14년 통합 솔루션 제안서-v2

(주)가넷정보기술

(주)가넷정보기술
Garnet Networking & Security
Total IT Solution

CONTENTS

1. 회사소개

인사말
Greeting

㈜가넷정보기술은 네트워크, 정보보안, 망분리(가상화), 시스템 유지보수를 전문으로 컨설팅, 설계, 구축, 유지보수를 ONE-STOP Service System으로 진행하는 TOTAL 정보기술 전문회사 입니다.
분야 최고의 전문가로 다양한 프로젝트 경험과 노하우를 바탕으로 귀사의 정보기술 분야 최고의 파트너가 되어 드리겠습니다.

일반현황

<table>
<tr><td>회 사 명</td><td colspan="2">㈜가넷정보기술</td><td>대 표 이 사</td><td colspan="2">임 정 헌 (林 正 憲)</td></tr>
<tr><td>대 표 번 호
팩 스 번 호</td><td colspan="2">051-925-1222(代)
051-925-1223</td><td>자 본 금</td><td colspan="2">1억5천만원</td></tr>
<tr><td>사업자번호</td><td colspan="2">617-86-14174</td><td>홈 페 이 지</td><td colspan="2">http://www.garnetit.co.kr</td></tr>
<tr><td>주 소</td><td colspan="5">부산광역시 수영구 민락본동로 15 202(민락동, 송현다미랑 B/D)</td></tr>
<tr><td>사 업 분 야</td><td colspan="5">네트워크통합(NI) / 정보보안 / 망분리(가상화) / 통합유지보수 / CCTV
/정보통신공사</td></tr>
<tr><td rowspan="2">주요협력사</td><td>시스코
(네트워크)</td><td>엑스게이트
(정보보안)</td><td>파이로링크
(웹방화벽,L4)</td><td>퓨전데이타
(망분리)</td><td>Infoblox
(DNS보안)</td></tr>
<tr><td>CISCO</td><td>AXGATE</td><td>PIOLINK</td><td>FusionData</td><td>Infoblox</td></tr>
</table>

사업분야

네트워크통합(NI)
- 유・무선 네트워크 컨설팅 및 설계
- 유・무선 네트워크 구축 및 유지보수

보안(Security)
- Firewall / IPS / VPN / UTM / 웹방화벽
- 네트워크접근제어(NAC) / L2보안스위치
- 시스템접근제어&감사 / DNS보안

망분리솔루션
- Enterprise 5.0
- CockpIT4!
- C-Cloud
- FS-PC(Mini PC-안드로이드O/S)

Garnet Networking & Security Total IT Solution

www.garnetit.co.kr

네트워크솔루션

백본스위치

CISCO

www.cisco.com

1. 제안배경

Why Cisco - 전 세계 네트워크 시장 점유율 1위 업체

i

- 네트워크 / IT분야의 선도 업체 제품

ii

- 업계 유일의 End-to-End 토탈 솔루션 제공
- 라우터/스위치 등 기존 LAN분야뿐만 아니라 무선,보안,UC, Video/Telepresence등 다양한 분야의 제품

iii

- 년간 60억불 이상의 기술 투자 및 제품 설계단계부터 친환경을 고려한 하드웨어/소프트웨어 설계 제품

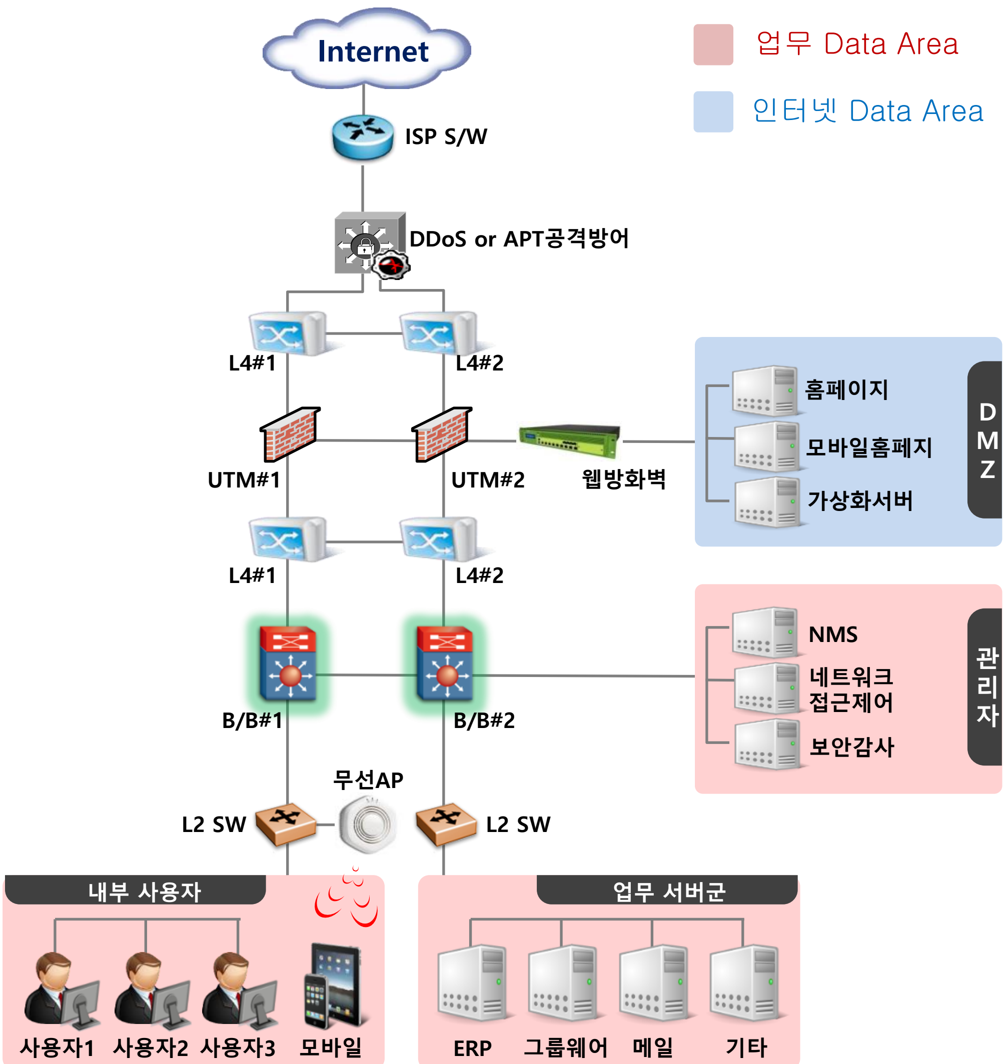
iv

- 체계적인 조직 구성 및 안정된 기술지원 제공(네트워크 밴더 중 유일하게 기술서비스 관련 인증 보유)

Key finding **"시스코 시스템즈" 는 인터넷 네트워킹 분야의 세계적인 리더**

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- 확장성이 뛰어난 시스템으로서 Borderless Networks를 기반으로 정교함
- 샷시형 장비로서 향후 업그레이드 필요 시 모듈 구입만으로 확장이 가능
- 네트워크 가동 시간 및 네트워크 복원력 극대화
- 통합된 고성능 보안 및 네트워크 관리

제품의 특장점

- 확장 가능한 인텔리전트 멀티레이어 스위칭 기능 구현
- 데이터와 음성 서비스의 통합
- 하나의 플랫폼을 와이어링 클로짓, 코어 데이터 센터 및 WAN 에지에 융통성있게 설치 할 수 있도록 슬롯 구성
- 통합 서비스 모듈, 10Mbps 및 10Gbps 이더넷의 인터페이스 옵션
- 초당 200,000 동시 연결을 지원하는 통합서버의 로드밸런싱 기능을 포함
- L4 ~ L7 컨텐츠 스위칭 기능

제품 도입 효과

- 향후 지속적인 신기술/신제품 개발 및 기술지원이 가능한 회사
- 다양한 고객 환경에서 검증된 장비의 안정성
- 장비간 호환성 제공을 통한 투자 보호
- 최소의 비용으로 24시간 기술 지원 서비스 센터를 보유한 회사

3. 제품 라인업

KEY MESSAGE **CISCO 백본스위치 제품 라인업**

구분	Nexus7010	Catalyst 6500	Catalyst 4500
이 미 지			
Switching Fabric	• 4.1Tbps	• 2Tbps	• 848Gbps
DRAM	• 4GB	• 2GB	• 2GB
Compact Flash	• 2GB	• 1GB	• 1GB
Forwarding Rate	• 720Mpps	• 720Mpps	• 250Mpps
Interface	• 10Slot 샤시 • 256개의 10G 포트 • 384개의 1G 포트 제공	• 9Slot 샤시 • 최대 10/100/1000 385 포트 장착	• 7Slot 샤시 • 최대 10/100/1000 244 포트 장착

4. 제품 비교자료

KEY MESSAGE 주요 백본스위치 비교 자료

구분	시스코(C6509)	알카텔-루슨트(OS9700E)	주니퍼(EX8208)
이 미 지			
Switching Fabric	• 2TBbps	• 1.92Tbps	• 3.1bps
DRAM	• 2GB	• 1GB	• 2GB
Compact Flash	• 1GB	• 2568MB	• 4GB
스위칭 패브릭 이중화	• YES	• YES	• YES
라우팅 처리용량	• 720Mpps	• 1428Mpps	• 960Mps
슬롯 당 대역폭	• 80Gbps	• 240Gbps	• 320Gbps
슬롯수(인터페이스모듈 + 관리용 모듈)	• 7 + 2	• 8 + 2	• 8+ 3

네트워크솔루션

워크그룹스위치

CISCO
www.cisco.com

1. 제안배경

- Why Cisco - 전 세계 네트워크 시장 점유율 1위 업체

i
- 네트워크 / IT분야의 선도 업체 제품

ii
- 업계 유일의 End-to-End 토탈 솔루션 제공
- 라우터/스위치 등 기존 LAN분야뿐만 아니라 무선,보안,UC, Video/Telepresence등 다양한 분야의 제품

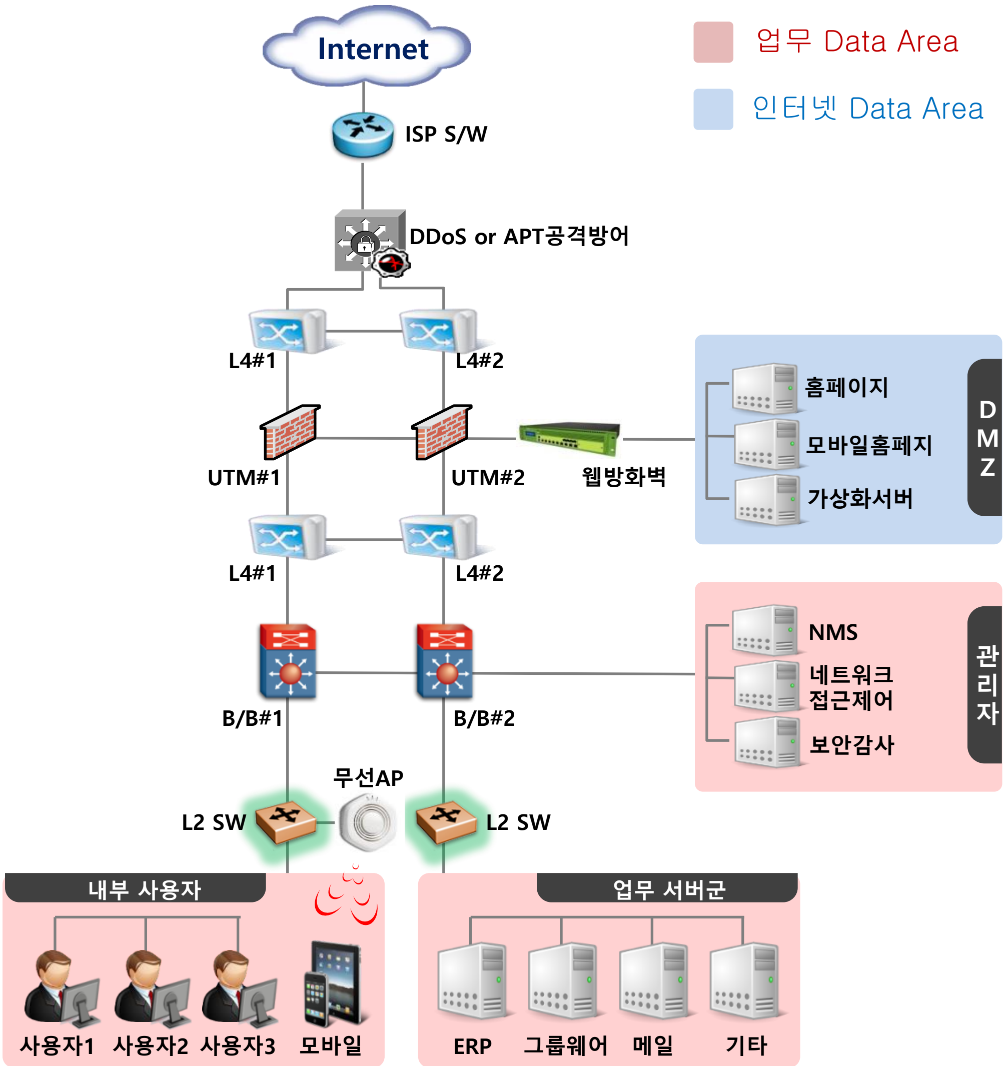
iii
- 년간 60억불 이상의 기술 투자 및 제품 설계단계부터 친환경을 고려한 하드웨어/소프트웨어 설계 제품

iv
- 체계적인 조직 구성 및 안정된 기술지원 제공(네트워크 밴더 중 유일하게 기술서비스 관련 인증 보유)

Key finding | **"시스코 시스템즈" 는 인터넷 네트워킹 분야의 세계적인 리더**

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- 차세대 24포트, 48포트 기가비트 이더넷 스위치
- 네트워크 관리 전용 포트 제공
- 저전력 아키텍처로 설계된 기가비트 스위치
- 업게 동등 수준의 이더넷 스위치 대비 약50%의 전력 소모량

제품의 특장점

- 혁신적인 스위치 기술탑재
  - StackPower(3750-X만 해당)
  - 802.3at PoE+
  - 802.1ae MACsec 암호화
  - 듀얼 리던던트 파워 서플라이(L3)
  - 필드 교체가 가능한 업링크 네트워크 모듈(L3)
- SFP+를 이용한 10G연결 지원
- 와이어 속도를 보장하는 트래픽 분류, 폴리싱 및 마킹

제품 도입 효과

- PoE+(포트당 최대 30W) 지원 및 최대 800W PoE budget 지원
- STP Advanced 기능 및 보안 기능 제공
- 엑세스 포트에 연결된 기기를 탐지하고 자동으로 구성을 적용하는 SmartPort
- Stack 미 구성 환경에서 새로운 스위칭 장비 추가시 Plug-and-Play 방식의 자동 구성

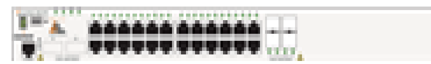
3. 제품 라인업

KEY MESSAGE **CISCO 워크그룹스위치 제품 라인업**

구분	WS-C3750X-12S-S	WS-C3560X-24P-S	WS-C2960S-24PS-L
이 미 지			
Switching Fabric	• 160Gbps	• 160Gbps	• 88Gbps
DRAM	• 512MB	• 256MB	• 128MB
Compact Flash	• 128MB	• 64MB	• 64MB
Forwarding Rate	• 35.7Mpps	• 65.5Mpps	• 41.7Mpps
Interface	• 1000BaseSX * 12포트 SFP 제공	• 10/100/1000 * 24포트 PoE 제공 • 1G SFP * 4포트 제공(옵션) • 10G SFP * 2포트 제공(옵션)	• 10/100/1000 * 24포트 PoE 제공 • 1G SFP * 4포트 제공

4. 제품 비교자료

KEY MESSAGE **워크그룹 스위치 비교 자료**

구분	시스코(WS-C3560X-24P-S)	알카텔(OmniSwitch 6850E-p24)	주니퍼(EX4200-24P)
이 미 지			
Switching Fabric	• 160Gbps	• 88Gbps	• 88Gbps
DRAM	• 256MB	• 512MB	• 1GB
Compact Flash	• 64MB	• 128MB	• 1GB
Interface	• 10/100/1000 * 24포트 PoE 제공 • 1G SFP * 4포트 제공(옵션) • 10G SFP * 2포트 제공(옵션)	• 10/100/1000 * 24포트 PoE 제공 • MiniGBIC combo * 4포트 SFP지원 • 2Port Stack 또는 10GE 업링크 지원	• 10/100/1000 * 24포트 PoE 제공 • 1G SFP * 4포트 제공(옵션) • 10G SFP * 2포트 제공(옵션)
라우팅 처리용량	• 65.5Mpps	• 65.5Mpps	• 65Mpps
라우팅 프로토콜	• RIPv1, RIPv2, EIGRP-Sub, OSPF	• RIPv1, RIPv2, OSPF	• RIPv1, RIPv2, OSPF
전원 이중화	• YES	• YES	• YES

www.garnetit.co.kr

네트워크솔루션

L4스위치

PIOLINK
www.piolink.co.kr

1. 제안배경

Why PIOLINK – ADC시장 점유율 1위 업체

i
- 파이오링크는 세계일류상품으로 선정됨
- 미국 Tolly Group 성능인증(Up to Spec)획득

ii
- 애플리케이션에 최적화 된 운영 시스템(Operating System)
- 애플리케이션을 효율적으로 전송 하기 위한 장비

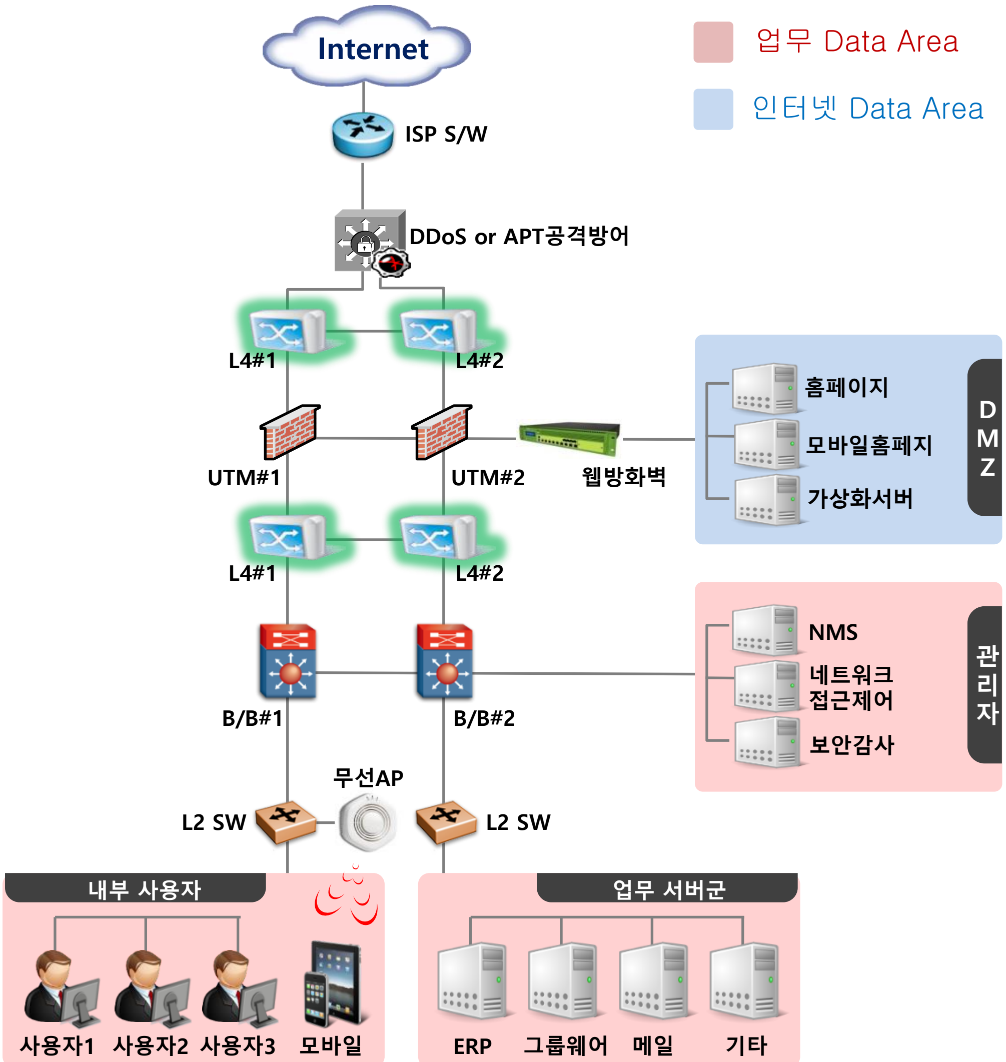
iii
- 네트워크 가용성, 보안성을 위한 애플리케이션 스위치

iv
- ADC 시장 점유율 1위 업체
- ADC 리더쉽 어워드 수상(시장점유율, 제품 기술혁신, 고객분포, 매출 성장률 등 종합평가)

Key finding “PIOLINK” 는 클라우드 데이터센터 최적화 전문기업

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- 애플리케이션을 효율적으로 전송 하기 위한 장비
  - 스마트 오피스, SNS, 교육, 엔터테이먼트 등 다양한 애플리케이션 서비스 증가
  - 네트워크 가용성과 보안, 자원 관리의 효율성과 경제성 제공
- 지능적 로드밸런싱, 부하분산 대상의 안정성/리소스 확보를 위한 기술 추가
- 서버/스토리지 등 클라우드 인프라 구축효과 극대화를 위한 핵심 제품

제품의 특장점

- 다양한 부하분산 / 트래픽 관리
- 애플리케이션 가속으로 응답속도 향상, 서비스 품질 향상, 서버 자원의 부하 감소로 자원 효율성 향상(메모리 캐싱, HTTP 압축, 커넥션 풀링, SSL 오프로딩)
- 차세대 보안
  - 시스템 보안 : 외부 공격에 대한 방어 기능으로 시스템 안정성 확보
  - 네트워크 보안 : 웹방화벽이 제공하는 다양한 필터링을 통해 데이터 안정성 보장
- 가상화
  - 자원간에 독립적인 CPU, 메모리, Throughput 기능 설정
  - 각각의 가상 인스턴스가 완벽하게 독립적으로 작동, 개별 재부팅 가능
  - 가상데이터센터의 중앙집중 관리를 위한 오케스트레이션 플러그인 제공

제품 도입 효과

- 합리적 IT자원 투자로 네트워크 가용성 확보, 비즈니스 신뢰도 증대
- 전통적인 부하분산과 더불어 전송 효율을 높이기 위한 캐싱, 압축, 가속기능 추가
- 애플리케이션 전송과정의 안전성을 보장하기 위한 각종 보안기능 추가
- 광범위한 대형 서비스, 재해복구센터(DR센터) 및 클라우드 데이터센터 구축 필수

3. 제품 라인업

KEY MESSAGE **PAS-K 제품 라인업**

구분	PAS-K1516	PAS-K2424	PAS-K4224
이 미 지			
Backplane	• 56Gbps	• 88Gbps	• 640Gbps
R A M	• 4GB	• 16GB	• 12GB
Compact Flash	• 64MB	• 64MB	• 64MB
SSD	• 40GB	• 40GB	• 40GB
Interface(10G)	• -	• -	• 16 * 10G port(1G/10G 자동인식)
Interface(1G)	• 8 * 1G SFP • 8 * 10/100/1000BASE-TX(총 16포트)	• 16 * 1G SFP • 8 * 10/100/1000BASE-TX(총24포트)	• 8 * 1G SFP(옵션)또는 • 8 * 10/100/1000BASE-TX(옵션)
Throughput	• 1.5Gbps	• 4Gbps	• 12Gbps
동시세션	• 3,600,000	• 16,000,000	• 18,000,000
L4 CPS(MAX.)	• 70,000	• 200,000	• 340,000
가상 ADC	• -	• 12 * Virtual Instance	• 20 * Virtual Instance
전원 이중화	• 500W Redundant	• 300W Redundant	• 250W Single

4. 제품 비교자료

KEY MESSAGE **L4스위치 제품 비교자료**

구분	파이오링크(PAS-K2424)	펌킨(LX4020)	알테온(4408)
이 미 지			
Interface	• 1G SFP * 16Port • 10/100/1000BASE-TX * 8Port	• 1G SFP * 8Port(Combo) • 10/100/1000BASE-TX * 12Port	• 10/100/1000BASE-T * 6Port • 1G SFP * 2Port
BackPlane	• 88Gbps	• 48Gbps	• 48Gbps
R A M	• 16.5GB	• 4GB	• 8GB
Compact Flash	• 64MB	• -	• -
SSD	• 40GB	• -	• -
Throughput	• 4Gbps	• 3.6Gbps	• 4Gbps
L4 CPS(MAX)	• 200,000	• 200,000	• 215,000
동 시 세 션	• 16,000,000	• 10,000,000	• 12,000,000

네트워크솔루션

L2보안스위치

www.garnetit.co.kr

www.handream.net

1. 제안배경

Why 한드림넷 – 국내 보안스위치 시장 점유율 No.1

i

- 날로 증가하는 유해트리픽을 실시간 탐지/차단하여 중단 없는 비즈니스를 실현
- ARP프로토콜의 취약점 ARP Spoofing을 실시간 탐지/차단하여 각 기관들의 기밀정보를 보호

ii

- 한드림넷의 핵심 기술인 MDS(Multi Dimension Security)엔진은 별도의 ASIC 기반이므로 전송 전송되는 트래픽에 대해 네트워크 성능 저하 없이 강력한 보안기능 수행

iii

- 한 화면에서 네트워크 현황을 볼 수 있는 "통합 네트워크 관리(VNM)" 제공

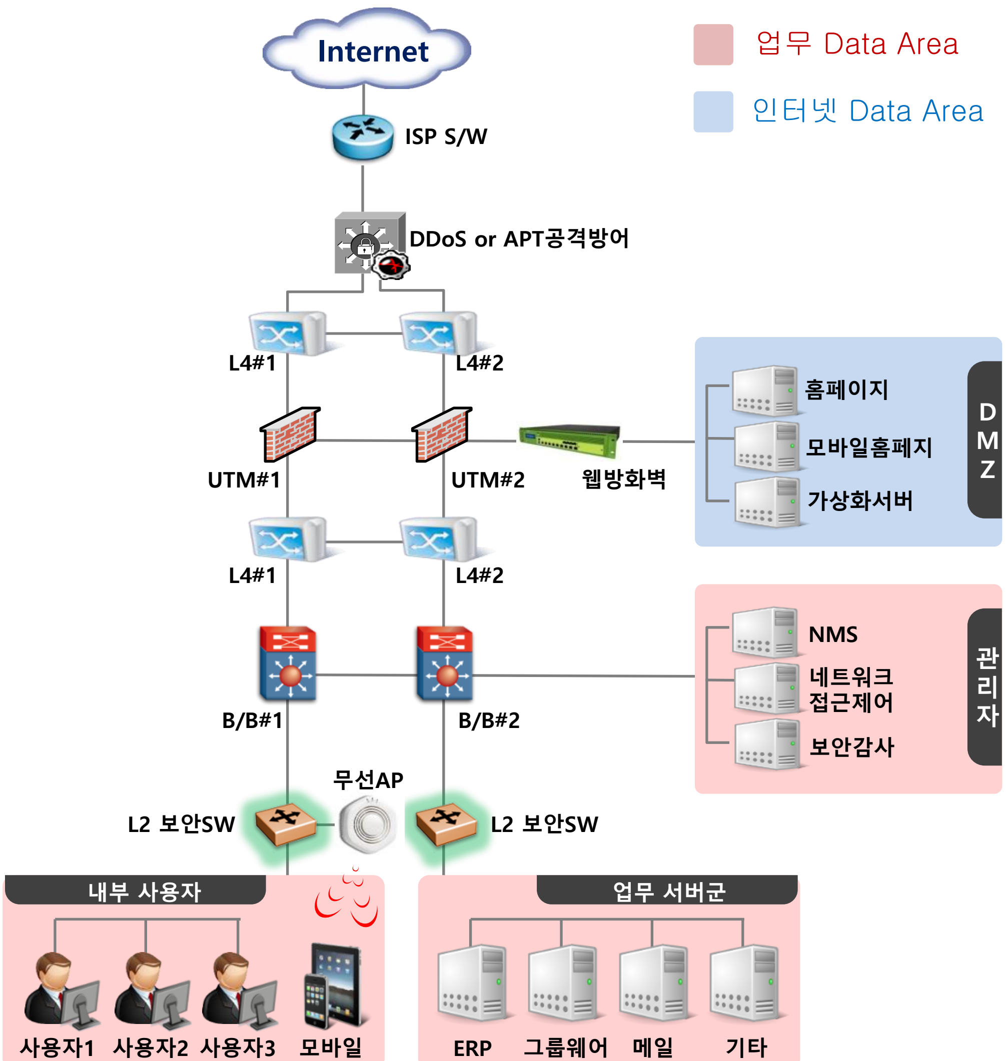
iv

- 국내 최대 래퍼런스와 공인기관을 통한 검증된 보안(CC인증, 보안적합성 검증 필)
- IPv6 대하여 CC인증을 받은 유일한 보안스위치

Key finding | **"한드림넷" 는 보안스위치 1등 브랜드**

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- L2 보안스위치 란 네트워크와 보안이 통합된 엑세스레벨의 보안 스위치
- 전체 보안침해 사고 중 내부에서 발생하는 것이 80% 차지
- 허가 받지 않은 사용자의 내부 네트워크 접근 경로의 다양화
- 악의적 내부 네트워크 사용자에 의한 해킹 및 바이러스의 손쉬운 배포
- 허가 받지 않은 내부 네트워크 사용자에 대한 감시/제어기능 미비

제품의 특장점

- H/W기반의 유해트래픽 차단 전용 보안 엔진
  - 선별적 유해트래픽 차단
  - 유해트래픽 차단시에도 Full Wire Speed 제공
- ARP Spoofing 차단
  - 중요 데이터/기밀 유출 방지
  - ID/PW등 개인 정보 유출 방지
  - IP 전화 도,감청 방지
  - 네트워크 품질 저하 방지
- 유해트래픽 차단 모니터링(VNM(Visual Node Manager)
  - 실시간 유해트래픽 차단 현황, 포트별 트래픽 현황
  - 실시간 IP 사용 현황,

제품 도입 효과

- Access 레벨에서 웜/바이러스에 의한 유해트래픽을 실시간 탐지/차단하여 장애예방
- ARP Spoofing 공격으로부터 개인/기업/공공기관의 도처 방지 및 금융정보와 기밀정보를 보호
- 유해트래픽만 선별적으로 차단하는 Smart Protection
- 국내 최대 레퍼런스와 공인기관을 통한 검증된 보안(CC인증, 보안적합성 검증 필)

3. 제품 라인업

KEY MESSAGE **L2보안스위치 제품 라인업**

구분	GS2024GPoE	SG2124GXPoE	GS2124GXF
이 미 지			
Backplane	• 48Gbps	• 144Gbps	• 144Gbps
R A M	• 256MB	• 512MB	• 512MB
Compact Flash	• 256MB	• 256MB	• 256MB
라우팅 처리용량	• 71.4Mpps	• 131Mpps	• 131Mpps
Interface	• 10/100/1000 * 24Port PoE • 1000BASE-X * 4Port(Combo)	• 10/100/1000 * 24Port PoE • 1000BASE-X * 4Port(Combo) • 10G * Port	• 10/100/1000 * 12Port • 1000BASE-X * 24Port • 10G * Port
PoE 총 파 워	• 740W	• 740W	• -
전원 이중화	• 이중화 가능	• 이중화 가능	• 이중화 가능

4. 제품 비교자료

KEY MESSAGE L2보안스위치 제품 비교자료

구분	한드림넷(SG2024GPoE)	파이오링크(TiFRONT-G24P)
제 품 명		
Backplane	• 48Gbps	• 72Gbps
R A M	• 256MB	• 512MB
Compact Flash	• 256MB	• 160MB
라우팅 처리용량	• 71.4Mpps	• 71.4Mpps
Interface	• 10/100/1000 * 24Port PoE • 1000BASE-X * 4Port(Combo)	• 10/100/1000 * 24Port PoE • 1000BASE-X * 4Port(Combo)
PoE 총 파 워	• 370W	• -
전원 이중화	• 이중화 가능	• 이중화 가능
802.1x 인증	• 지원 가능	• 지원 가능
ID/PW를 통한 Web 인증	• 지원 가능	• 지원 불가
스위치 관리 기능	• 지원 가능	• 지원 가능
스위치에 Radius 서버 인증	• 지원 가능	• 지원 불가

www.garnetit.co.kr

네트워크솔루션

EMS, NMS, SMS

HAMON SOFT
주식회사하몬소프트
www.hamonsoft.co.kr

1. 제안배경

■ **Why 하몬소프트 – IT 유/무선 인프라 통합관리솔루션 전문 업체**

i
- 현재 구축되어 있는 관리 인프라의 전체적인 시각화 인지 필요

ii
- 모든 관리 솔루션에 대한 주요 이벤트 통합 필요

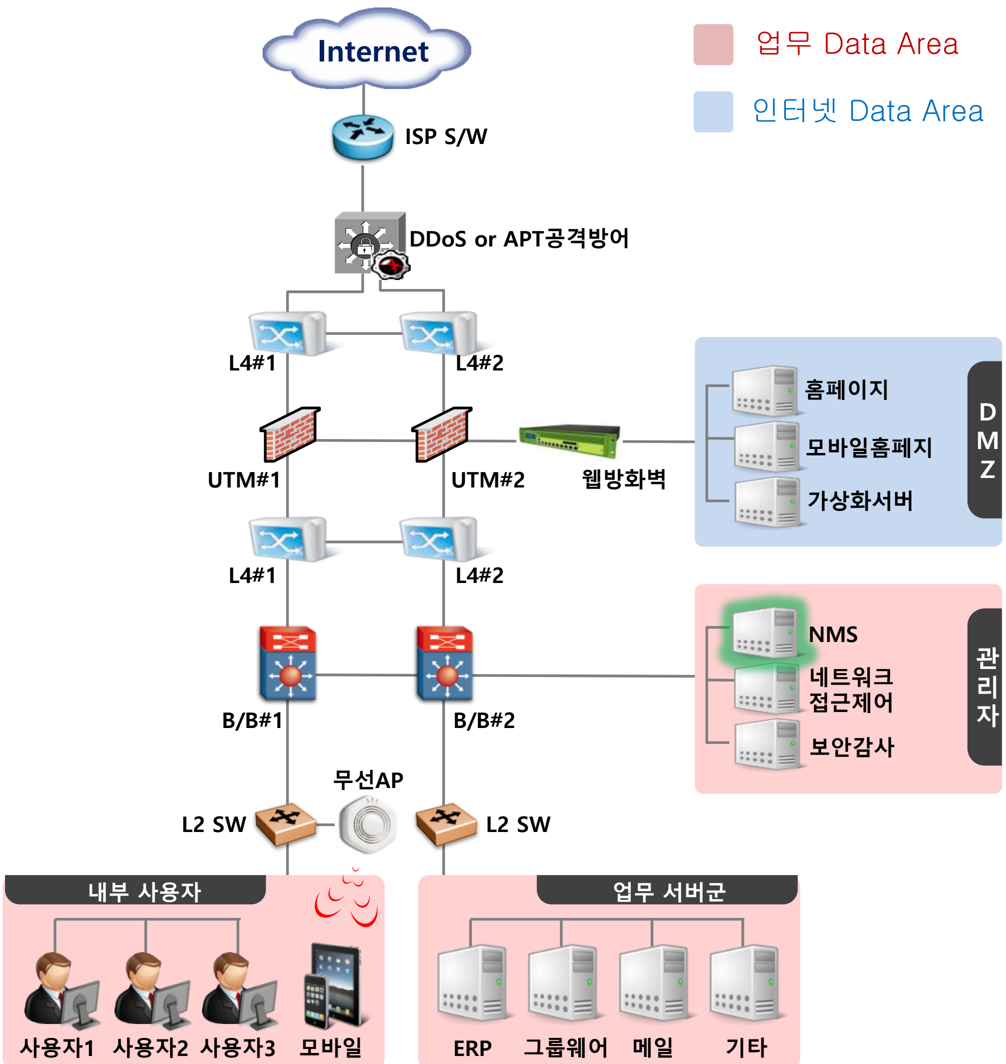
iii
- 주요 이벤트 발생에 대한 즉각적인 대응 방안 구축 필요

iv
- 다양한 관리 시스템을 통한 이벤트 및 정보수집이 필요

Key finding | **"하몬소프트" 는 IT 인프라 통합관리 전문회사**

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- 네트워크, 트래픽, 서버 및 센서의 현황을 시각적으로 모니터링 기능을 제공
- 기 구축 관리 솔루션과 연동 기능을 제공
- 이벤트 발생시 다양한 형태의 위협 요소에 대한 제어 기능을 제공

제품의 특장점

- 수집 성능 고도화에 의한 안정적인 시스템 운영
- Flow를 활용한 트래픽 상세 분석 시스템 제공
- 편리한 필터링 시스템
  - 그룹 필터 기능, 문자 필터 기능, 정렬기능, 값에 대한 크기 비교 필터 기능 등 다양한 조건으로 검색 가능
- 향후 확장성에 유리
  - 다양한 솔루션 보유(NMS, TMS, SMS, UPS, NAS, VoIP, ddOs, CCTV, BIS등)
  - 추가 시스템 도입 및 향후 시스템 확장성에 유리함
- 고객 맞춤형 대시보드 제공

제품 도입 효과

- 장애 자동 감지 시스템 구축을 통한 신속한 장애 처리 지원
- 서비스 관점의 시스템 상황판 구축을 통한 운영 현황 요약정보 제공
- 성능 추이 분석용 데이터 베이스 구축을 통한 장애 예방 조치 지원
- 자동화된 운영 보고서 출력 시스템 구축을 통한 운영 효율성 제공

3. 제품 라인업

KEY MESSAGE **Netis 제품 라인업**

통합관제시스템

Netis-EMS

- +NMS 네트워크관리시스템
- +Flow 네트워크관리시스템
- +SMS 네트워크관리시스템
- +FMS 네트워크관리시스템
- +UPS 네트워크관리시스템
- +NAS 네트워크관리시스템
- +UMS 네트워크관리시스템
- +FNMS 네트워크관리시스템
- +VoIP 네트워크관리시스템
- +CCTV 네트워크관리시스템
- +LOG 네트워크관리시스템
- +TAC 네트워크관리시스템
- +BIS 네트워크관리시스템
- +U-City 네트워크관리시스템
- +GIS 네트워크관리시스템

통합관제시스템

IP관리 | Config 관리 | 토폴로지 | 작업관리 | Syslog Trap | 폴링엔진 | 알람

\+

- \+ 이벤트 통합연동
- \+ 기 구축 시스템 연동
- \+ 통합관제 상황판

4. 제품 비교자료

KEY MESSAGE NMS 제품 비교자료

구분	하몬소프트(NETIS)	넷크루즈(NetPManager)	네비스탁(IseeNet)
회사 규모 (연구소 인력)	• 40명 (연구소 24명)	• 50명 (연구소 32명)	• 30명 (연구소 16명)
회사 연혁	• 6년	• 11년	• 14년
고객사수 (전체 솔루션)	• 180~200 고객사	• 230~250 고객사	• 150~180 고객사
자체 개발 능력 보유	• 100% 자체 개발	• 60% 자체 개발	• 70% 자체 개발
자체 디자인 능력 보유	• 자체 디자이너 보유	• 자체 혹은 외주 개발	• 자체 혹은 외주 개발
고객사수 (대시보드 구축)	• 100~120 고객사	• 50~70 고객사	• 50~70 고객사
대시보드 구현 기술	• 실버라이트, 플랙스, HYML5 등	• 플랙스 등	• 플랙스 등
연동기술	• 1) CSV 파일 연동 • 2) TCP/IP 소켓통신 • 3) XML 연동 • 4) SNMP TRAP 연동 • 5) SYSLOG 연동 • 6) SOAP Protocol 연동 • 7) DB to DB 연동	• 1) CSV 파일 연동 • 2) TCP/IP 소켓통신 • 3) XML 연동 • 4) SOAP Protocol 연동 • 5) DB to DB 연동	• 1) CSV 파일 연동 • 2) TCP/IP 소켓통신 • 3) XML 연동 • 4) SOAP Protocol 연동 • 5) DB to DB 연동
동일 제품군 여부	• 모든 제품이 동일 DB 사용	• 제품마다 DB가 모두 다름 • (이유: 여러 회사 제품 인수 해서 개발)	• 모든 제품이 동일 DB 사용
보안 알고리즘 적용 여부	• 국정원 인증 아리아 알고리즘 사용	• 보안 알고리즘 사용 안함	• 자체 보안 알고리즘 사용
장애 발생 시 음성 지원	• 지원	• 미지원	• 미지원

무선솔루션

Controller, AP

www.garnetit.co.kr

www.arubanetworks.co.kr

1. 제안배경

Why Aruba – 무선랜 전문업체의 전문성과 높은 시장 점유율, 우수한 장비성능을 보유한 글로벌 회사

i
- ICSA Labs Firewall 유일한 무선랜 인증
- ICSA Labs WLAN 업계 최초 WPA, WPA2 인증

ii
- 보안과 성능을 중시하는 기업 무선랜
- 다양한 기능(WLAN Controller, WLAN Management, Location Appliance, NAC Appliance 등)의 통합

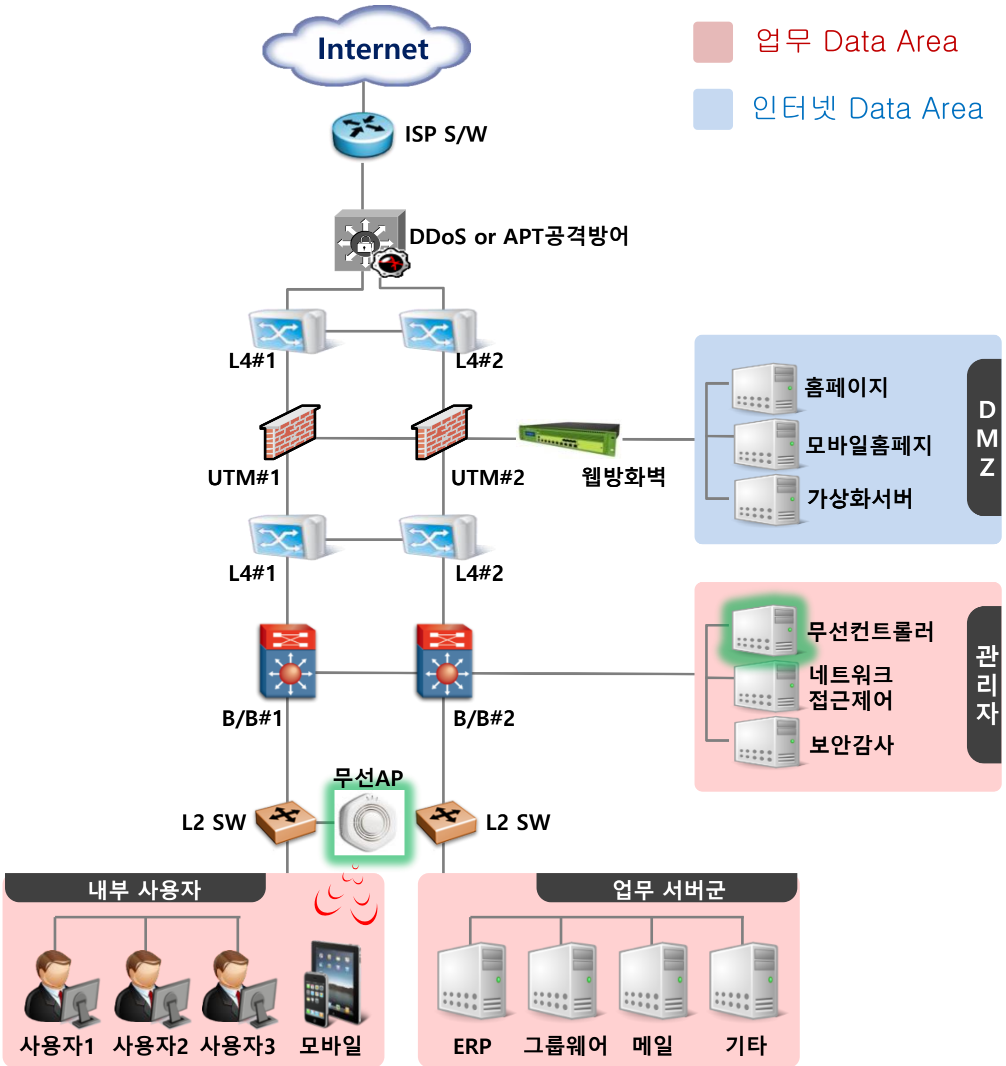
iii
- 무선랜 전담 엔지니어 외에도 본사 소속의 한국 전담 TAC 엔지니어를 한국 지사내 보유하고 있는 Aruba의 지원 전문성

iv
- 업계 최고의 단말수용 능력 및 독보적 RF 성능

Key finding “아루바 네트웍스” 는 무선랜 분야의 세계적인 리더

2. 네트워크 구성도

KEY MESSAGE 네트워크 구성 특장점



제품의 개요

- 802.11표준 자체가 보안을 위한것이 아니고 접속을 위한 표준으로 감청의 위협, 무선의 위협으로 나타나고 있다
- AP에서의 작업 불필요, 실시간 무선환경 화면 제공으로 구축의 용이성
- 상태감지 방화벽 내장, 권한별 접근제어, L1 ~ L7 무선침입보호의 보안성
- 유선 및 무선구간에서의 양방향 품질보상 능력, 멀티미디어 환경에서 VoIP정보 자동 감지

제품의 특장점

- 관리성, 보안성 및 확장성이 뛰어난 중앙집중형 구조의 무선 네트워크 시스템을 통해 손쉬운 네트워크 관리 및 보안을 유지
- 클라우드 기반 자동설정 지원
- 설정, 관리, Help 등 모든 메뉴 100%한글화 지원
- 강력한 WLAN 보안
  - Stateful Firewall, NAC, Centralized Encryption
  - Hardware-based AAA
  - L1 ~ L7 Wireless IPS/Rogue AP Prevention
- 손쉬운 확장성 및 에너지 효율성

제품 도입 효과

- 가격대비 최고의 성능 및 기능
- 고속단말 가속기능, APP별 최대 11배 다운로드 성능 제공
- 손쉬운 설정, 유지보수 가능, 운영비용 절감
- 간편한 컨트롤러 연동방식 지원, 투자비용 보호

3. 제품 라인업(ControlI)

KEY MESSAGE **Aruba 제품 라인업(무선컨트롤러)**

구분	Aruba 6000	Aruba 3200/3400/3600	Aruba A200
이 미 지			
규 격	• IEEE 802.1x, 802.2 10-BASE-T • 1G SFP 포트 10EA 제공, 10G 2EA 제공 • 모듈 당 10/100Mbps Mag 포트 1EA	• 10/100/1000BASE-T 또는 1000BASE-X 4EA 지원 가능	• 1 * Fast Ethernet, 2 * Gigabit Ethernet
성 능	• 모듈 형식의 확장 • 최대 수용 AP수 512개(모듈 당) • 최대 수용 사용자수 8,192명(모듈 당) • 콘트롤러 속도 20Gbps(모듈 당)	• 최대 수용 AP수 128개 (Aruba 3600) • 최대 수용 AP수 64개 (Aruba 3400) • 최대 수용 AP수 32개 (Aruba 3200) • 콘트롤러 속도4G/4G/3G(3600/3400/3200)	• 최대 수용 AP수 6개 • 최대 수용 사용자 수 100명 • 콘트롤러 속도 1Gbps
표준규격 및 호환성	• 무선 표준 규격 802.11a/b/g/n 및 802.11h, 802.11d, 802.11f, 802.11i 지원 • Web 인증 지원, Wi-Fi 인증	• 무선 표준 규격 802.11a/b/g/n 및 802.11h, 802.11d, 802.11f, 802.11i 지원 • Web 인증 지원, Wi-Fi 인증	• 40GB
AP 관련 기능	• SSID별 Bandwidth 제어 기능 지원 • Multi SSID 지원을 통하여 AP당 16개 이상의 SSID지원 • AP의 Mesh/브릿지 기능 지원 • WiFi Hotspot 기능 • 유선사용자 수용	• SSID별 Bandwidth 제어 기능 지원 • Multi SSID 지원을 통하여 AP당 16개 이상의 SSID지원 • AP의 Mesh/브릿지 기능 지원 • WiFi Hotspot 기능 • 유선사용자 수용	• SSID별 Bandwidth 제어 기능 지원 • Multi SSID 지원을 통하여 AP당 16개 이상의 SSID지원 • AP의 Mesh/브릿지 기능 지원 • WiFi Hotspot 기능 • 유선사용자 수용
IDS/IPS 관련 기능	• 네트워크에 연결된 불법 AP 자동 탐지 및 차단 • 네트워크에 연결된 불법 AP 중 WEP 또는 WPA 지원하는 AP 자동 탐지 및 자동 차단 • 단말 및 AP 위치 추적 가능	• 네트워크에 연결된 불법 AP 자동 탐지 및 차단 • 네트워크에 연결된 불법 AP 중 WEP 또는 WPA 지원하는 AP 자동 탐지 및 자동 차단 • 단말 및 AP 위치 추적 가능	• 네트워크에 연결된 불법 AP 자동 탐지 및 차단 • 네트워크에 연결된 불법 AP 중 WEP 또는 WPA 지원하는 AP 자동 탐지 및 자동 차단 • 단말 및 AP 위치 추적 가능

4. 제품 라인업(무선AP)

KEY MESSAGE **Aruba 제품 라인업(무선AP)**

구분	AP-125	AP-124	AP-105
이 미 지			
규 격	• Wi-Fi Certified 802.11a/b/g/n	• 1Wi-Fi Certified 802.11a/b/g/n	• Wi-Fi Certified 802.11a/b/g/n
안 테 나	• 내장 안테나 - 2.4 ~ 2.5 GHz - 5.150 ~ 5.950 GHz	• 안테나: 외장형 안테나를 부착할 수 있는 RP-SMA Type 인터페이스 3개 제공	• 내장 안테나 : 2.4 – 2.5 GHz 5.150 – 5.950 GHz
성능 및 보안	• 유선 Interface : 10/100/1000 Base T(RJ-45) 2개 이상 • Console Port 1개 제공 • SNMP 제공 • 2 x Gigabit Ethernet • 이중화 혹은 Wired AP 기능 제공 • 보안: WPA2 인증 제품	• 유선 Interface : 10/100/1000 Base T(RJ-45) 2개 이상 • Console Port 1개 제공 • SNMP 제공 • 2 x Gigabit Ethernet • 이중화 혹은 Wired AP 기능 제공 • 보안: WPA2 인증 제품	• 유선 Interface : 100/1000 Base T(RJ-45) 1개 • Console Port 1개 제공 • SNMP 제공 • 보안: WPA2 인증 제품
호 환 성	• 무선 기기간의 상호 연동성을 보장하는 Wi-Fi 인증 • 다양한 무선 LAN 카드와 테스트를 진행하여 호환성을 보장	• 무선 기기간의 상호 연동성을 보장하는 Wi-Fi 인증 • 다양한 무선 LAN 카드와 테스트를 진행하여 호환성을 보장	• 무선 기기간의 상호 연동성을 보장하는 Wi-Fi 인증 • 다양한 무선 LAN 카드와 테스트를 진행하여 호환성을 보장
안 정 성	• 802.3af 규격(POE)을 준수하는 Access Point 제공으로 전원 안정성 제공	• 802.3af 규격(POE)을 준수하는 Access Point 제공으로 전원 안정성 제공	• 802.3af 규격(POE)을 준수하는 Access Point 제공으로 전원 안정성 제공

5. 제품 비교자료

KEY MESSAGE **무선 제품 비교자료**

관리 요구 사항	아 루 바	시 스 코
• 손쉬운 설치와 운영 및 자동 채널 및 파워 조절	YES	YES
• 노이즈와 주변 간섭으로 에 대한 동적 RF 관리를 통한 성능 향상	YES	YES
• 14개의 추가 5GHz 채널 (DFS 승인) 에의한 무선랜 용량 증가	YES	YES
• 서로다른 서브넷간, 컨트롤러간 고속로밍 지원	YES	YES
• 유/무선, AP <-> 컨트롤러간 QoS tags 실현	YES	YES
• 멀티캐스트 최적화 및 multi-channel 사용 및 IGMP snooping	YES	NO
• 애플리케이션 특성 및 트래픽 로드에 따라 RF 스캔 간격을 자동적으로 조절 함으로써 데이터 유실 방지	YES	NO
• 실시간 RF Heat-map을 통한 실시간 RF 방사를 통해 설치후 RF 재 설정 및 측정업무 방지	YES	NO
• 채널 로드발란싱을 통한 client 성능 향상	YES	NO
• 사용자 접속 타입에 따른 "평등한" RF 접속 권한 분배 (예. 고속 11g 대비 저속 11b)	YES	NO
• 트래픽 shapping을 통한 과밀도 사용자 환경 트래픽 분산	YES	NO
• 업/다운 "Airtime" 분배	YES	NO
• 802.11 채널 재 사용을 통한 전반적인 무선랜 속도향상	YES	NO
• 같은 채널 간섭 완화 방책	YES	NO
• 주변 채널 간섭 완화 방책	YES	NO
• 5GHz가 가능한 사용자에 대한 5GHz 자동 로드발란싱으로 인한 전반적인 무선랜 성능 향상	YES	NO

www.garnetit.co.kr

보안솔루션

통합보안시스템 (UTM)

AXGATE

www.axgate.com

1. 제안배경

■ **Why AXGATE – 고성능 차세대 방화벽**

i

- 스마트폰 등 IP기반 단말기의 증가에 따른 안정적인 처리를 보장하는 고성능 차세대 방화벽
- 국내 최초 120Gbps 방화벽을 출시한 국내 최고 성능의 제품

ii

- 고성능 방화벽, VPN Security 기술과 고품질 Integrated Security 기술의 강력한 결합
- 검증된 기술력을 가진 제품이 안정성, 신속성, 미래지향적인 보안시스템의 기본

iii

- 통합 보안으로 관리 효율성 증대
- 단순 PORT나 IP 가 아닌 Application과 사용자를 구분하고 제어할 수 있는 새로운 통합 보안 솔루션

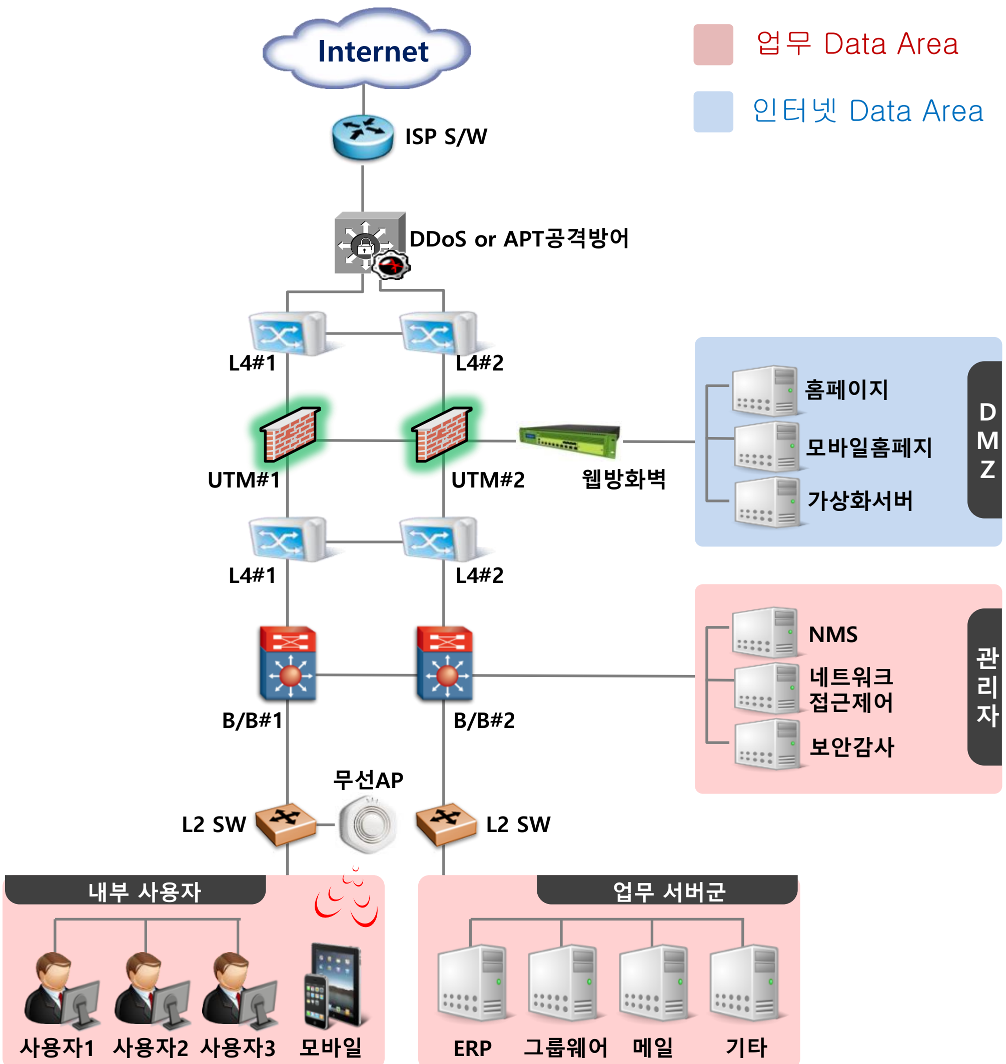
iv

- 최근 보안 위협의 키워드는 "다변화, Zero-day, 고도화된 악성코드이다

Key finding | **"AXGATE" 는 변화하는 보안 환경의 차세대 리더**

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- 철저한 시장 검증을 통해 기술력과 성능, 안정성을 인정받은 AXGATE는 차세대 네트워크 통합 보안 솔루션으로 F/W, IPS, VPN, Anti-DDOS, Anti-Spam 등 다양한 통합 보안 기능을 제공
- 자체 개발 OS 사용으로 개별 모듈의 병렬처리 - 여러 기능 구동 시 성능저하 최소화
- 자체 개발 Fast path를 통한 패킷 포워딩
- Multi-Core System에 최적화된 설계 - cash miss를 최소화하여 성능 향상

제품의 특장점

- 안정적인 고성능 구현 - 국내 최고 120Gbps F/W 성능 발휘 (AXGATE20000)
- VPN
  - D-Cube 기술을 IPSec과 연동하여 안정성 높은 고대역폭의 암호화된 Tunnel 제공
- 어플리케이션 제어
  - 업무에 불필요하거나 내부 정보 유출의 위험이 있는 어플리케이션 식별/제어
- Zone기반 보안정책
  - Security Zone 별 개별 정책 수립으로 불필요한 보안모듈 적용으로 성능저하 방지
- 사용자제어 방화벽
  - 사용자 계정을 이용한 접근제어 가능 (그룹별, 개인별 보안 정책 차등 적용 가능)

제품 도입 효과

- AXGATE는 고성능, 고품질의 네트워크 보안기술과 능동적, 종합적인 통합보안기술의 유기적 결합을 통한 시너지 효과를 제공
- 안정적인 고성능 Firewall 구축이 가능하고 보안성이 확장된 유연한 VPN구축
- 외부의 보안위협으로부터 자유로운 Network 환경 구현이 가능
- 모듈별 TOP-N 정보 및 실시간 트래픽 / 로그 등의 직관적 대쉬보드를 통한 모니터링 환경 제공

3. 제품 라인업 (1)

KEY MESSAGE **AXGATE 제품 라인업 – Low End devices**

구분	AXGATE 50	AXGATE 80	AXGATE 100
이 미 지			
C P U	• MIPS 500MHz(Single Core)	• MIPS 700MHz(Dual Core)	• Intel ATOM 1.8GHz(Dual Core)
R A M	• DDR2 1GB	• DDR2 1GB	• DDR3 1GB
Flash Memory	• 4GB	• 4GB	• 2GB
HDD	• N/A	• N/A	• 500MB (Optional)
Interface	• 10/100/1000Base-T x 6	• 10/100/1000Base-T x 6	• 10/100/1000Base-T x 6
Firewall Throughput	• 1.5 Gbps	• 2 Gbps	• 2 Gbps
IPS Throughput	• -	• 480 Mbps	• 720 Mbps
VPN Throughput	• 400 Mbps	• 1 Gbps	• 300 Mbps
VPN Tunnel	• 1,000	• 1,000	• 2,000
동시세션	• 200,000	• 200,000	• 200,000
Power	• 43W Single	• 40W Single	• 150W Single

3. 제품 라인업 (2)

KEY MESSAGE **AXGATE 제품 라인업 – Middle End devices**

구분	AXGATE 1000	AXGATE 2000	AXGATE 5000
이 미 지			
C P U	• MIPS 1GHz(Quad Core)	• Intel Xeon 3.0GHz(Dual Core)	• Intel Xeon 3.4GHz(Quad Core)
R A M	• DDR3 4GB	• DDR3 4GB	• DDR3 8GB
Flash Memory	• 4GB	• 4GB	• 4GB
HDD	• 1TB	• 500GB	• 1TB
Interface	• 10/100/1000Base-T x 4 • 1000 Base-X x 4 (Combo)	• 10/100/1000Base-T x 4 • 1000 Base-X x 4	• 10/100/1000Base-T x 4 • 1000 Base-X x 4 • 10G Base-R (OPTION)
Firewall Throughput	• 4 Gbps	• 8 Gbps	• 20 Gbps
IPS Throughput	• 1.4 Gbps	• 2.6 Gbps	• 7 Gbps
VPN Throughput	• 2.8 Gbps	• 1.5 Gbps	• 4 Gbps
VPN Tunnel	• 10,000	• 10,000	• 20,000
동시세션	• 2,000,000	• 2,000,000	• 4,000,000
Power	• 150W Single	• Dual Redundant	• 300W Dual Redundant

3. 제품 라인업 (3)

KEY MESSAGE **AXGATE 제품 라인업 – High End devices**

구분	AXGATE 10000	AXGATE 10000S	AXGATE 20000
이 미 지			
C P U	• Intel Xeon 2.53GHz (Quad Core x 2)	• Intel Xeon 3.06GHz (Hexa Core x 2)	• Intel Xeon 2.9GHz (Octa Core x 2)
R A M	• DDR3 24GB	• DDR3 24GB	• DDR3 64GB
Flash Memory	• 4GB	• 4GB	• 4GB
HDD	• 2TB	• 2TB	• 4TB
Interface	• 10/100/1000Base-T (Option) • 1000 Base-X x 8 • 10G Base-R x 4	• 10/100/1000Base-T (Option) • 1000 Base-X x 8 • 10G Base-R x 4	• 10/100/1000Base-T (Option) • 1000 Base-X x 8 • 10G Base-R x 4
Firewall Throughput	• 40 Gbps	• 58 Gbps	• 120 Gbps
IPS Throughput	• 10 Gbps	• 17 Gbps	• 20 Gbps
VPN Throughput	• 5.6 Gbps	• 7 Gbps	• 10 Gbps
VPN Tunnel	• 40,000	• 40,000	• 80,000
동시세션	• 14,000,000	• 14,000,000	• 30,000,000
Power	• 600W Dual Redundant	• 460W Dual Redundant	• 600W Dual Redundant

4. 제품 비교자료 (1)

KEY MESSAGE **UTM 제품 비교자료**

구분		AXGATE	시큐아이(NXG)	퓨쳐시스템
제 품 명				
네트워크	NAT	• Static NAT, Dynamic NAT, Exclude NAT	• Static NAT, Dynamic NAT, PAT, LSNAT	• Static NAT, Dynamic NAT, PAT, LSNAT
	Routing	• Static / Dynamic	• Static / Dynamic	• Static / Dynamic
	Multicasting	• PIM-SM, PIM-DM, IGMP	• PIM-SM	• N/A
	다중 회선 LB	○	○	○
	다중 회선 Bonding	○	X	○
	QoS	○	○	○
	VRRP	○	○	○
	L2 Bridge	○	○	○
	VLAN	○	○	○
	회선 Load Balancing	○	○	○

4. 제품 비교자료 (2)

KEY MESSAGE **UTM 제품 비교자료**

구분		AXGATE	시큐아이(NXG)	퓨쳐시스템
방화벽	Inspection	• Stateful Inspection • Deep packet Inspetion	• Stateful Inspection • Deep packet Inspetion	• Stateful Inspection • Deep packet Inspetion
	키워드 필터링	○	○	○
	사용자기반 방화벽	○	○	○
	Zone기반 보안정책 설정	○	○	• N/A
	외부인증서버 연동	○	○	○
	보안 정책 시간 스케줄링	○	○	○
VPN	암호화 알고리즘	• 3DES, AES, SEED, ARIA & SHA1, SHA256, SHA512(with CMVP)	• 3DES, AES, SEED, DES, CAST, BLOWFISH	• 3DES, AES, SEED, ARIA, PRIDE, NES, FACE, SHA1, SHA2
	인증 알고리즘	• MD5, SHA1, HAS-160	• MD5, SHA1, HAS-160	• MD5, SHA1, SHA256, HAS-160
	Bridge 환경의 IPSec 지원	○	• N/A	• N/A
	DPD(Dead Peer Detection)	○	• N/A	○

4. 제품 비교자료 (3)

KEY MESSAGE **UTM 제품 비교자료**

구분		AXGATE	시큐아이(NXG)	퓨쳐시스템
IPS	차단기법	• 해당 패킷 또는 세션 차단 • 특정 프로토콜및 서비스, IP에 대한 제한	• 해당 패킷 또는 세션 차단 • 특정 프로토콜및 서비스, IP에 대한 제한	• 해당 패킷 또는 세션 차단 • 특정 프로토콜및 서비스, IP에 대한 제한
	세션 및 트래픽 임계치 설정	○	○	○
	Signature-based	○	○	○
	Behavior-based	○	○	○
	User defined Sig	○	○	○
	IPS 시그니처 수	• 최대 5,000 개	• 3,000개 이상	
	자체 CERT 팀	○	X	○
Anti-DDOS/ Virus	DDos 차단	• TCP, SYNM UDP, ICMP, HTTP, • DNS Flooding	• SYN, ICMP, UDP Flooding	• SYN, ICMP, UDP Flooding
	SIP 공격 차단	• SIP register, SIP invite, SIP bye • SIP message	○	• N/A
	스캔 차단	• SNY, ACK, NULL, FIN, XMAS • UDP PORT	○	○
	탐지기법	• 패킷처리기반 탐지(File-based)	• File-based, Stream-based	• File-based, Stream-based
	지원프로토콜	• HTTP, SMTP, POP3, FTP	• HTTP, SMTP, POP3, FTP	• SMTP, POP3, FTP

4. 제품 비교자료 (4)

KEY MESSAGE **UTM 제품 비교자료**

구분		AXGATE	시큐아이(NXG)	퓨쳐시스템
Contents Filtering	URL 차단	○	○	○
	유해사이트 DB 업데이트	○	○	○
	Application 제어	• Messenger, P2P, WebHard, WebMail, SNS	• Messenger, P2P, WebHard, WebMail, SNS	• Messenger, P2P
IPv6	IPv4/IPv6 Dual Stack	○	○	○
인증	CC인증	• EAL4(FW+VPN)	• EAL4(FW+VPN)	• EAL4(IPS+VPN)

www.garnetit.co.kr

보안솔루션

웹방화벽

PIOLINK
www.piolink.co.kr

1. 제안배경

Why PIOLINK – 최적의 애플리케이션 딜리버리 서비스 제공

i

- 클라우드 데이터센터에서 웹 어플리케이션 안전을 보장하는 고성능 웹 애플리케이션 방화벽
- 대용량, 고성능, 고신뢰성 웹 애플리케이션 방화벽 1위

ii

- 국내 1위 ADC기술 기반의 차별화된 웹 방화벽 플랫폼
- 웹 방화벽 최초 12Gbps throughput/2,000만 동시세션

iii

- RSA 2,048bit key환경에서 안정적인 SSL 가속
- 클라우드 데이터센터를 위한 ‘AppTenant’ 지원

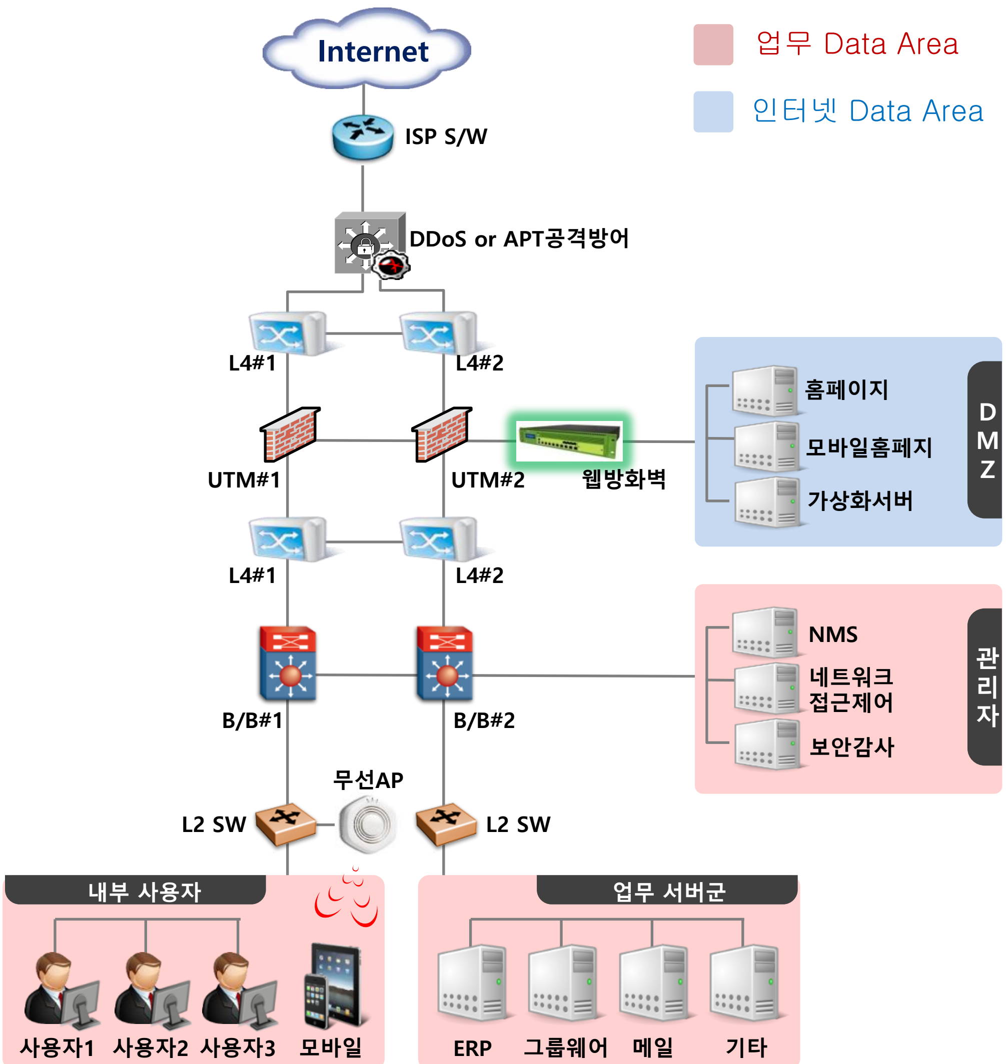
iv

- OWASP Top 10 / 국정원 8대 취약점 완벽 대응
- 웹 방화벽의 선택 기준은 빠른 서비스 응답을 보장하는 고성능과 보안성

Key finding “PIOLINK” 는 클라우드 데이터센터 최적한 전문기업

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- 대용량, 고성능, 고신뢰성 웹 애플리케이션 방화벽 1위
- 웹 방화벽 최초 12Gbps throughput / 2,000만 동시세션
- 클라우드 데이터센터를 위한"App Tenant'지원
- OWASP Top 10/ 국정원 8대 취약점 완벽 대응

제품의 특장점

- 요청검사
  - 애플리케이션 접근제어, 과다요청제어(Web DoS)
  - 버퍼 오버 플로우 차단, 업로드파일/요청형식 검사
  - 폼 필드 검사, 쿠키 보호, SQL/스크립트 차단
- 컨텐츠보호
  - 신용카드 정보유출 차단, 주민등록번호 유출 차단, 계좌번호 유출 차단
  - 웹 변조 방지, 응답형식 검사, 코드 노출 차단
- 적응학습
  - 애플리케이션 접근제어 학습, SQL/스크립트 학스, 쉘 코드 학습
- 위장
  - URL 정보 위장, 서버 정보 위장, 부적합 에러 처리, 스크립트 마스킹

제품 도입 효과

- 웹서비스 응답 지연이나 손실되는 패킷 없이 안전하고 빠른 서비스 가능
- 다양한 구성방식과 모든 IP계층을 보안(ACL/SSL/,DoS/DDoS/L7컨텐츠 필터링 등)
- 이중화 구성 시 Bypass 포트로 전원 차단시에도 안정적
- 사용자가 원하는 대로 보안설정을 쉽게 세팅 및 실시간 대시보드, 모니터링 서비스, 정보 분석 및 리포트 제공

3. 제품 라인업

KEY MESSAGE **웹방화벽 제품 라인업**

구분	WEBFRONT-KSE	WEBFRONT-KGE	WEBFRONT-KXG
이 미 지			
C P U	• 56Gbps	• 88Gbps	• 640Gbps
R A M	• 8GB	• 16GB	• 24GB
SSD	• 40GB	• 40GB	• 40GB
HDD	• 500GB	• 500GB	• 500GB
Interface(10G)	• -	• -	• 16 * 10G Fiber port (1G/10G 자동인식)
Interface(1G)	• 16 * 1G Fiber port • 8 * 1G Copper port(총 24포트)	• 16 * 1G Fiber port • 8 * 1G Copper port(총 24포트)	• 16 * 10G Fiber port (1G/10G자동인식)
Interface(옵션)	• 1 pair * Fiber Bypass (1G/10G자동인식)	• 1 pair * Fiber Bypass (1G/10G자동인식)	• 8 * 1G Fiber port • 8 * 1G Copper port • 1 pair * Fiber Bypass (1G/10G자동인식) • 1 pair * Copper Bypass
Throughput	• 1.5Gbps	• 3Gbps	• 6Gbps
동시세션	• 4,000,000	• 8,000,000	• 12,000,000

4. 제품 비교자료

KEY MESSAGE 웹방화벽 제품 비교자료

구분	파이오링크(WEBFRONT-KGE)	펜타시큐리티(WAPPLES1000)	트리니티소프트(GW-3000)
제 품 명			
Backplane	• 88Gbps	• -	• -
RAM	• 16GB	• 8GB	• 8GB
SDD	• 40GB	• -	• -
HDD	• 500GB(1TB확장가능)	• 500GB	• 500GB
Interface	• 8 * 10/100/1000BaseTX • 16 * 1000BaseSFP(총 24포트)	• 8 * 10/100/1000 BaseTX • 2 * 1000 BaseSFP	• 4 * 10/100/1000 BaseTX • 4 * 1000 BaseSFP(Combo)
Bypass(옵션)	• 2 x 1000 Base Optical Bypass (1G/10G자동인식)	• 2 x 1000 Base Optical Bypass • 4 x 1000 Base Optical Bypass	• 4 * 1000 Base Optical Bypass
Throughput	• 3Gbps	• 2Gbps	• 2Gbps
동시 세션 수	• 8,000,000	• -	• -

www.garnetit.co.kr

보안솔루션

개인정보유출 차단 솔루션

NASOL
Network Advanced Solution
www.nasol.co.kr

1. 제안배경

Why Nasol – 개인정보 차단율/ 처리성능/안정성 1위 기업

i
- 각 기관 홈페이지내의 게시판에 자유롭게 글을 올리면서 개인의 주민번호, 여권번호, 외국인등록번호 운전자번호 등과 같은 개인정보가 등록되어 사회 문제화 되는 사례가 발생

ii
- 시스템 폭주에 대비 안정적인 웹 시스템 운영 필요
- 보안 모듈 탑재로 인한 보안 서버 구축

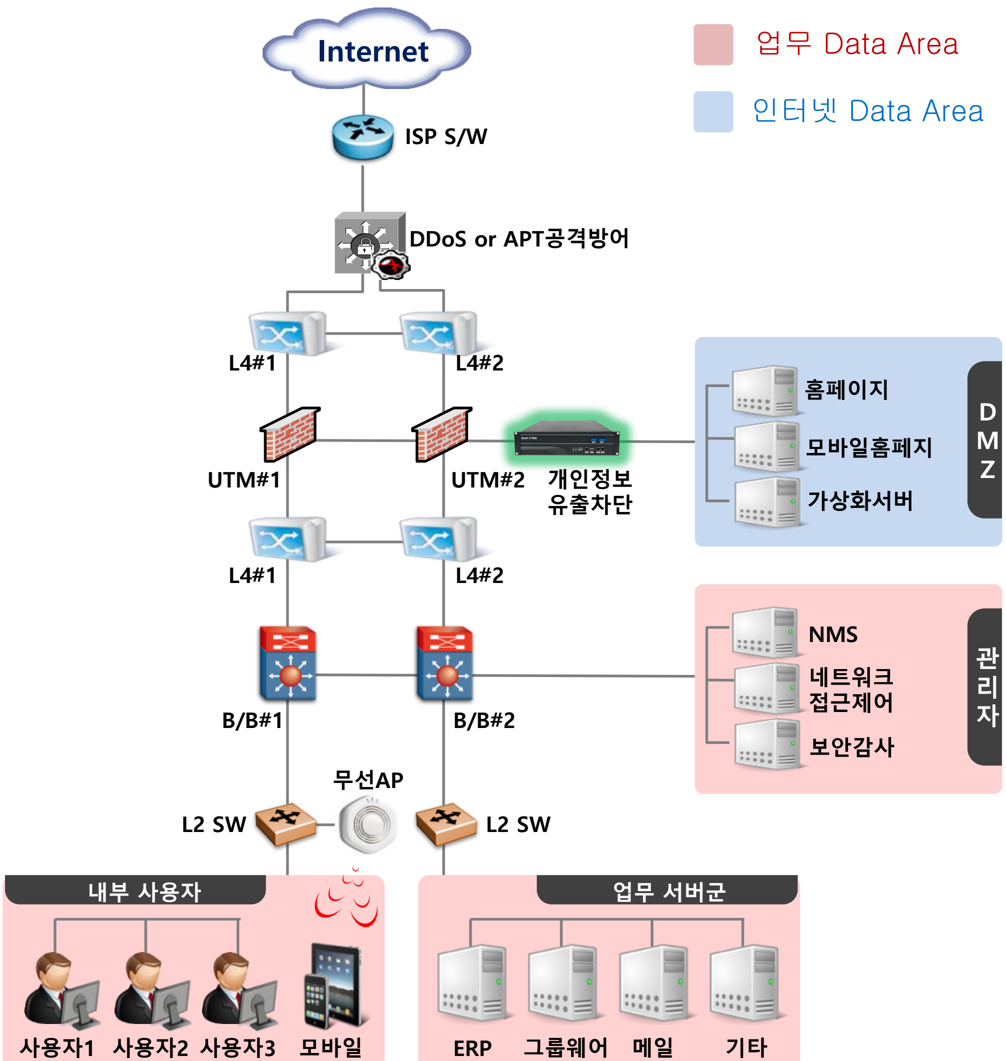
iii
- 개인정보 유출 차단율 과 장비의 처리량이 우수한 제품

iv
- 국정원 CC인증(EAL2)와 GS인증을 받은 안정성 있는 제품

Key finding | **SmartXFilter 개인정보의 차단율과 장비 성능이 1위 제품**

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- 개인정보 차단기능과 웹 가속기 기능을 동시에 한 장비에서 수행하는 일체형 제품
- 보안 모듈 탑재로 인한 보안 서버 구축
- 캐싱 기술을 적용한 처리량의 증가
- SSL 및 SSL 가속 기능 탑재

제품의 특장점

- 개인정보차단기능
  - 웹 서버나 DB서버로부터 전송되는 컨텐츠에 대한 개인정보차단 기능
  - 첨부파일 내의 개인정보 차단(HWP, MS OFFICE, 압축파일, HTML, HTM 등)
- 웹 가속기 기능
  - 컨텐츠의 개인정보를 검색한 후 데이터의 압축 전송 및 압축 캐싱의 지원으로 응답속도 향상
- 입력차단(사전차단)
- 출력차단(사후차단)
- 시스템 처리 용량 증가
- 개인정보의 차단을 위해 서버소스의 수정은 전혀 없음

제품 도입 효과

- 다양한 형태의 문서 차단(pdf, zip, xls 등등)
- 검사 방식의 차별화로 완벽한 개인정보 차단
- 시스템 폭주시의 안정적인 운영
- 홈페이지의 응답속도의 개선
- 웹 시스템의 부하 감소

3. 제품 라인업

KEY MESSAGE **웹 개인정보 유출차단 제품 라인업**

구분	SmartXFilter PL1000	SmartXFilter PL2000	SmartXFilter PL3000
이 미 지			
C P U	Xeon Quadcore 2.13 GHz	Xeon Quadcore 2.13 GHz	Xeon Quadcore 2.13 GHz x 2
R A M	• 2GB	• 2GB	• 4GB
HDD	• 500GB		
Interface	• 10/100/1000 Base-T Copper 2 Port		
Interface(옵션)	• 2 * 1G Fiber port • 2 * 10G Fiber port		
Throughput	• 1Gbps		
처리 세션 수	• 1,000	• 3,000	• 4,000
바이패스 카드	• 내장		

4. 제품 비교자료

KEY MESSAGE 개인정보유출 차단솔루션 제품 비교자료

구분	SmartXFilter	타사제품
기 능	• 개인정보 유출 차단& 웹가속기 기능 동시지원	• 개인정보 유출만 차단
응답속도	• 웹 가속기 기능의 탑재로 홈페이지 응답 속도가 향상 되고 한번 검색한 파일은 압축캐싱 하여 효율을 높임	• 응답속도가 저하될 가능성 많음
성 능	• 장비내에 하드웨어적인 바이패스 카드의 탑재로 장애 시 바이패스 가능하며 오탐이 적고 처리량이 큼	• 오탐이 자주발생하고 하드디스크 장애에 대한 처리가 어려움
차단방법	• 개인정보의 입력시(Inbound)와 출력시(Outbound) 동시 차단	• 개인정보 입력시만 차단(Inbound 차단)
설치의 용이성	• 웹서버의 소스를 변경하지 않고 간단히 웹 서버 앞단에 설치만 하면 이를 통과하는 모든 시스템에 대해 적용 가능	• 웹서버의 소스 수정이 반드시 필요하며, 게시판 변경 시 항상 소스를 수정해야 하므로 관리가 어려움
주요기능	• 개인정보차단 • 웹가속 기능으로 홈페이지 응답속도 향상 및 웹서버 부하감소, SSL및 SSL가속기능 지원	• 개인정보차단

www.garnetit.co.kr

보안솔루션

네트워크접근제어 (NAC)

NetMan

www.netman.co.kr

1. 제안배경

■ **Why NetMan – 국내 유일의 유,무선 통합 네트워크 접근제어 전문 업체**

i
- 국내 유일의 유,무선 통합 네트워크 접근 제어 솔루션
- 네트워크에 접속하는 시점에서부터 보안 강화 필요

ii
- 보안 위협에 대해 사전 대응으로 보안 사고를 예방
- 유선랜 환경에서의 NAC은 802.1x 지원, 스위치와의 연동만이 유일한 대안

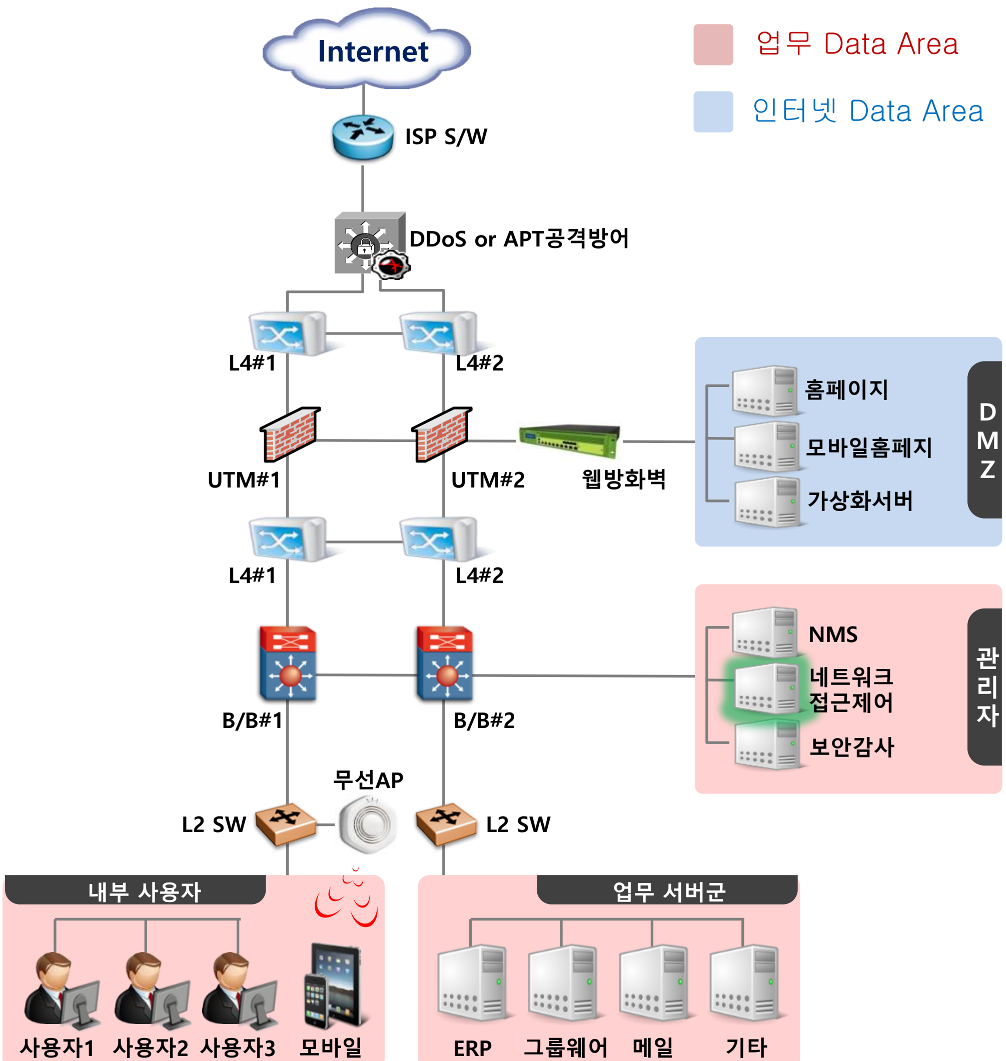
iii
- 네트워크 접근 단계에서 원천적인 차단이 불가능한 유선랜 보안 취약점이 존재
- 무선랜 환경에서의 중복되는 사용자 인증 처리 문제점 발생

iv
- 유,무선별로 이원화된 보안 정책 및 관리 포인트
- 각각의 인증 솔루션 도입으로 인한 비용 증가 발생

Key finding **"넷맨" 국내 유일의 유,무선 통합 네트워크 접근제어 전문업체**

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- 이원화된 유, 무선 네트워크 환경을 통합 관리하는 유일한 NAC 솔루션
- Smart NAC의 강력한 기능으로 내부 보안의 문제점들을 해결
- 다양한 네트워크 환경에서 보안과 안정성이 검증된 솔루션
- 11년간 네트워크 보안 관리 솔루션을 개발 전문 업체로 성장해왔으며 신뢰할 수 있는 기업의 제품

제품의 특장점

- 사용자 인증
  - 유, 무선 통합 Client를 이용한 사용자 인증과 웹 기반의 Clientless 사용자 인증
  - 802.1x 기반의 무선 보안 암호화 인증 Client 제공
- 단말 인증
  - ARP 기반의 단말 접근 통제
  - 비인가 단말에 대한 네트워크 접근 차단 및 격리
  - 주요 네트워크 장비 및 단말에 대한 IP충돌 보호
- 단말 보안 취약성
  - 필수, 불법 소프트웨어 검출, 필수 소프트웨어 설치 유도/불법 소프트웨어 삭제
  - 불법 우회 경로 탐지 및 차단
- IT자산관리

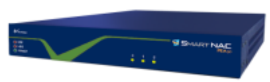
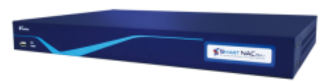
제품 도입 효과

- 편리한 IP신청 및 할당 기능
- 편의성 및 보안이 향상된 Smart NAC DHCP
- Smart NAC가 제공하는 지속적인 Upgrade Service
- CC인증(EAL 2), GS인증을 통한 높은 신뢰성

3. 제품 라인업

KEY MESSAGE **네트워크접근제어 제품 라인업**

구분	SNAC-PM1000	SNAC-PM3000	SNAC-PM5000
Policy Manager			
설명	• 사용자 인증 정책 서버 • 사용자 및 단말의 네트워크 사용 이력 관리 • 단말의 물리적인 네트워크 위치 추적		

구분	SNAC-PEA30	PSNAC-PEA70	SNAC-PEA100
이 미 지			
설명	• 접근 단말에 대한 허용/격리/차단, IP보호 및 오남용 방지 • DHCP 서비스, 불법 DHCP 서버 검출 • 802.1Q Trunk 연결 지원		

구분	SNAC-Pclient(SE)	SNAC-Pclient(XE)	SNAC-Pclient(Wired & Wireless)
이 미 지			
설명	• WinXP/Vista/Win7.., 무선 서플리컨트 • 802.1x/WPA2 지원, 단말의 무결성 점검		

4. 제품 비교자료

KEY MESSAGE 네트워크접근제어 제품 비교자료

구분	넷 맨	G 사	F 사
이 미 지			
구 성 요 소	• Policy Manager, Policy Enforcement Agent Policy Client	• Policy Center, Sensor • Thin Agent	• Enterprise, Manager(CEM) • CounterACT
	• 고가용성 보장을 위한 Active-Stanby 구성	• 고가용성 보장을 위한 Active-Stanby 구성	• 고가용성 보장을 위한 Active-Stanby 구성
	• CS 기반 (Access/802.1Q 연결방식)	• WEB 기반(Access/802.1Q 연결방식)	• CS기반(Mirroing 연결방식)
사 용 자 인 증	• 무선랜 인증/유선랜 인증 암호화 Client 지원	• 무선랜 인증/유선랜 인증 암호화 Client 지원	• 무선랜 인증/유선랜 인증 암호화 Client 지원 안함
	• 웹 기반의 IP/Password 인증	• 웹 기반의 IP/Password 인증	• 웹 기반의 IP/Password 인증
단 말 인 증	• ARP 기반의 접근 통제	• ARP기반의 접근통제	• Mirroling기반
	• 불법 단말의 네트워크 접근 차단	• 불법 단말의 네트워크 접근 차단	• 불법 단말의 네트워크 접근 차단 안됨
	• DHCP IP할당 내역 통계 정보 제공	• DHCP IP할당 내역 통계 정보 제공 안됨	• DHCP IP할당 내역 통계 정보 제공 안됨
단말 무결성 검증	• 소프트웨어 설치 정보 검색 가능	• 소프트웨어 설치 정보 검색 가능	• 소프트웨어 설치 정보 검색 가능
	• ARP Spoofing을 발생기킨 단말 검출 및 알람	• ARP Spoofing을 발생기킨 단말 검출 및 알람	• ARP Spoofing을 발생기킨 단말 검출 및 알람
	• 단말에 허용되지 않은 IP를 가진 인터페이스가 존재할 경우 탐지 및 차단	• 단말에 허용되지 않은 IP를 가진 인터페이스가 존재할 경우 탐지 및 차단	• 단말에 허용되지 않은 IP를 가진 인터페이스가 존재할 경우 탐지 및 차단하지 못함
IT자산 관리	• 단말의 하드웨어 정보 통계	• 단말의 하드웨어 정보 통계	• 단말의 하드웨어 정보 통계
	• 네트워크 트래픽 관리	• 네트워크 트래픽 관리 안됨	• 네트워크 트래픽 관리 안됨
운영 편의성	• 인사 DB연동 가능	• 인사 DB연동 가능	• 인사 DB연동 가능
인 증	• CC인증(EAL 2) • GS인증	• CC인증(EAL2) • GS인증	• CC인증(EAL4) • GS인증 없음

www.garnetit.co.kr

보안솔루션

시스템접근제어&감사

www.modosone.com

1. 제안배경

■ **Why 모두스원 – 시스템접근제어&보안감사 솔루션 기술력 No1.**

i
- 사용자의 실수(Human Error)에 대한 대비책이 없음
- 한국기업 82%가 내부장에 의한 보안사고로 발생(CERT, CSO 매거진 발췌)

ii
- 인증 받은 사용자가 네트워크 장비 혹은 서버에 접속 시 어떤 작업을 하는지 알 수 가 없음
- 장애 발생시 가장 빠른 복구를 위한 로그 추적 기능이 없음

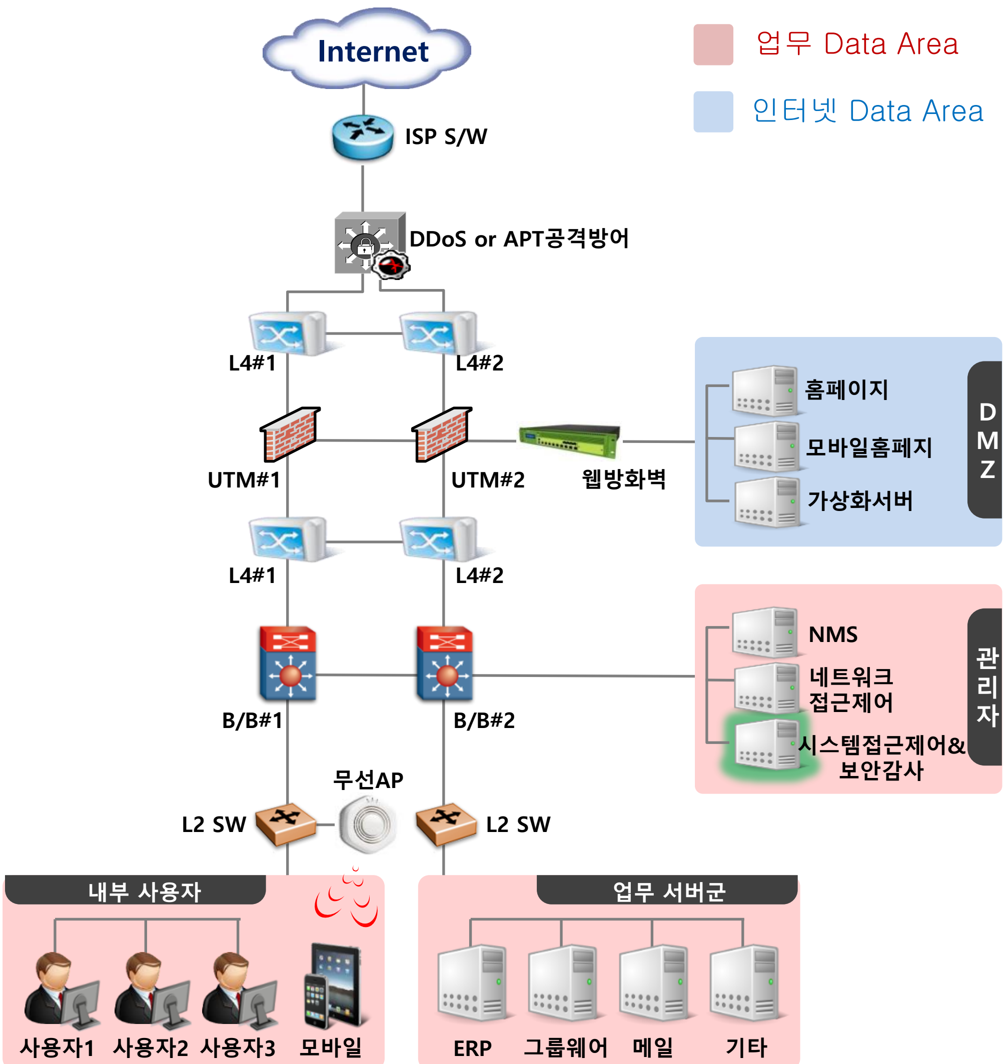
iii
- 넘쳐나는 Agent를 관리하기 위한 관리자의 어려움 발생
- 내부직원의 온라인 활동에 대한 로그, 모니터링 그리고 감사가 필요함

iv
- 수사에 사용될 수 있는 데이터 수집 및 보관
- 안전한 백업과 복구 프로세스의 수립이 필요

Key finding “보안감사 접근통제” 는 휴먼에러 방지에 따른 무장애 서비스

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- 서버 및 네트워크 장비에 대한 원격지 사용자의 인증, 암호화 통신, 권한 및 접근제어, 명령어 제어, 세션관리 및 작업내역 모니터링, 실시간 감사, 로깅을 수행하는 장비
- 웹 기반의 GUI를 제공하며, 관리자, 그룹관리자, 사용자의 3단계 레벨 사용자 관리
- 세션 및 작업로그 검색 및 백업(이력관리)
- 접속 리스트 및 Telnet/SSH/FTP/SFTP/RDP등 접속 버튼 제공

제품의 특장점

- 서버와 클라이언트에 Agentless 방식
- 명령어제어(금지명령어 및 사용자 실수에 의한 명령어 실행 차단)
- 권한제어(서버 및 네트워크 접근 시 권한에 따른 접속제어)
- 다양한 인증 연동(PKI 인증 연동, RADIUS 인증 연동)
- 한번의 로그인으로 여러 서버 동시 접속이 가능
- 감사로그(사용자들의 모든 로그 저장 및 명령어 저장, 정책위반 저장)
- 장애 발생 시 빠른 복구를 위한 로그 제공

제품 도입 효과

- 명령어 제어 및 세션제어에 따른 Human error를 사전에 방지하여 고 가용성 실현
- 작업자긍에 의한 시스템 장애 발생 시 작업로그의 빠른 추적에 따른 복구방안 제시
- 기존의 유지보수 업체들이 작업시간의 서비스 지연을 방지하는 효과 발생
- 사용자들은 각자가 가지고 있는 장비의 접근 권한에 따라 작업함으로써 사용자 편리

KEY MESSAGE **시스템접근제어&보안감사 제품 라인업**

구분	GATEONE-TM G100	GATEONE-TM G1000
Policy Manager		
규격설명	• 1 ~ 50node까지 사용가능 한 매니저 S/W • Telnet, SSH, FTP, SFTP, RDP(원격터미널) 프로토콜 지원 • CC인증(EAL3), GS인증	• 1 ~ 100node까지 사용가능 한 매니저 S/W • Telnet, SSH, FTP, SFTP, RDP(원격터미널) 프로토콜 지원 • CC인증(EAL3), GS인증

구분	GATEONE-TM G2000	GATEONE-TM G3000
Policy Manager		
규격	• 1 ~ 300node까지 사용가능 한 매니저 S/W • Telnet, SSH, FTP, SFTP, RDP(원격터미널) 프로토콜 지원 • CC인증(EAL3), GS인증	• 300node이상 ~ 사용가능 한 매니저 S/W • Telnet, SSH, FTP, SFTP, RDP(원격터미널) 프로토콜 지원 • CC인증(EAL3), GS인증

4. 제품 비교자료

KEY MESSAGE 시스템접근제어&보안감사 제품 비교자료

구분	GATEONE	SECUREGUARD	NGS	HI-WARE	I/O-insight
솔루션 탑재 OS	Linux	Embedded Linux	Linux	Window Server	Window Server
솔루션 사용 DBMS	MySQL	MySQL	MySQL	Oracle	MS-SQL
감사대상 서버 Agent 설치	설치안함	설치함 (window감사)	설치안함	설치안함	설치안함
사용자 PC Agent 설치	설치안함	설치함	설치함	ActiveX설치	설치함
자체 OTP 지원	지원	불가	불가	불가	불가
금지명령어/허용명령어	지원	지원	지원	지원	지원
금지명령어 정규 표현식 지원	지원	불가	지원	지원	불가
Script내 금지명령어 탐지/차단	지원	불가	불가	불가	불가
Script 실행 시 Script 내용저장	지원	불가	불가	불가	불가
VI 실행모드 명령어 탐지/차단	지원	불가	불가	불가	불가
CC인증	인증 (시스템접근관리, EAL3)	비인증	비인증	인증 (기타, EAL2)	비인증

www.garnetit.co.kr

보안솔루션

DNS보안

Infoblox
CONTROL YOUR NETWORK

www.Infoblox.com

1. 제안배경

Why Infoblox – DNS보안 전용 어플리케이션 선두 기업

i

- 기존 소프트웨어 타입의 일반 DNS 서버 방식 구현
- DNS 보안사고 및 취약점에 대한 우려가 급증

ii

- 장애발생시 OS 제조사의 기술지원 제한

iii

- 도메인 접근 이력에 대한 직관적인 로깅 / 모니터링 체계 마련 시급

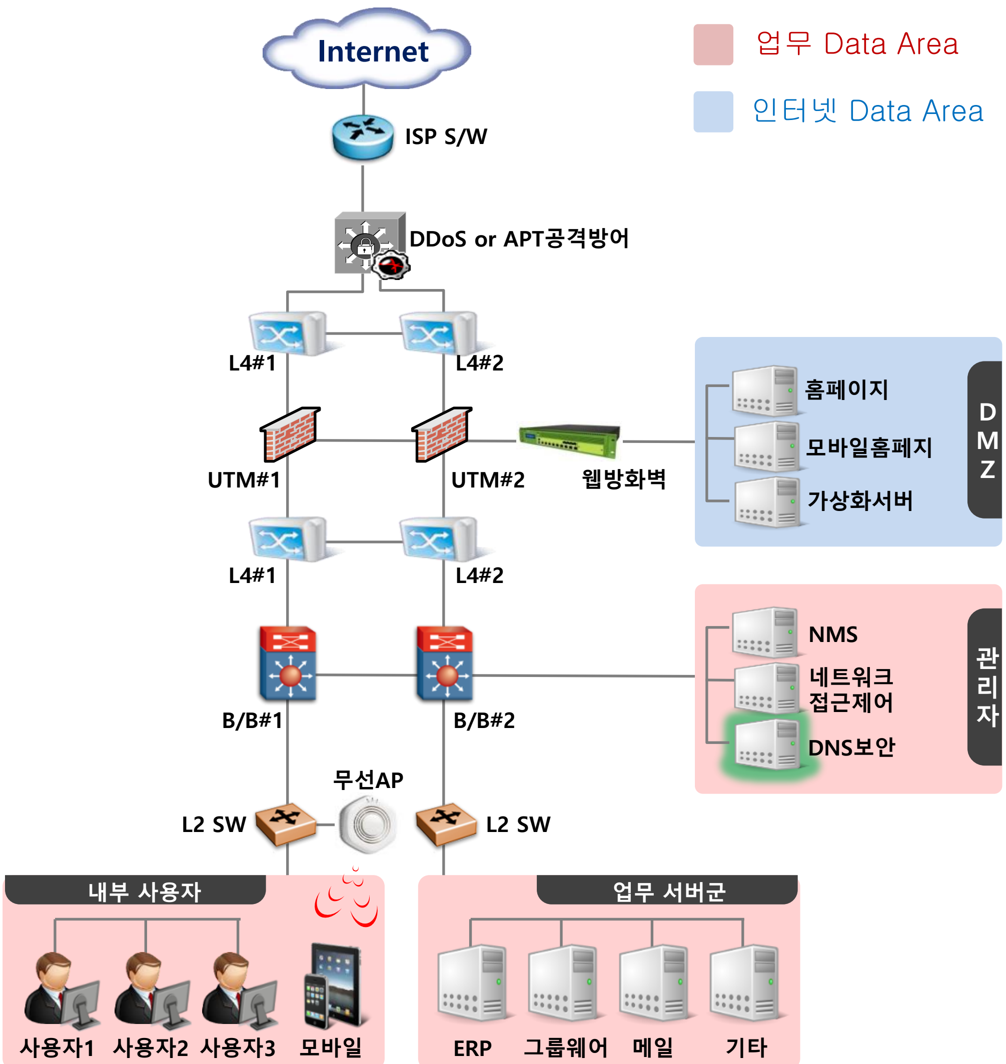
iv

- 인터넷 환경이 비즈니스 환경의 기본 인프라 -> 체계적 도메인 관리환경 필요성 급증
- IP 관리체계의 내부 보안 중요성은 확대되나, 도메인에 대한 기술적/보안적 관리는 매우 허술함

Key finding | **"Infoblox" 는 핵심 프로토콜 서비스용 통합형 어플라이언스**

2. 네트워크 구성도

KEY MESSAGE **네트워크 구성 특장점**



제품의 개요

- 핵심 프로토콜 서비스용 통합형 어플라이언스(DNS, DHCP, RADUS, TFTP 서비스 일체)
- DNS, DHCP, RADIUS 등에 각기 필요한 OS 기반 서버 중복 투자 부담 해소
- 하드웨어 플랫폼으로 기존 소프트웨어 기반 솔루션의 한계 극복
- 데이터 관리를 위한 별도의 DB 시스템 구성 불필요(장비에 DB 탑재)

제품의 특장점

- 전용 장비로써 하드웨어 HA Failover 기능 제공
- 직관적인 통합 관리 화면 제공
- 관리자 권한 기능
  - 접속 권한 레벨에 따른 관리자 그룹 설정 기능 제공
- DNS query response 분석/모니터링, DNS Query Log 리포팅, DHCP History 리포팅
  - 통계 및 리포팅 기능
- DNS 시스템 상태 모니터링 기능
- DNS 공격 및 취약점에 대한 대처 기능

제품 도입 효과

- DNS 보안사고 급증에 대한 예방 환경 확보(DNS 파밍, 피싱, 캐시포이즈닝 등)
- 외부 접속자의 악의적인 도메인 접근 시도에 대한 모니터링 및 처리 체계 확보
- 전담 기술지원, 트러블슈팅 시 책임소재 명확화
- 직관적인 웹 기반 GUI 방식으로 사용자의 편리성 제공

3. 제품 라인업

KEY MESSAGE **DNS보안 제품 라인업**

구분	Trinzic 820	Trinzic 1420	Trinzic 2220
이 미 지			
설 명	• 소기업 및 지사 애플리케이션용 • 독립 실행형 장치로 구성하거나 HA구성 할 수 있음	• 중소기업 및 지사 애플리케이션용 • 독립 실행형 장치로 구성하거나 HA구성 할 수 있음 • 현장 교체 하드 드라이브 및 전원 공급 장치를 지원하며, 예비 전원 공급 장치가 옵션으로 제공	• 대규모 ISP, 통신 사업자 및 기타 네트워크 사업자용 • 복원력과 보안을 높이면서, 가능한 최저 TCO로 높은 DNS 캐싱 처리량을 제공 • 예비 전원 공급 장치 및 하드 드라이브 (RAID10)을 제공합니다
Interface	• 10/100/1000BASE-T(LAN포트) * 2Port • 10/100/1000BASE-T(HA포트) * 1Port • 10/100/1000BASE-T(MGT포트) * 2Port	• 10/100/1000BASE-T(LAN포트) * 2Port • 10/100/1000BASE-T(HA포트) * 1Port • 10/100/1000BASE-T(MGT포트) * 2Port • 1000BASE-X(SFP포트) * 1Port(옵션)	• 10/100/1000BASE-T(LAN포트) * 2Port • 10/100/1000BASE-T(HA포트) * 1Port • 10/100/1000BASE-T(MGT포트) * 2Port • 1000BASE-X(SFP포트) * 1Port(옵션)
초당 DNS 쿼리 수	• 15,000	• 50,000	• 143,000
초당 DHCP 임대 수	• 105	• 4300	• 600
USB 포트	• USB 2.0/1.0 호환 1개	• USB 2.0/1.0 호환 1개	• USB 2.0/1.0 호환 1개
예비 하드 웨어	• 지원 안함	• 보조 전원 공급장치(옵션)	• 핫 스왑형 예비 전원 공급 장치, 팬 및 디스크 4개로 구성된 RAID-10

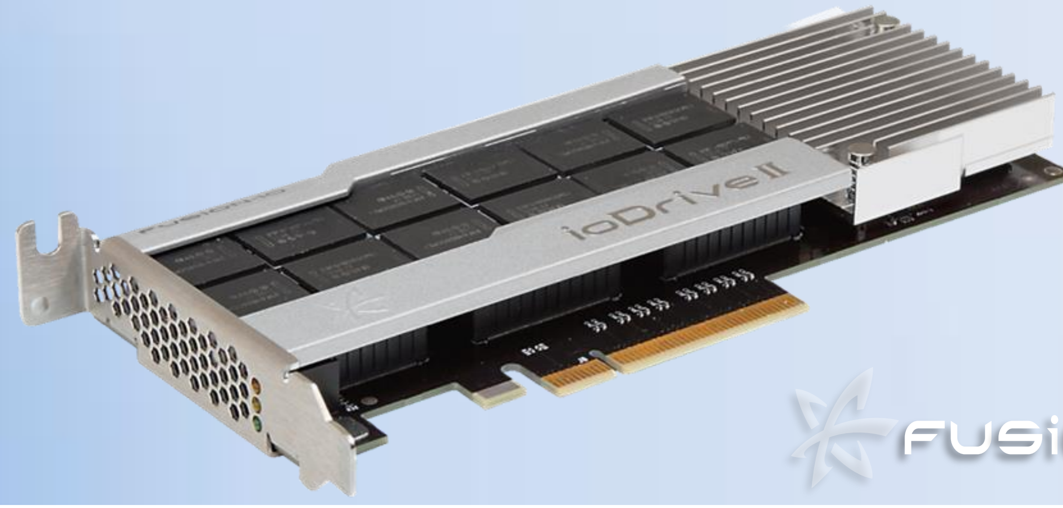
4. 제품 비교자료

KEY MESSAGE **DNS보안 제품 비교자료**

관리 요구 사항	Infoblox	BlueCat
GUI 관리상에서의 자동적인 DNS Firewall 기능.	Yes	No
DHCP Fingerprinting	Yes	No
Reporting 기능	Yes	No
DNS 설정의 부분 배치 스케줄 기능	Yes	No
CSV Import 기능	Yes	No
장비 모니터링 기능	Yes	No
Grid 통합 관리 기능	Yes	No
Full IPv6 기능	Yes	No
유연한 GUI	Yes	No
BlackList rule_set 기능	Yes	No
Workflow (역할별 관리자 권한 위임 기능)	Yes	No
bulk dns update (대량의 DNS 정보 업데이트 기능.)	Yes	No
IDN Converter 기능	Yes	No
Match Destinations	Yes	No

IO Accelerator 솔루션

FUSION-IO



1. 제안배경

- **Why FUSION-IO – 낸드플래시(전원이 없는 상태에서도 계속해서 데이터가 저장되는 플래시 메모리)기반의 메모리 스토리지**

i

- 고성능 CPU와 느린 Disk IO 사이의 지연을 줄여줌으로써, Database와 Application의 성능 문제를 해결

ii

- 4년 연속 Enterprise Flash Storage시장에서 독보적인 세계 1위
- DB, 가상화, 빅데이터 등 다양한 분야에 적용, 최대 효과 발휘

iii

- 서버(PCIe슬롯)에 직접장착하여 최고의 가속 성능(I/O이슈가 있는 Application에 이용)
- 외장공유스토리지로 최고의 확장성 (DB처리성능 17배 향상)
- 캐싱장비로 최고의 호환성 (기존 SAN/NAS 변경 없이 속도 향상)

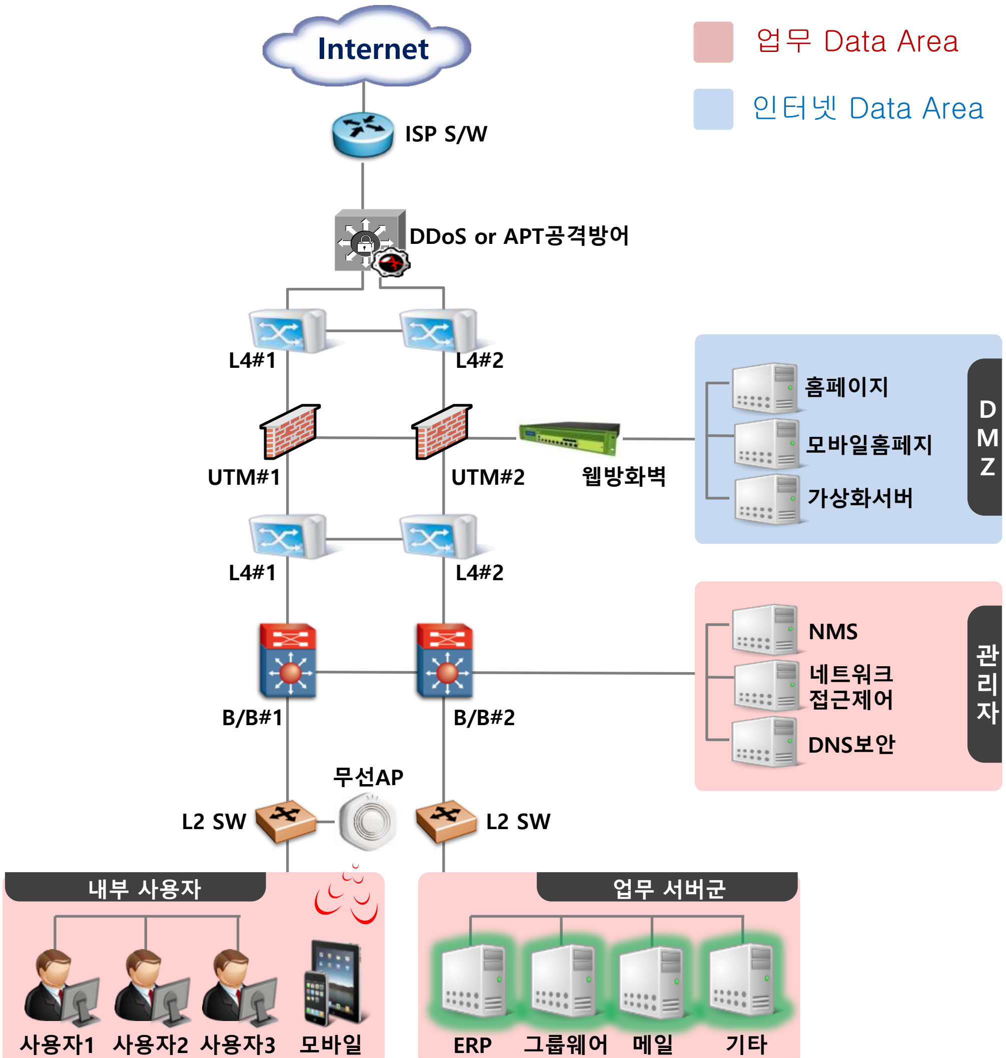
iv

- 퓨전아이오는 낸드플래시 메모리 저장장치의 선두 기업으로 수 많은 포춘500, 포춘100의 기업 고객이 있으며 그들의 시스템과 애플리케이션을 가속함

Key finding **"FUSION-IO" 는 어플리케이션 및 데이터베이스 서버의 최고 성능을 보장**

2. 네트워크 구성도

KEY MESSAGE 구성 특장점



제품의 개요

- Fusion-IO는 NAND Flash를 사용하여 저장 장치를 만든 업계 최초의 회사
- ioMemory는 갑작스런 정전/전원 차단에도 Power cut safe기술을 통하여 안전하게 데이터를 보호
- ioMemory가 장착되는 PCIe는 CPU에 가장 빨리 Data를 직접 전달할 수 있는 가장 가까운 경로로써 I/O 성능에 최적화

제품의 특장점

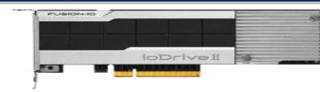
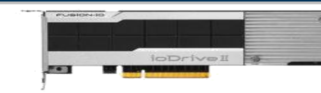
- 세계 최초의 Flash Memory 기반 PCIe Storage
- 5년 연속 Enterprise Flash Storage 세계 1위
- 기존 하드웨어 환경의 변경 없이 적용이 가능
- 캐싱을 이용한 무 중단 쓰기 가능
- 활성화된 작업set의 캐시화
- 모든 주요 스토리지의 방식을 지원
- SAN/NAS/DAS 등 모든 방식의 스토리지와 호환
- File, Volume, Disk 에 따라 캐시 관리의 제어가 가능

제품 도입 효과

- DB 성능 개선, 서버당 처리성능 혁신 및 획기적인 TCO 절감
- Batch, Query, 분석성능 개선
- Replication, Backup 시간단축
- 가상화 환경의 I/O Bottleneck 문제 해결

3. 제품 라인업

KEY MESSAGE **FUSION-IO 제품 라인업**

구분	IoDrive2 MLC				IoDrive2 SLC	
이 미 지						
Capacity	• 365GB MLC	• 785GB MLC	• 1.2TB MLC	• 3.0TB MLC	• 400GB SLC	• 600GB SLC
Read Bandwidth - 1MB	910 MB/s	1.5 GB/s	1.5 GB/s	1.5 GB/s	1.4 GB/s	1.5 GB/s
Write Bandwidth - 1MB	590 MB/s	1.1 GB/s	1.3 GB/s	1.3 GB/s	1.3 GB/s	1.3 GB/s
Ran. Read IOPS - 512B	137,000	270,000	275,000	143,000	360,000	365,000
Ran. Write IOPS - 512B	535,000	800,000	800,000	535,000	800,000	800,000
Ran. Read IOPS - 4K	110,000	215,000	245,000	136,000	270,000	290,000
Ran. Write IOPS - 4K	140,000	230,000	250,000	242,000	270,000	270,000
Read Access Latency	68µs	68µs	68µs	68µs	47µs	47µs
Write Access Latency	15µs	15µs	15µs	15µs	15µs	15µs
Bus Interface	PCI Express 2.0					
Weight	6.6 ounces			9.5 ounces	6.6 ounces	
Form Factor	HH x HL			FH x HL	HH x HL	
Warranty	5 years or maximum endurance used					

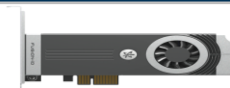
3. 제품 라인업

KEY MESSAGE **FUSION-IO 제품 라인업**

구분	IoScale			
이 미 지				
Capacity	• ioScale 410GB	• ioScale 825GB	• ioScale 1650GB	• ioScale 3.2TB
Form Factor	HHxHL	HHxHL	HHxHL	FHxHL
Read Bandwidth (1MB)	1.4 GB/s	1.4 GB/s	1.4 GB/s	1.5 GB/s
Write Bandwidth (1MB)	700 MB/s	1.1 GB/s	1.1 GB/s	1.3 GB/s
Random Read IOPS (512 bytes)	78K	135K	144K	115K
Random Write IOPS (512 bytes)	535K	535K	535K	535K
Read Access Latency	77µs	77µs	77µs	92µs
Write Access Latency	19µs	19µs	19µs	19µs
Power Profile	< 25W	< 25W	< 25W	< 25W
PBW (typical)	2	4	8	20
Weight	156g			269g
NAND Type	MLC (Multi Level Cell)			

3. 제품 라인업

KEY MESSAGE **FUSION-IO 제품 라인업**

구분	IoDrive2 DUO		IoFX	
이 미 지				
Capacity	• **2.4TB MLC**	• **1.2TB SLC**	• **420GB**	• **1650GB**
Read Bandwidth - 1MB	3.0 GB/s	3.0 GB/s	1.4 GB/s	1.4GB/s
Write Bandwidth - 1MB	2.5 GB/s	2.5 GB/s	700MB/s	1.1GB/s
Ran. Read IOPS - 512B	540,000	700,000	N/A	N/A
Ran. Write IOPS - 512B	1,100,000	1,100,000	N/A	N/A
Ran. Read IOPS - 4K	480,000	580,000	N/A	N/A
Ran. Write IOPS - 4K	490,000	535,000	N/A	N/A
Read Access Latency	68µs	47µs	77µs	77µs
Write Access Latency	15µs	15µs	19µs	19µs
Bus Interface	PCI Express 2.0 x8 electrical x8 physical			
Weight	312g		190g	
Form Factor	Full-height, half-length		half-height, half-length	
Warranty	5 years or maximum endurance used		3 years or maximum endurance used	

www.garnetit.co.kr

망분리솔루션

퓨전데이타

FusionDATA
Anytime, Anywhere, Any devices
www.fusionsys.net

1. 망 분리 필요성

KEY MESSAGE **정보보호의 중요성**

• 정보유출 사례로 인한 내부정보 유출 및 외부침입을 방지해야 할 필요성 대두

2012. 07	통신사	외부 침입으로 인한 870만명 고객정보 유출
2011. 11	게임사	외부 침입으로 인한 1320만명 고객 정보 유출
2011. 07	포탈사이트	외부 침입으로 인한 3500만명 고객 정보 유출
2011. 05	증권사	해커의 의해 1만 6천 고객 정보 유출
2011. 05	전자금융	8,000명의 입사지원자 정보 유출
2011. 04	캐피탈	해커에 의해 175만명의 고객정보 유출
2010. 02	반도체	장비납품업체가 내부직원과 결탁하여 95건의 반도체 기술을 유출
2009. 05	선박	선박 엔진부품 설계도면 1만7,000여장을 유출하여 동일부품 중국, 미국, 일본 등에 수출
2008. 09	정유사	집단소송을 유도하기 위해 법무법인과 고객센터 운영 자회사 직원이 결탁하여 1,100만명에 달하는 고객정보 유출
2008. 04	텔레콤	고객 600만명의 개인정보를 제휴사에 판매
2008. 03	전자	연구소 간부가 중국내 전자회사로 이직하며 PDP 설계/생산 기술을 유출

1. 망 분리 필요성(계속)

KEY MESSAGE 망 분리 법안 발의 및 증빙자료

정보통신망법 개정

(근거법령 : 제28조)

① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실・도난・누출・변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적・관리적 조치를 하여야 한다.

1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립・시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치・운영
3. 접속기록의 위조・변조 방지를 위한 조치
4. 개인정보를 안전하게 저장・전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신 소프트웨어의 설치・운영 등 컴퓨터바이러스에 의한 침해 방지조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

② 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.

근거시행령

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 (제15조의 2)

② 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다. 다만, 제3호의 조치는 전년도 말 기준 직전 3개월간 그 개인정보가 저장.관리되고 있는 이용자수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다.

1. 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근권한의 부여・변경・말소 등에 관한 기준의 수립・시행
2. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치・운영
3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷 망 차단
4. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영
5. 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치

개정 후 12개월 뒤 의무 시행

개정 2012. 2 → 유예기간 → 시행 2012. 8 → 계도기간 → 의무화 2013. 2

2. 망 분리 개요

KEY MESSAGE 망 분리란?

업무영역과 인터넷 영역을 격리하여 사용

- 모든 사내 업무 시스템 사용
- 업무영역내 자유로운 문서교환 가능
- 외부 인터넷 및 저장매체 사용 불가
- 파일 전송센터를 통한 외부 자료 전달
- 인터넷 영역으로 자료 유출 차단

- 외부 인터넷 사용
- 업무 영역의 자료 접근 불가
- 외부 데이터 반입 차단

Key finding “망 분리” 는 이제 선택이 아닌 필수의 시대

3. 망 분리 방식

KEY MESSAGE 망 분리 구성 방식

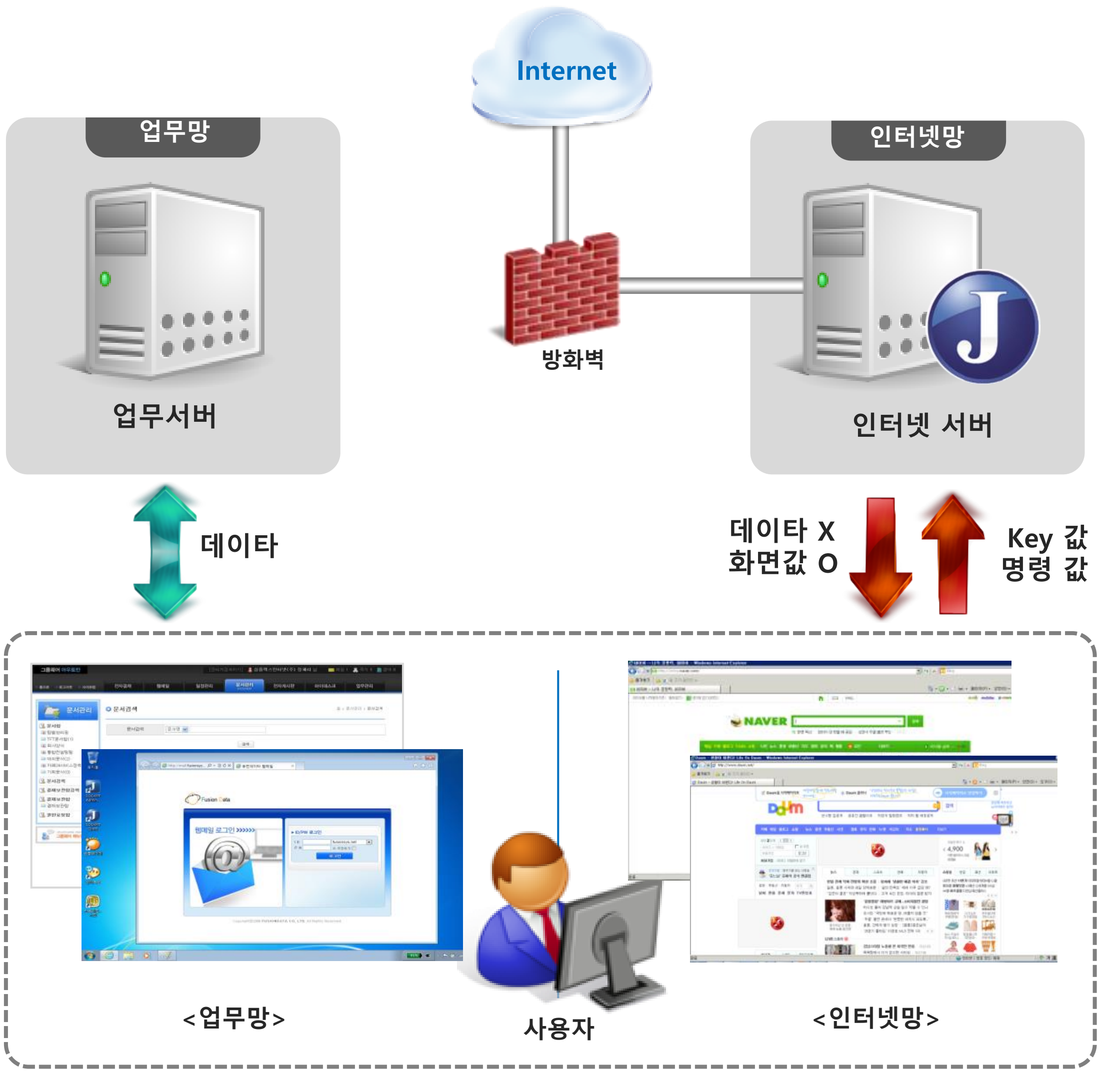
4. 망 분리 방식 별 장·단점

KEY MESSAGE 망 분리 방식 별 장·단점

구분	방안		장점	단점
물리적(H/W) 망 분리	PC 이중화		• 1명의 사용자당 2PC 구성으로 명확한 망 분리 적용	• 업무 효율성의 저하 • 영역간 자료 이동 시 보안 위협 • 구축의 고비용 및 업무 장소의 협소
	망 전환 방식		• PC영역 이중화(업무용, 인터넷 접속 HDD)	• 네트워크 전환 시 리부팅 으로 인한 업무 효율성 저하
논리적(S/W) 망 분리	Client PC 기반	[CBC]	• PC 영역의 HDD 분할 사용 • 1대의 PC 에 2개의 OS 사용으로 인한 Client PC 의 자원 사용 • 업무 망 / 인터넷 망 브라우저간의 자동 전환	• Client PC 의 고사양 지원 • Client PC 의 H/W 장애 시 업무 및 인터넷 사용에 대한 동시 장애 발생 • Client PC 유지보수 및 자료유출 방지를 고려해야 함
	서버 가상화	[VDI]	• 관리적 측면의 중앙 통제성 높음 • 자료 중앙저장 • 장애 포인트 적고 배포 및 유지보수 편리 • 저사양의 Client PC 사용 가능	• 초기 높은 구축 비용 (서버 및 스토리지 구축) • ActiveX 호환성 높음 • 업무 VM / 인터넷 VM 간의 화면 전환
		[APP]	• **인터넷을 사용하기 위한 브라우저만 가상화** • 관리적 측면의 중앙 통제성 높음 • 자료 중앙저장 • 저사양의 Client PC 사용 가능	• 초기 구축 비용 (서버 구축) • ActiveX 호환성 (일부 사이트 문제)

5. 망 분리 개념도

KEY MESSAGE 망 분리 개념도



업무 망 이용 시

1. 업무망 접속 (그룹웨어, e-mail등..)
2. 사용자의 PC는 로컬 인터넷 브라우저로 접속

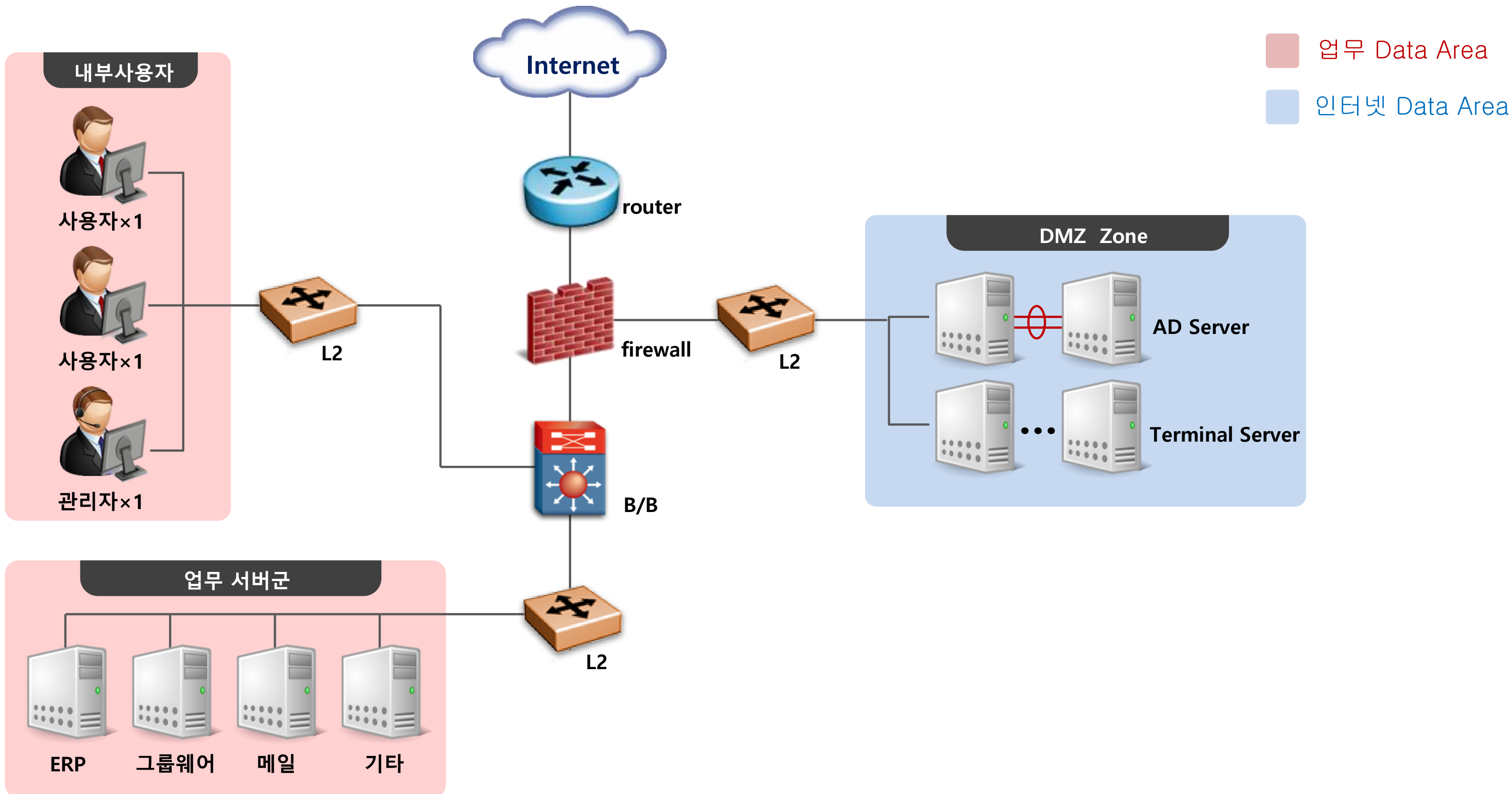
인터넷 망 이용 시

1. 인터넷 접속
2. 사용자 PC는 CockpIT Server farm 으로 접속
3. 서버에서 인터넷 브라우저가 실행
4. 사용자는 화면 값을 받아서 인터넷을 자유롭게 사용

6. 서버기반 가상화(외부망)

KEY MESSAGE 망 분리 시스템 구성도 – 인터넷 가상화

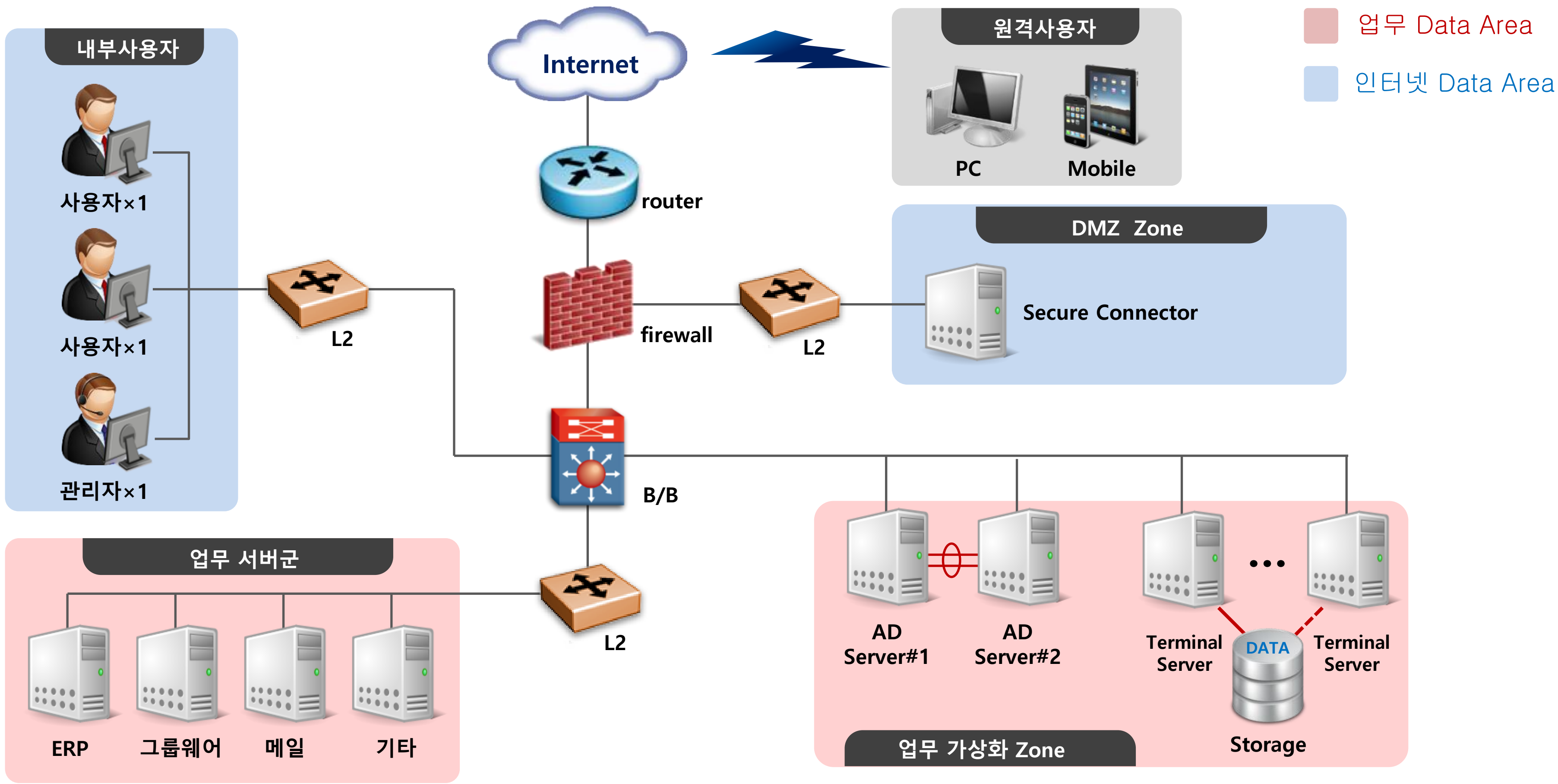
- 업무 망 영역은 내부 사용자의 로컬 PC로 이용하고 외부 인터넷 망은 DMZ에 Terminal Server를 이용하여 접속



7. 서버기반 가상화(업무망)

KEY MESSAGE 망 분리 시스템 구성도 – 업무 가상화

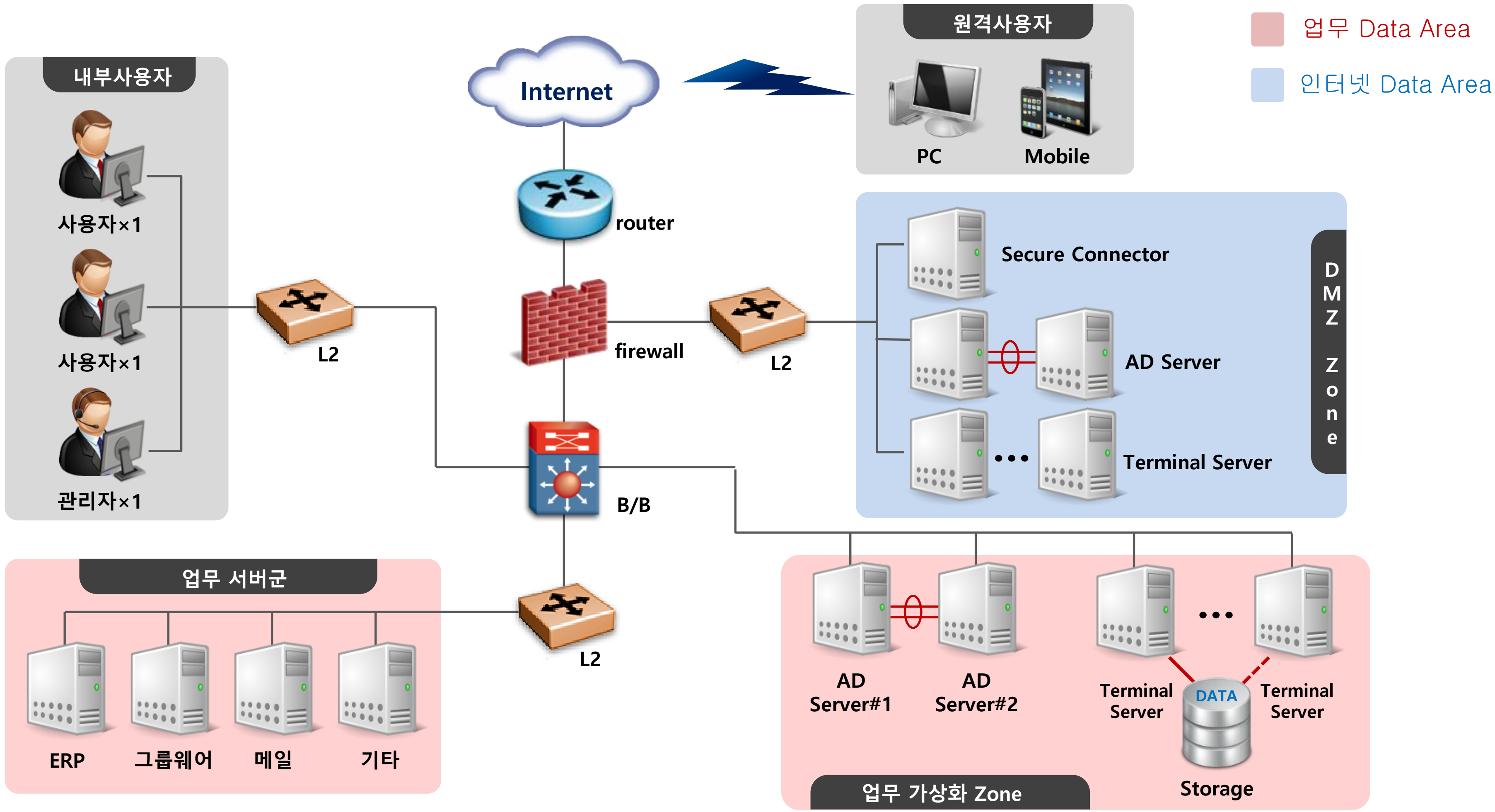
- 인터넷 망 영역은 내부 사용자의 로컬 PC로 이용하고 내부 업무 망은 업무 가상화 Zone에 Terminal Server를 이용하여 접속
- 외부에서 접속 시에는 DMZ Zone의 Secure Connector를 통해 접속



8. 서버기반 가상화(업무 및 외부망)

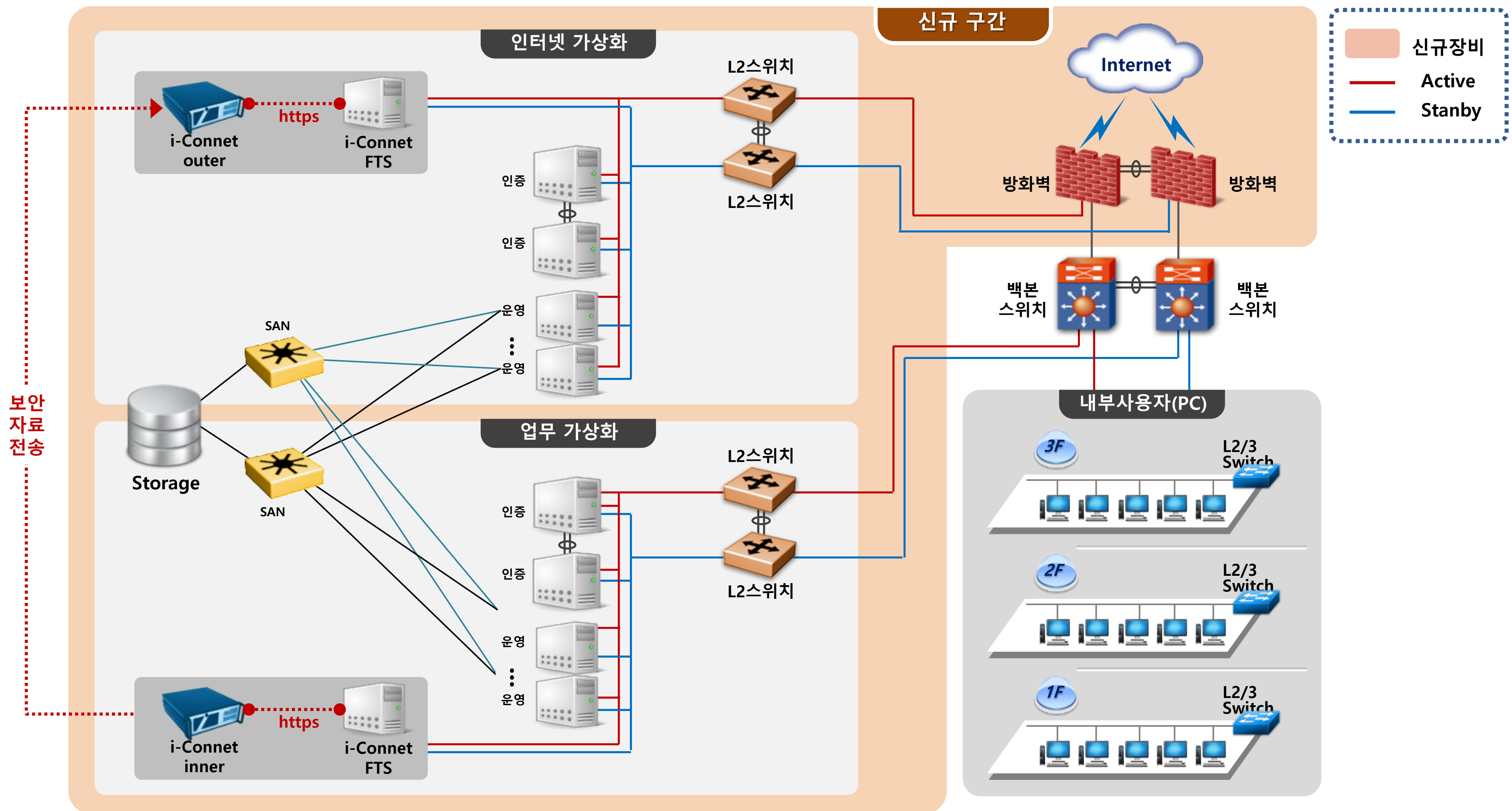
KEY MESSAGE 망 분리 시스템 구성도 – 업무 가상화 + 인터넷 가상화

- 업무 망 영역은 업무 가상화 Zone의 Terminal Server에 접속, 외부 인터넷 망은 DMZ Zone을 이용하여 Terminal Server에 접속
- 이로 인해 사용자 PC는 어떠한 업무 데이터도 존재할 수 없음



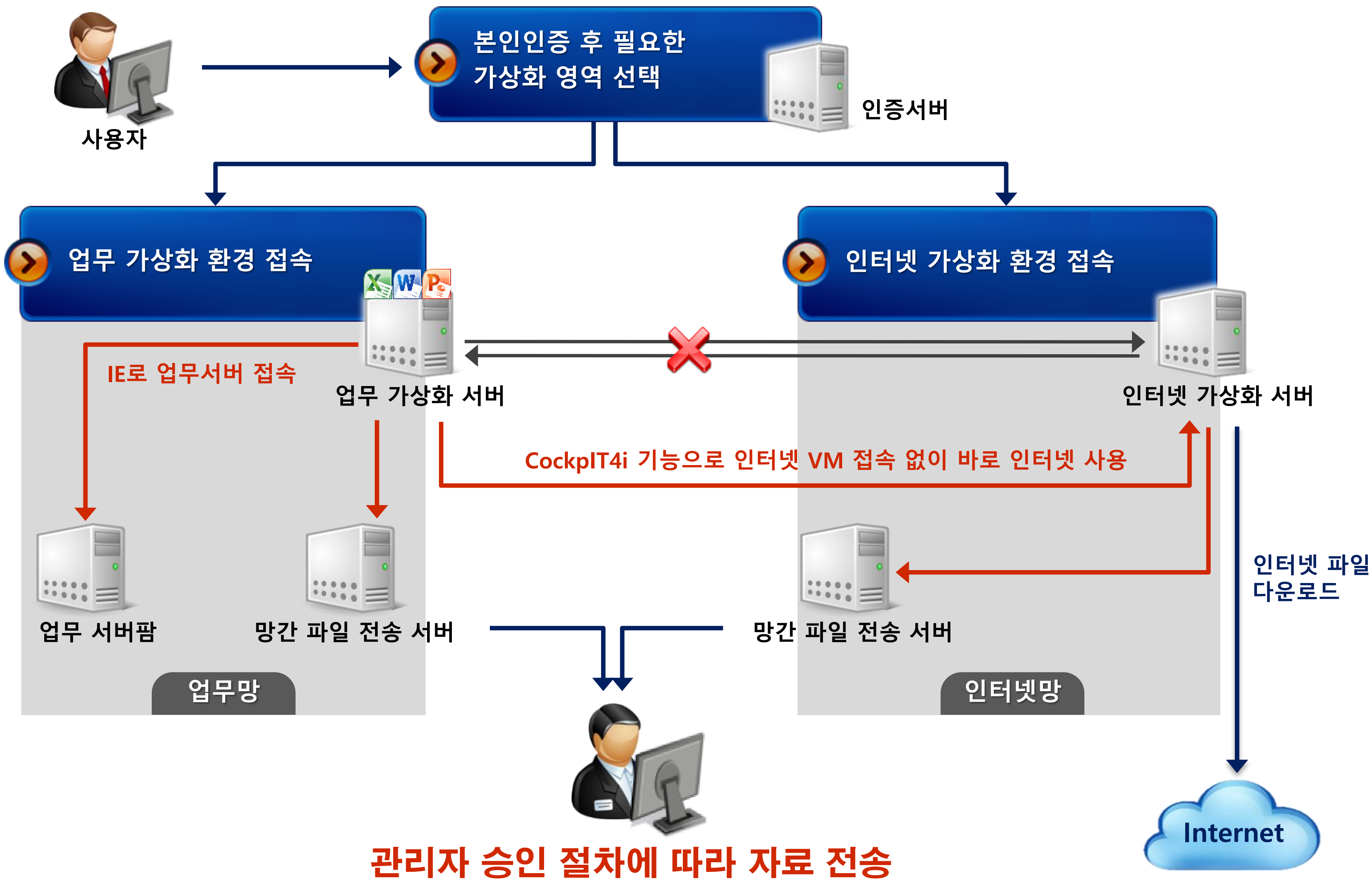
9. 상세 구성도

KEY MESSAGE 업무 가상화 + 인터넷 가상화 (상세 구성도)



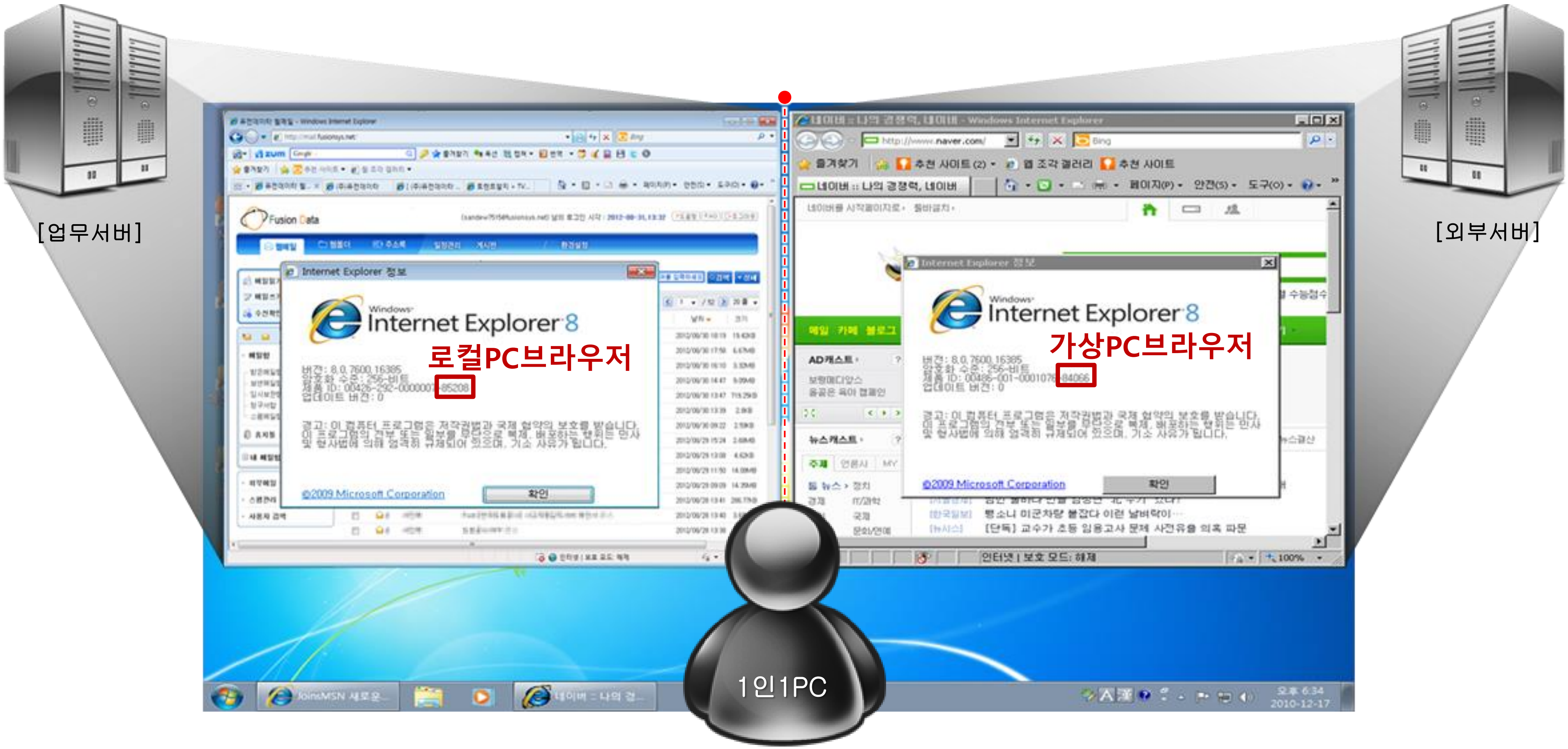
10. 프로세스 흐름도

KEY MESSAGE 업무 + 인터넷 가상화 프로세스 흐름도



11. 주요 특장점

KEY MESSAGE 구동화면



1인 1PC에서 내부 망과 외부 망을 분리하여 접속

11. 주요 특장점(계속)

KEY MESSAGE **자동 망전환**

자동 필터 링

explorer에서 대역을 인식하여 자동으로 망 전환
- 관리 툴에서 내부 망 대역을 설정 (White List 지정)
- 사용자가 주소 창에 IP혹은 도메인 명을 기입했을 때,
  White List에 등록된 대역 -> 내부 망 explorer로 접속 // 그 외 대역 -> 외부 망 explorer로 접속

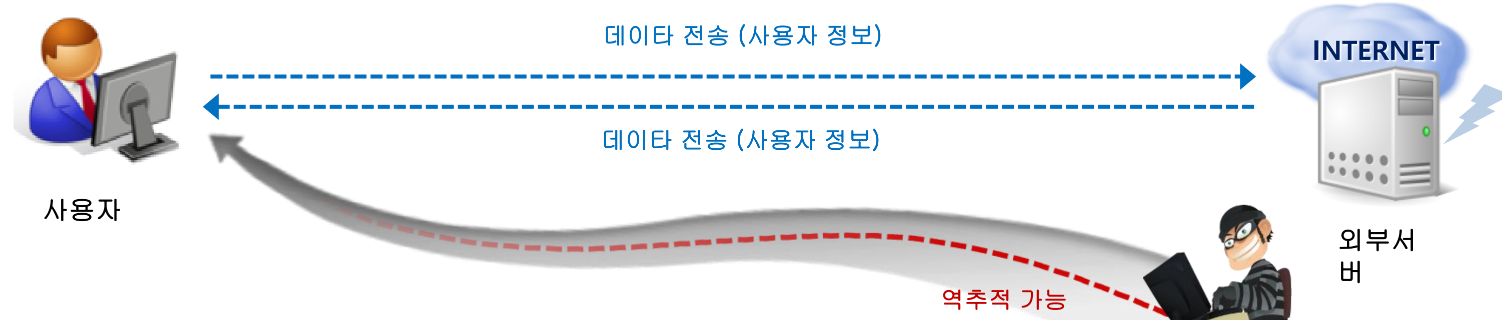
웹사이트 접속 시 자동 필터 링	
내부망 대역(White List)	외부망 대역(Black List)
(ex. 그룹웨어, ERP, E-mail, 사내 웹 하드 등.,)	(ex. 네이버, 다음 등 내부서버 외 모든 사이트)

- 내부망 explorer
- 외부망 explorer

11. 주요 특장점(계속)

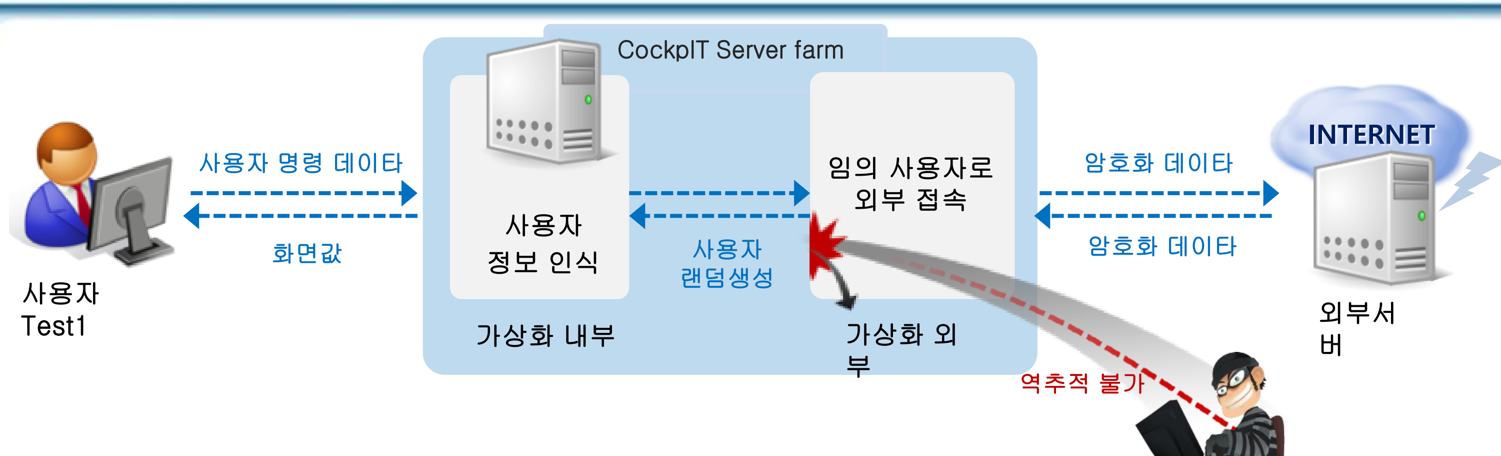
KEY MESSAGE 외부망 접속 시 사용자 정보 암호화

기존시스템



- 사용자 정보가 외부서버에 노출 되기 때문에 침입 가능성 높음

사용자 정보 암호화



- 내부 사용자의 정보가 서버에서 임의의 정보로 변경되기 때문에 외부로 노출 되지 않음

11. 주요 특장점(계속)

KEY MESSAGE **자동 배포**

망분리 솔루션 자동배포

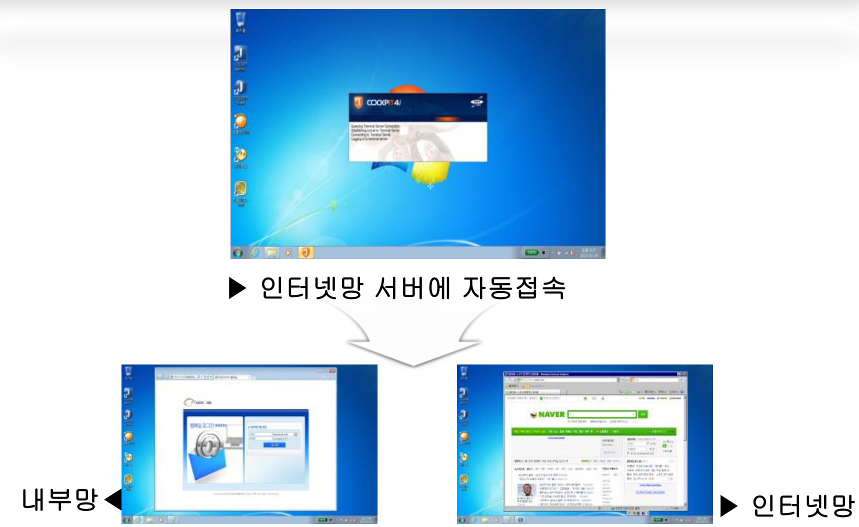
별도의 설치 없이 업무PC의 도메인 설정으로 *CockpIT i* 이용

- 업무PC의 도메인 설정
- 인터넷망 서버로부터 *CockpIT i* 를 사용자들에게 자동 배포
- 사용자 환경은 전혀 변하지 않음

기존 시스템

솔루션
자동배포

망분리 솔루션 자동배포



- 기존환경 그대로 사용

12. 우위 기술력

KEY MESSAGE **VDI/SBC를 사용한 성공적인 망 분리를 위해서는 아래의 문제를 해결할 기술력이 있어야 한다.**

망 분리 구축 핵심 현안		비고
가상환경에서 정상동작 하지 않는 프로그램의 수행 지원	• 문서 위변조 방지 프로그램, 가상화 프린터로의 출력을 지원 하지 않는 프로그램, 가상화 환경에서 화면 미리 보기 지원 하지 않는 프로그램 • 대법원 사이트,국세청, 한국 토지 정보 시스템, 민원24시, 대법원 인터넷 등기, 기타 금융권, 공공 기관 등 광범위하게 존재 • 일반 기업 내부 업무 시스템에서도 이와 같은 어플리케이션 다수 존재	▪ 업무 가상화 인터넷 가상화 모두에 필요 ▪ 다수 고객 요구 사항
두 개의 브라우저 사용 불편 제거 - 업무용, 인터넷 용 브라우저	• 업무용 브라우저는 로컬 PC 브라우저, 인터넷 브라우저는 가상화 브라우저 • 두 개를 동시에 사용해야 하는 불편함 해소 ➔ 망 자동 전환 기능	• 본사 특허 기술
사용자 로컬 프린터 기능 호환성	• 많은 환경에서 사용자 단말기에 직접 프린터를 연결해서 사용하는 환경 존재 ➔ 가상화 프린터 리다이렉션 기능의 제약 사항 존재 • 제어판에서 설정한 프린터 설정 정보가 로그 오프 하면 초기화 되는 문제 ➔ 현장에서 심각한 문제	• 전사 도입 단계에서 필수
멀티미디어 사용으로 인한 전체 대역폭 관리	• 전사적 가상화 도입에는 가상화 프로토콜로 인한 전체 망 트래픽 제어가 필수 • 멀티미디어로 인한 트랙픽에 의한 망 마비 상태 제어 가능해야함 • 멀티미디어의 화질보다, 망 트래픽 조절이 가능해야함.	• 전사 도입 단계에서 필수
USB 장치 리다이렉션	• 전사적 가상화 도입 환경에서는 각종 USB 장치들을 사용자 단말에 연결 가능해야 한다.	• 전사 도입 단계에서 필수
키보드 보안 프로그램 정상 지원	• RDP 및 일부 프로토콜에서 키보드 보안 프로그램 비정상 동작	• 전사 도입 단계에서 필수
하드웨어 성능 최적화를 위한 구축 기술	• 망 구성 및 스토리지 성능이 최적화되도록 구축 • 스토리지 성능이 사용자 체감 성능에 가장 중요한 변수 • 구축 경험을 통해서 많은 현장 데이타를 축적하는 것이 중요	• 전사 도입 단계에서 필수

KEY MESSAGE

주요 레퍼런스

병원/일반 고객사

다림 C&C · 무영종합건축사무소 · LG 텔레콤 · 세종병원 · 성애병원 · 원광대학교 산본병원 · 서울대학교 병원

동신병원 · 미디어 채널 · 수로텍 · 온세통신 · 리츠칼튼 호텔

금융권 고객사

동양시스템즈 · 동양증권 · 비씨카드 · 메리츠화재 · 금융결제원 · 기업은행 · 외환은행

국민은행 · 하나은행 · 미래에셋 · 부국증권 · AIG 손해보험 · KDB생명 · 그린손해보험

공공권 고객사

경기도청 · 국토연구원 · 한국토지공사 · 안산시청 · 한국국제협력단 · 헌법재판소 · 한국자산관리공사 · 국방기술품질원 · 방송통신위원회

안양시 · 국가기록원 · 대한지적공사 · 우정사업진흥회 · 한국통신사업자연합회

Thank you

Please contact : Garnet Information Technology

Call 051-925-1222
FAX 051-925-1223

www.garnetit.co.kr

영업문의(임정헌이사) : 010-6594-1272
이메일 : jhim@garnetit.co.kr

기술문의(윤성민팀장) : 010-6679-2479
이메일 : smyun@garnetit.co.kr