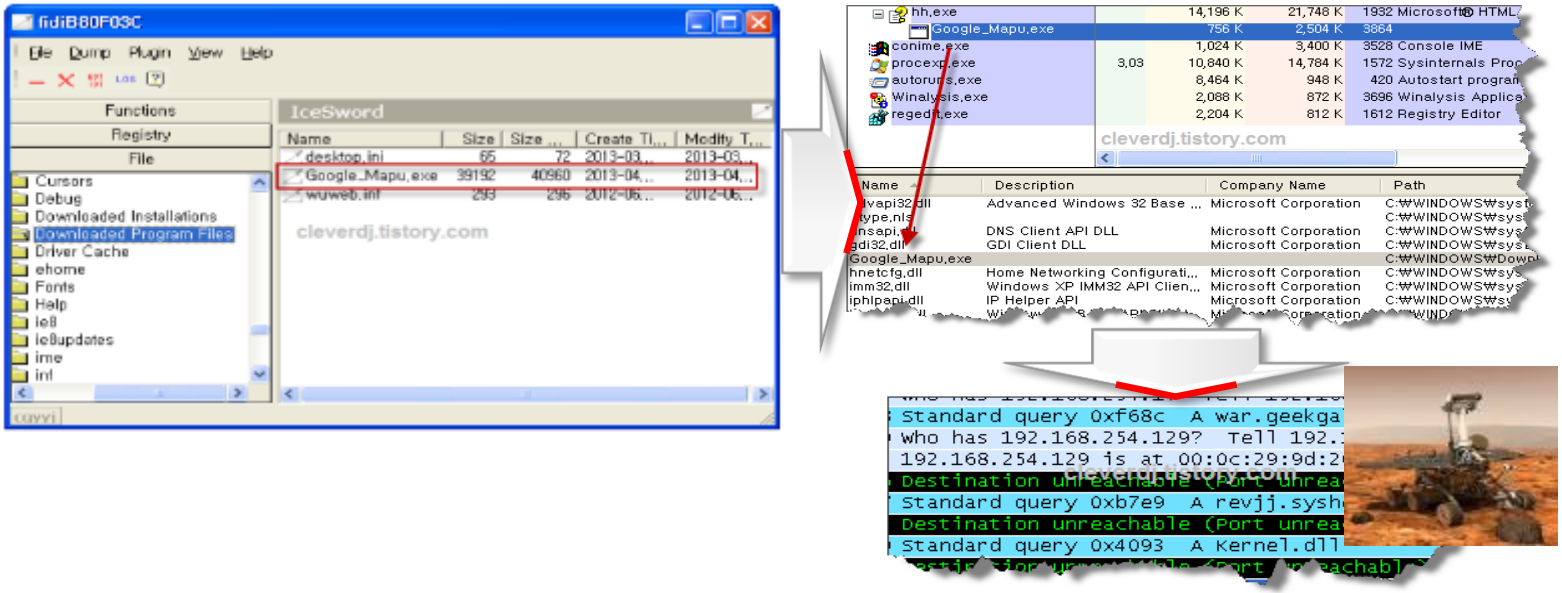
APT공격은 특정 대상을 표적으로 내부 시스템의 취약점을 이용해 침투한 뒤 한동안 이를 숨겨놓았다가 주요 정보를 유출하거나 시스템을 무력화하는 데 쓰인다. 기존의 안티바이러스 프로그램에 탐지되지 않도록 악성코드를 제작할 수 있고, 자체 전파하는 바이러스와 달리 다량의 트래픽을 발생시키는 것도 아니어서 네트워크 관리자의 감시도 쉽게 피할 수 있다.

이처럼 APT 공격의 경우 알려지지 않은 새로운 해킹 기술을 사용해 관리자 계정을 탈취하거나 은밀히 상대방의 PC에 잠입하는 등의 기술을 사용해 공격한다.

CITRIX

APT 공격 예

- 첨부파일 클릭과 동시에 백그라운드로 백도어가 복사되고 서비스로 등록됨



Next Attack ??

CITRIX®

전통적인 기업 PC 구조

사용자 어플리케이션
기업 데이타
+ 악성 코드 + 데이타

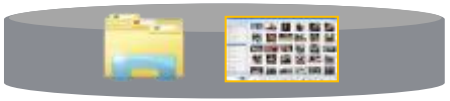
기업 어플리케이션

Windows OS 이미지

CITRIX

데스크탑 초기화 방식

데이터 중앙 저장



- 사용자 데이터 별도 관리
- 관리자에 의해 중앙 관리

로그오프시 Reset

- 재부팅, 로그온시 설치된 모든 프로그램 Reset
- 공통 OS, 업무 어플리케이션 이미지를 공유
- 로그온 시 새로운 Clean이미지를 배포

1 : 1

새 이미지 배포

1 :n

기존 PC 방식

데스크탑 공유 Reset 방식

CITRIX

데스크탑 초기화 방식 장점

보안/안정성 향상

사용자 컴퓨팅 환경 표준화

VDI 구축 /운영 비용 절감

사이버 공격시 가장 신속한 업무 복귀

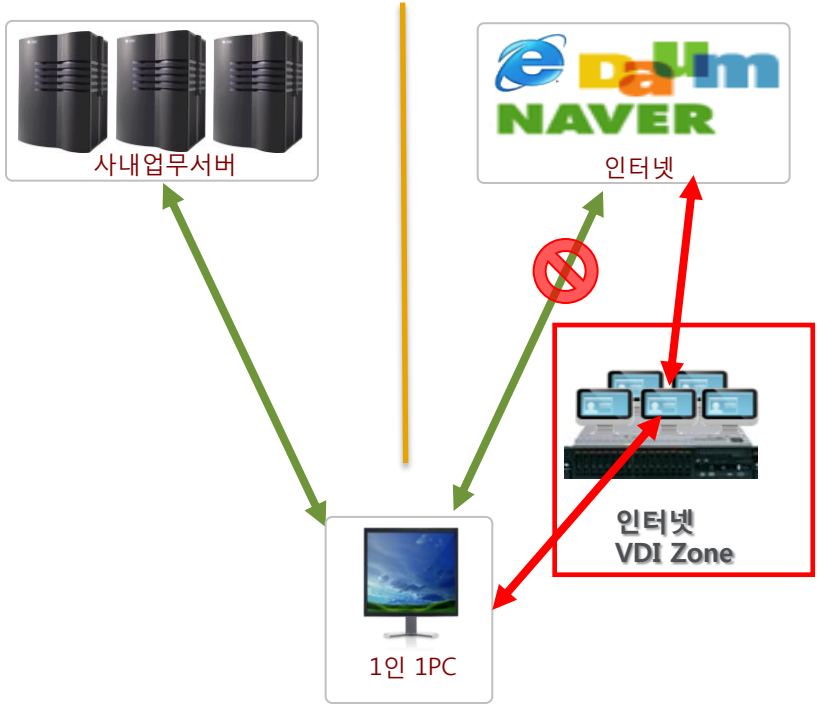
CITRIX®

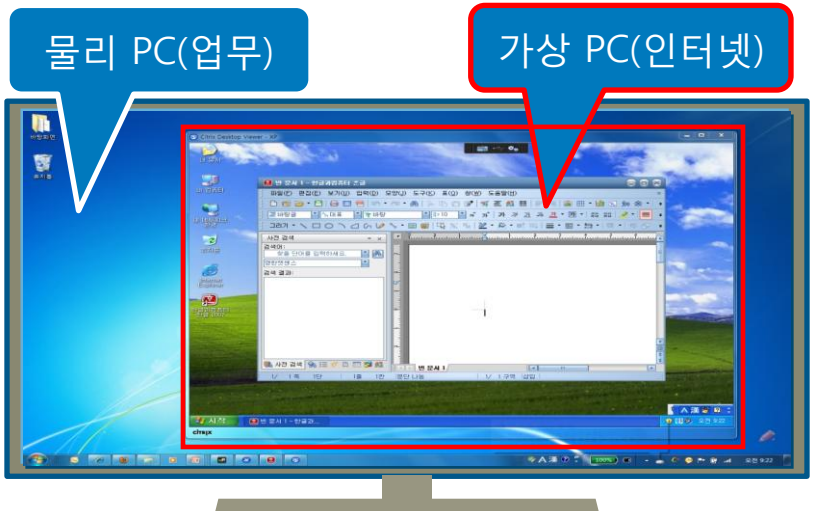
어떻게 망분리 할것인가?
VDI 망분리 종류와 장단점

CITRIX®

망분리 타입(인터넷 망분리)

인터넷망분리(PC : 인터넷 차단, 업무망 접속)





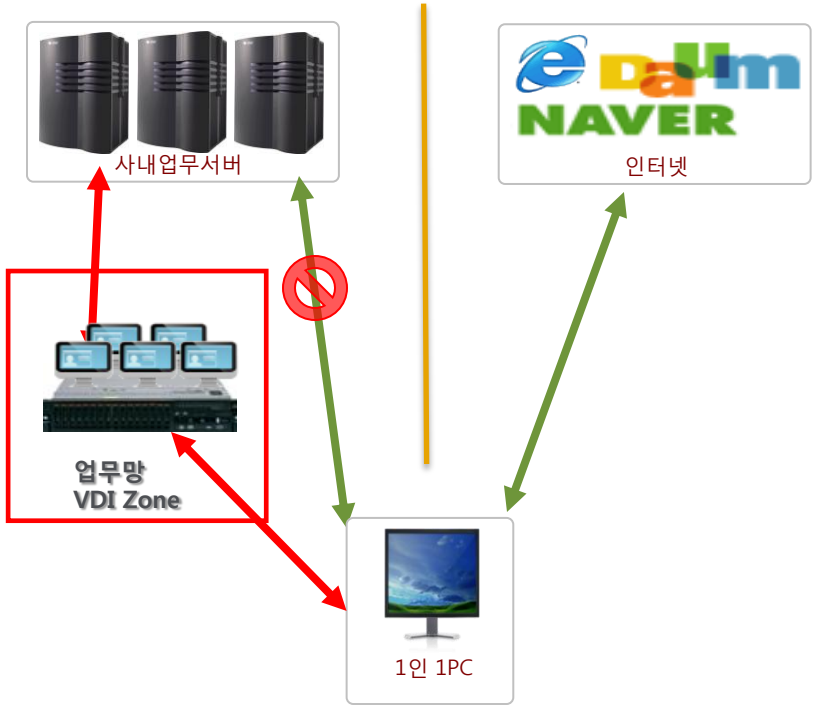
인터넷 망분리

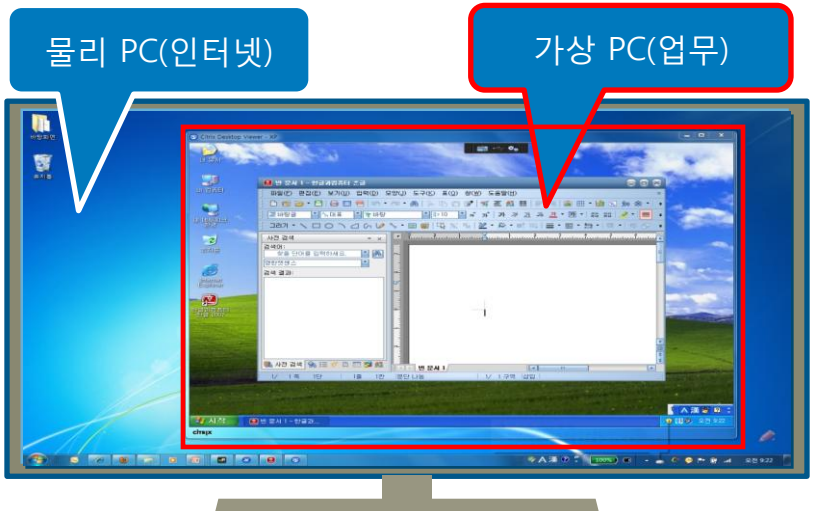
장점	단점
• 가장 빠르게 적용 • 보안이 뛰어남 • 업무환경 변화 적음 • 업무망분리에 비해 저비용	• 스마트워크 업무 불가

CITRIX

망분리 타입(업무망분리)

업무망분리(PC : 인터넷접속, 업무망 차단)





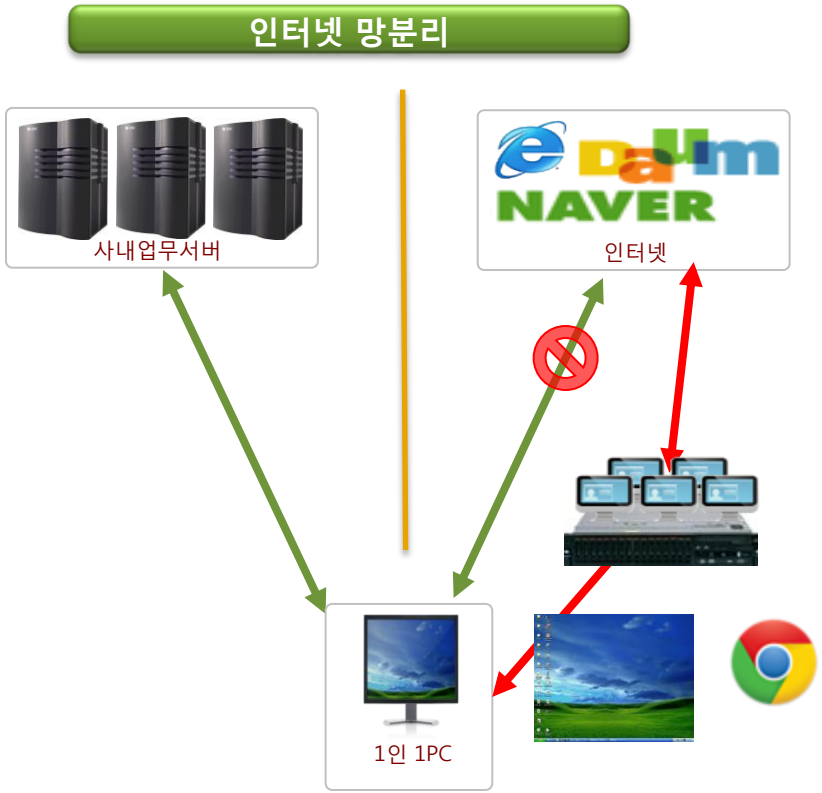
업무망 망분리

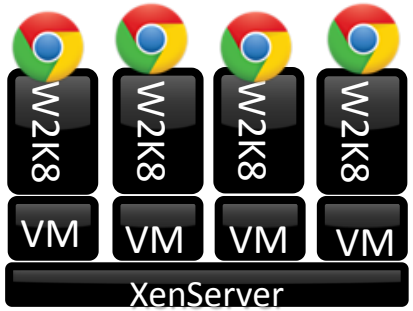
장점	단점
• 장애, 사이버공격에 신속한 대응 • 스마트워크 지원 • 정보중앙 저장 및 유출 방지	• 업무환경 변화 많음 • 인터넷 망분리에 비해 고비용

시트릭스 망분리 가이드

CITRIX®

망분리 타입-1 (인터넷 망분리)





SBC (Server Base Computing)

- 서버당 **200 User**
- 브라우저만 제공
- 용도 : 인터넷 검색
  개인 이메일

Product : Citrix XenApp

VDI (Virtual Desktop Infra)

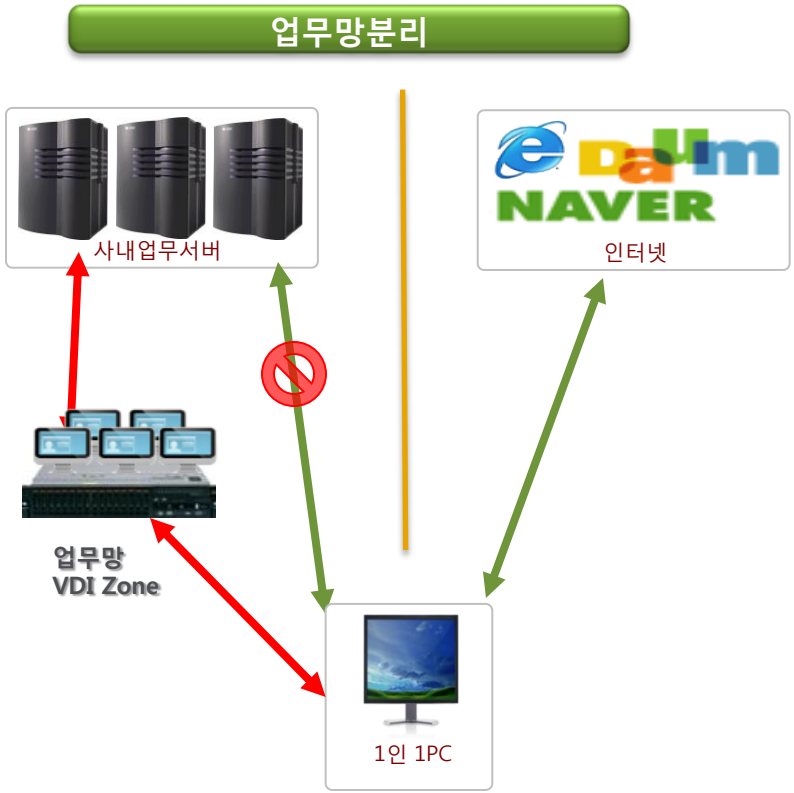
- 서버당 50 User
- OS 제공
- 용도 : 인터넷 뱅킹
  인터넷 쇼핑

Product : Citrix XenDesktop

1000 명 규모 인터넷망분리 시니리오 (500VM 필요,동시접속 50%)	
Full VDI (100%)	SBC(80%) + VDI (20%)
VDI 서버 10대	SBC 서버 2대 VDI 서버 2대

CITRIX

망분리 타입-2(업무망분리)



1000 명 규모 업무망분리 시나리오 (1000VM 필요,동시접속 100%)		
	Dedicate VM	**Reset VM**
서버수량 (서버당 50VM)	20대	20대
스토리지* (VM당 30GB)	**30TB** = 30GB * 1000VM	**1.3TB** = 30GB * 1 + 1GB* 1000VM
장점	• 100% 개인화 지원	• 중앙 단일 이미지로 표준화 및 보안이 뛰어남. • 구축비용 감소.
단점	• 기존 PC의 관리방식과 동일하여 표준화 및 관리 어려움.	• 어플리케이션 호환성 테스트 필수

* 개인 데이터 저장공간 제외됨.

CITRIX

M생명 구축 사례

다우기술 VDI 지원팀
김정도 부장
(jdkim@daou.com)

CITRIX®

사업 추진 개요

2011년 4월 가상 데스크탑 1,000VM 구축 추진

2011년 9월 가상데스크탑 1,000VM 이행

2012년 4월 A사 제품으로 1,000VM 구축완료

2013년 4월 가상데스크탑 500VM 확대 구축 추진

2013년 5월 Citrix 1,500VM 이관 이행

2013년 11월 Citrix 1,500VM 구축 완료

확장 추진 시 도전과 기회

- **취약한 네트워크 인프라**
- **전사 화상회의 문화의 확산 요구**
- TCO
- **변화관리**
- Winsows XP EOS

- **전사 IPT(IP Telephony) 전환**
- **금융권 망분리 의무 적용**
- Windows XP EOS

CITRIX®

Citrix 선정 배경

#1 UC 환경에 최적화된 VDI환경 제공

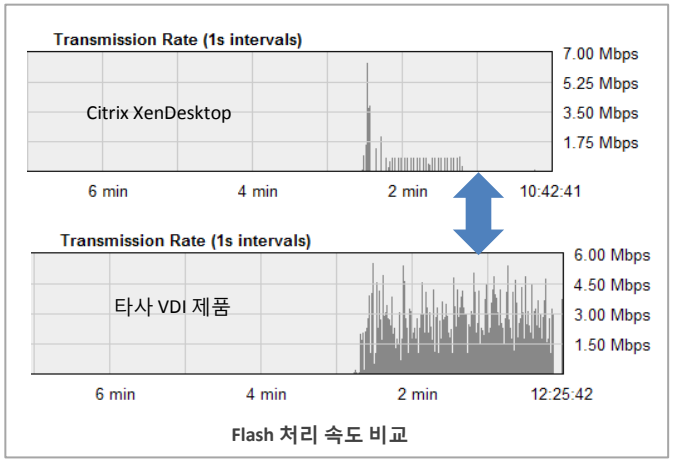
	단말기 #1	단말기 #2	단말기 #3	결과
단말기 모델명	모델 A	모델 B	모델 C	
단말기 Spec	Dual-core AMD G-Series T48E 1.65 GHz	Dual-core AMD G-Series T48E 1.65 GHz	Dual-core AMD G-T56N 1.65 GHz	Thin Client 단말기 3ea로 Test결과 영상/오디오 Delay 없이 우수함.
적용 Citrix Receiver	Receiver 3.1적용	Receiver 3.1적용	Receiver 3.1적용	Receiver 3.1버전에서 가장 최적화 됨.
USB 마이크폰	MS LX-3000	MS LX-3000	MS LX-3000	오디오 출력 우수
USB 웹캠	MS HD Cinema	Logitech C210	Logitech C210	비디오 출력 우수

CITRIX®

Citrix 선정 배경

#2 네트워크 최적화 기능 제공

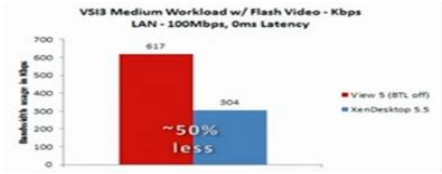
- ✓ 타사 대비 수배 빠른 Flash기반 웹 프로그램과 동영상 재생 속도 성능
- ✓ 로컬클라이언트 장치 또는 서버의 성능을 고려한 플래시 재생으로 성능 및 확장성 개선
- ✓ 타사 대비 수배 작은 네트워크 대역폭 점유

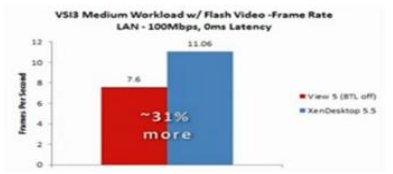


Flash 처리 속도 비교

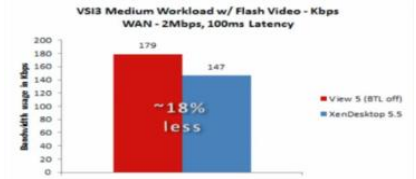
대역폭 프레임 Rate

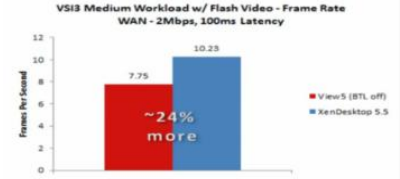
LAN 환경





WAN 환경





Citrix HDX for Multimedia 지원 요건

- ✓ 사용자 단말단에 설치된 Codec 을 통해 가속.
- ✓ Virtual Desktop에 IE 7 이상, Adobe Flash Player 10 이상 필요.
- ✓ AVI, MPEG, MPG, ASF, WMA, WMV 파일 포맷 지원

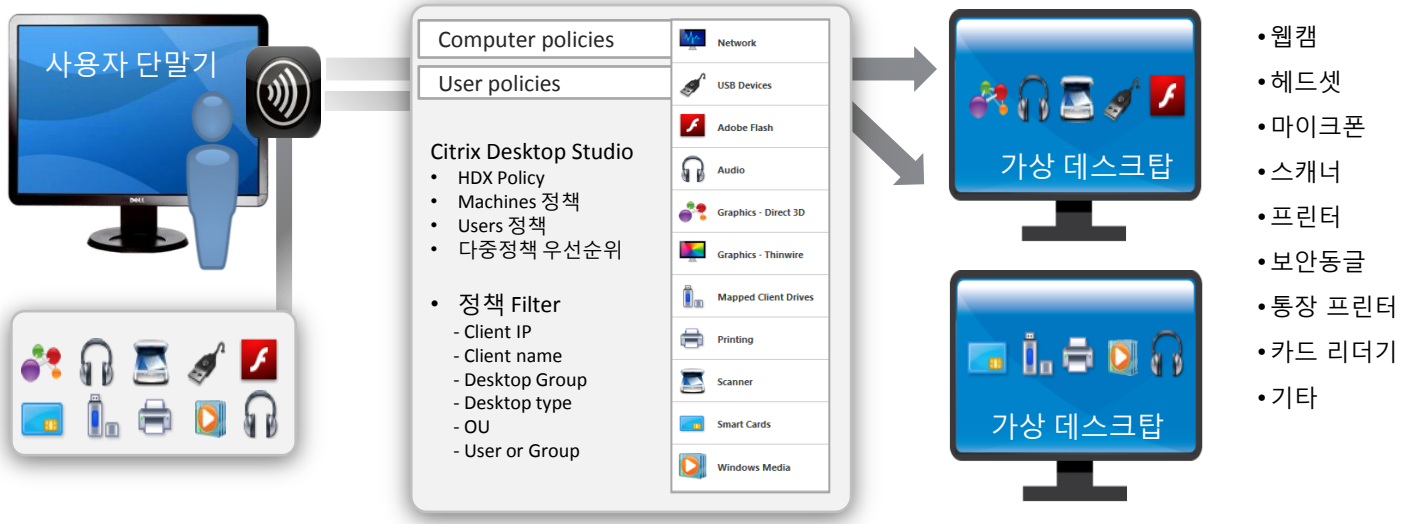
Citrix HDX for Flash 지원 요건

- ✓ 사용자 단말단에 IE에 Adobe Flash Player 10 이상 필요.
- ✓ Virtual Desktop에 IE 7 이상, Adobe Flash Player 10 이상 필요.

Citrix 선정 배경

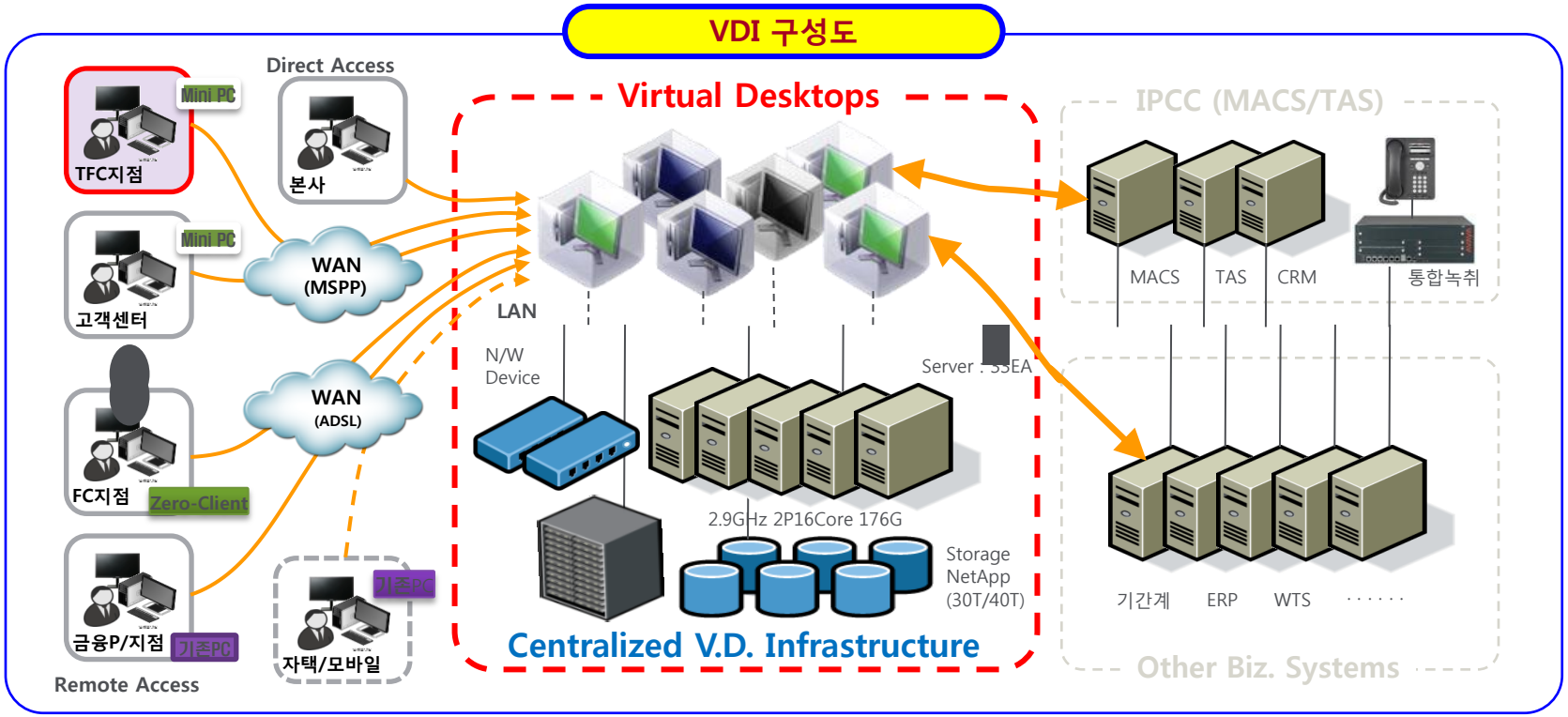
#3 다양한 업무용 주변장치 지원

- 접속PC 및 주변장치
- Citrix XenDesktop 정책 적용
- 가상데스크톱에서 주변장치 이용



- 웹캠
- 헤드셋
- 마이크폰
- 스캐너
- 프린터
- 보안동글
- 통장 프린터
- 카드 리더기
- 기타

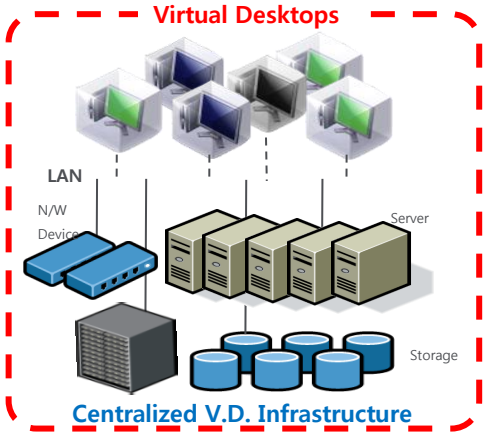
시스템 구성도


VDI 구성도
Direct Access
Mini PC
TFC지점
본사
Mini PC
고객센터
WAN
(MSPP)
WAN
(ADSL)
FC지점
Zero-Client
금융P/지점
기존PC
Remote Access
기존PC
자택/모바일
Virtual Desktops
LAN
N/W
Device
Server : 35EA
2.9GHz 2P16Core 176G
Storage
NetApp
(30T/40T)
Centralized V.D. Infrastructure
IPCC (MACS/TAS)
MACS
TAS
CRM
통합녹취
기간계
ERP
WTS
· · · · · ·
Other Biz. Systems

사용자 가상데스크탑 환경

가상데스크탑

- OS : Windows 7
- CPU : 2 vCPU
  (2P/16 Core Server)
- RAM : 3G
- HDD : OS 40G / DATA 40G



단말기(Mini-PC)

- OS : Windows 7
- CPU : Pentinum 2.5Ghz
- RAM : 2G
- HDD : SSD 16G or 64G

* Zero Client일부 사용

가상화 추진 Keyword

TCO 측면(1VM 당 가격)

- 집적도
- Dedupe / Thin Provisioning
- 한번에 많이 vs 점진적 도입
- Snap Shot
- PC유지보수 비용
- 교체 주기
- 망분리

변화관리 측면(저항)

- Smart Office
- OTP
- Windows 7
- 망분리

CITRIX®

향후 추진 계획

- *앱 가상화(Citrix XenApp) 적용 확대*
  - *영업포털을 FC 주요도구로 활용 하도록 유도*
  - *그룹웨어 등 확대 적용*

- *망분리를 위한 전사 확대 적용*
  - *가상화 관리 포털 구현 2014년 상반기*
  - *본사 2014년 / 지점 2015년 확대 추진 전사 가상화 전환 완료*

- *가상화와 IPT 인프라를 활용한 새로운 혁신 모델 개발*

가상 데스크톱 ➔ 비즈니스 혁신 도구

CITRIX®

망분리 고려사항

설계 고려사항

- 사용자 환경 분석의 객관성
- 네트워크 Bandwidth 예측
- 어플리케이션 호환성 확보

성능

- VM 리소스 설정
- 스토리지 IOPS
- 국내 포탈 환경에 맞는 네트워크
- 동영상 네트워크 부하

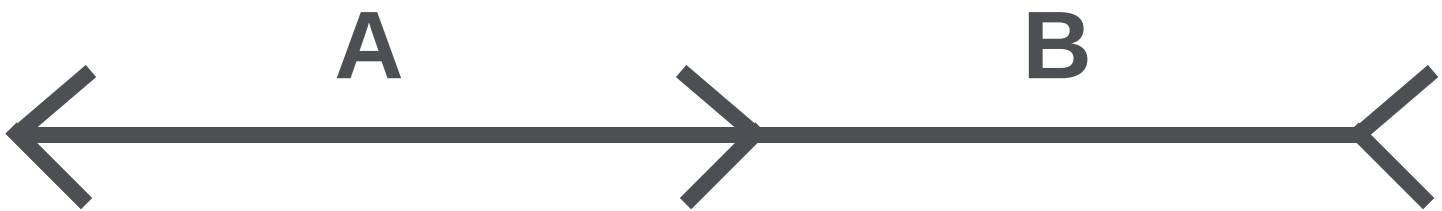
호환성 이슈

- 기존 보안 어플리케이션과의 호환성
- 인터넷뱅킹 ActiveX 호환성

사용자 편의성

- 사용자 접근 편리
- 사용자 편의 기능
- 망분리 호환 기능

CITRIX®



Work better. Live better.