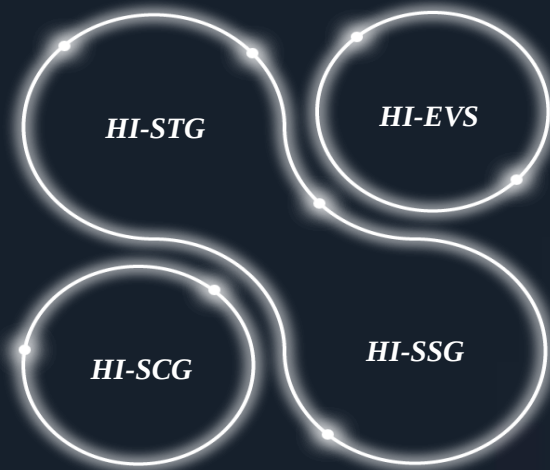


HI-Ware 4.0



RAMS(Remote Access Management System) 2011.10



- 1 제안 회사 소개
- 2 주요 사업 영역 및 고객 사 현황
- 3 주요 제품 소개 (HI-Ware)
- 4 제안 제품의 필요성
- 5 주요 구축 사례
- 6 대규모 고객 사 운영 방식 (*예제)

■ 제안사인 (주)넷앤드휴먼인터페이스는 2007년 창립 이래 2008년 법인전환을 통하여 신뢰성 및 기술력을 바탕으로 국내 접근통제 및 관리 시스템 분야에서 독보적인 행보를 거듭하고 있는 업체 입니다.

2008년 주요 공급 시스템인 HI-Ware 시리즈를 국내 최초로 Web2.0 flex 방식으로 정식 출시 하여 2011년 현재 60여 곳의 대형 고객사를 보유하고 있습니다. 또한 지속적인 R&D 투자로 인프라 접근통제 시스템 및 3D 통합 연동 상황시스템의 원천 기술을 확보 하였으며 이러한 창의적인 노력으로 매년 지속적인 성장을 거듭하는 인프라 운영관리 솔루션 전문 기업입니다.

■ 회사소개

구 분	세부 내역	주요 연혁
회사 명	(주)넷앤드휴먼인터페이스	2011.04 : HI-Ware 4.0 출시 2011.04 : 기술혁신 형 이노비즈 인증 2011.03 : GS인증 획득 2010.11 : KT TACS 시스템 구축 완료 2010.01 - 12 : 40여 고객사 확보 2010.03 : 벤처기업 인증 2010.02 : 정보기술 연구소 설립 2010.01 : 자본금 증자 2009.11 : HI-EVS 패키지 출시 2009.08 : HI-SCG 출시 2009.04 : HI-SSG 출시 2009.01 - 12 : 20여 고객사 확보 2008.02 : 여의도로 본사 이전 2007.12 : 법인전환 2007.06 : HI-STG 1.0 버전출시 2007.02 : 회사 설립
대표 자	신 호 철	
사업 분야	소프트웨어 개발, 장비 접근통제 시스템 공급, 네트워크 관리 시스템 공급	
주 소	서울시 영등포구 여의도동 44-2번지 태양빌딩 802호	
연락처	02) 2661-1410 FAX 02) 2661-1420 http://www.netand.co.kr	
설립 연도	2007/02/28	
자본 금	1억 원	
인력 / 수상	25명 / 정보기술연구소 보유 / 벤처기업인증 / 이노비즈인증 / GS인증	
사업자 등록 번호	109-86-11375	

주요 사업 영역 및 고객 사 현황

■ ㈜넷앤드휴먼인터페이스는 최상의 기술력과 다양한 구축 경험을 통하여 고객사의 인프라가 중단 없이 서비스를 유지 할 수 있도록 다양한 접근통제, 인증, 감사, 통합관리 시스템을 제공합니다. HI-Ware로 제공되는 모든 솔루션은 기존 서비스에 영향 없이 즉시 사용이 가능한 Gateway 구조로 설계되었으며 이러한 구성으로 보다 편리하고 신뢰성 있는 인프라 운영 환경을 제공합니다.

주요 공급 제품

HI-Ware 4.0

- STG : 네트워크 및 서버의 접근통제 및 보안감사 시스템
- SSG : 윈도우 원격접속 터미널 통제 및 보안감사 시스템
- SCG : Serial Console 접근 제어 및 감사, 전원제어 시스템
- SGS : Application의 Gateway Proxy 형식의 접근통제 시스템
- SWG : Web Service 작업내역의 역 추적 및 보안감사 시스템
- EVS : Web 2.0의 다중 Point System 통합관리 시스템
- TIM : 이 기종 서버 계정관리 및 패스워드 자동화 시스템
- NAMS : 3D 형식의 네트워크 통합관리 시스템

수상 및 인증 현황

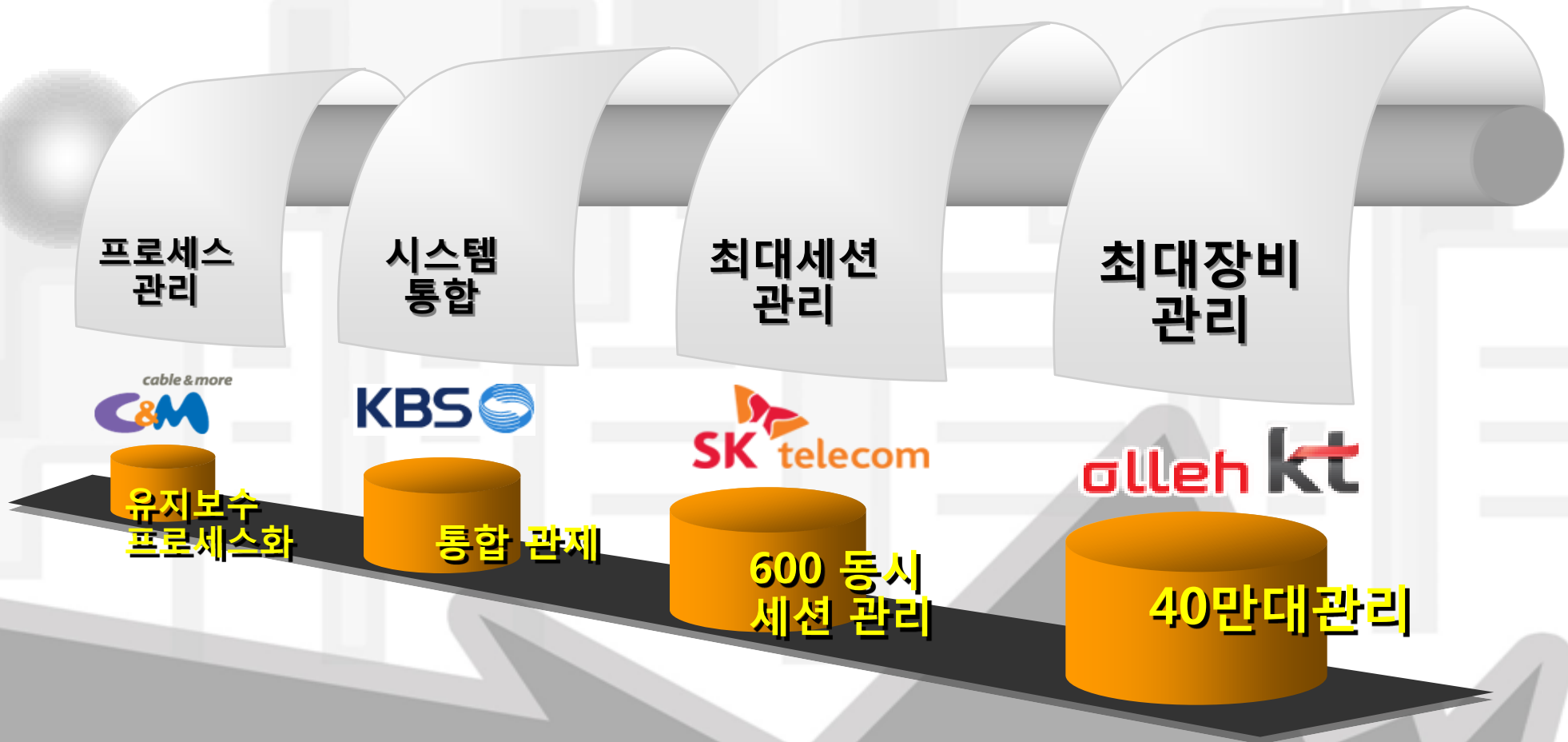


주요 고객 사

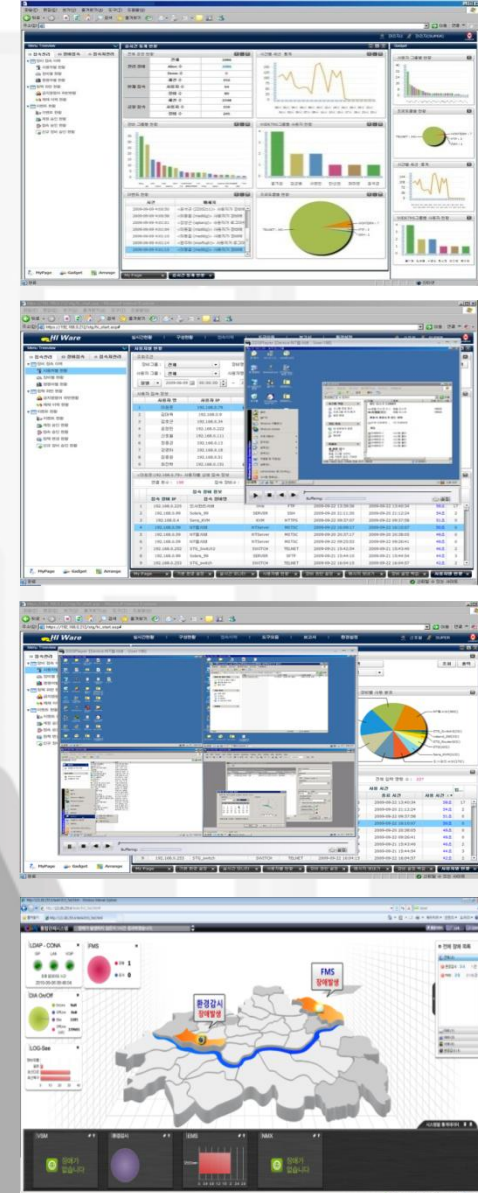
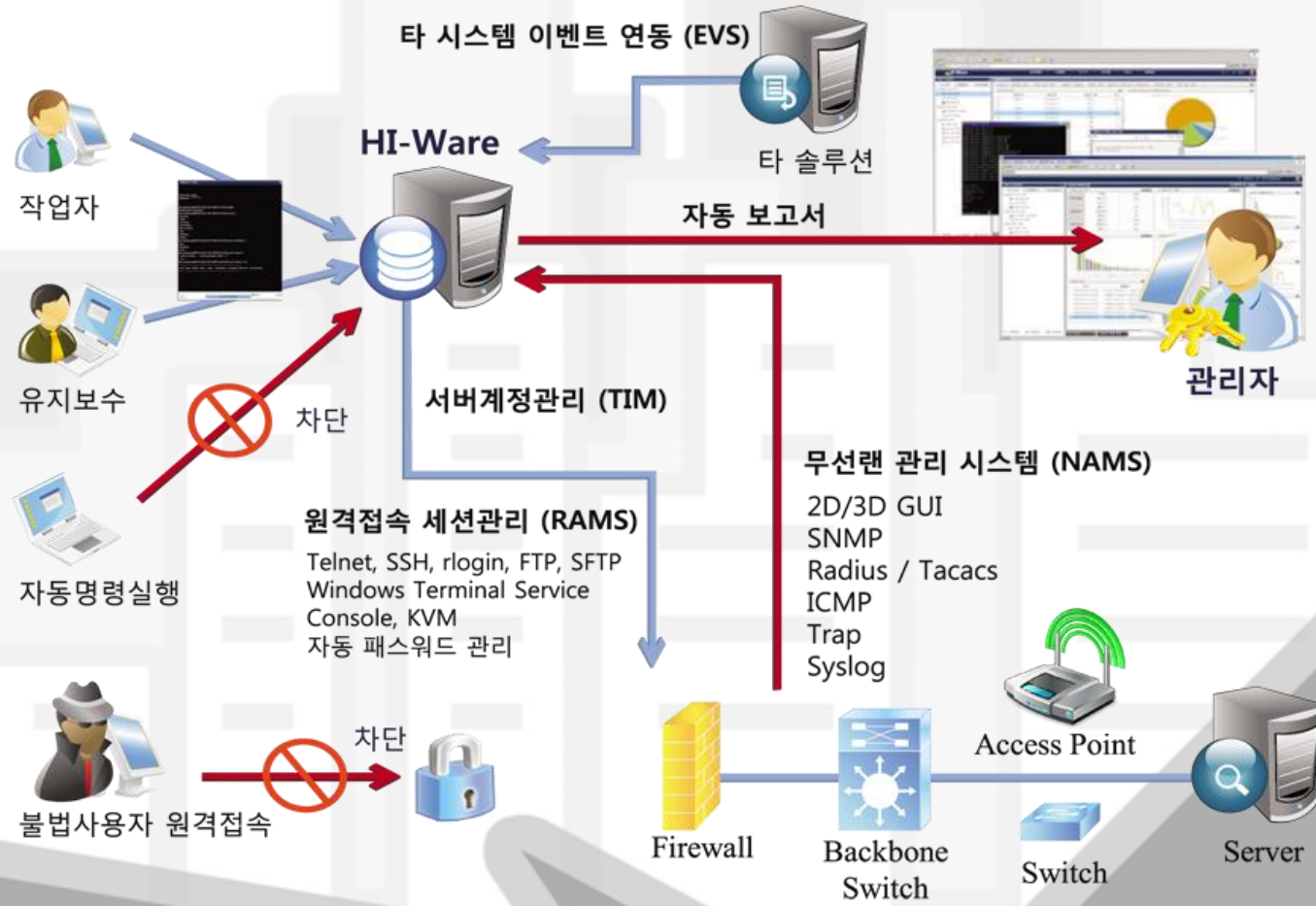


HI-Ware의 모든 시스템은 최대 사용량에 검증된 시스템 입니다.

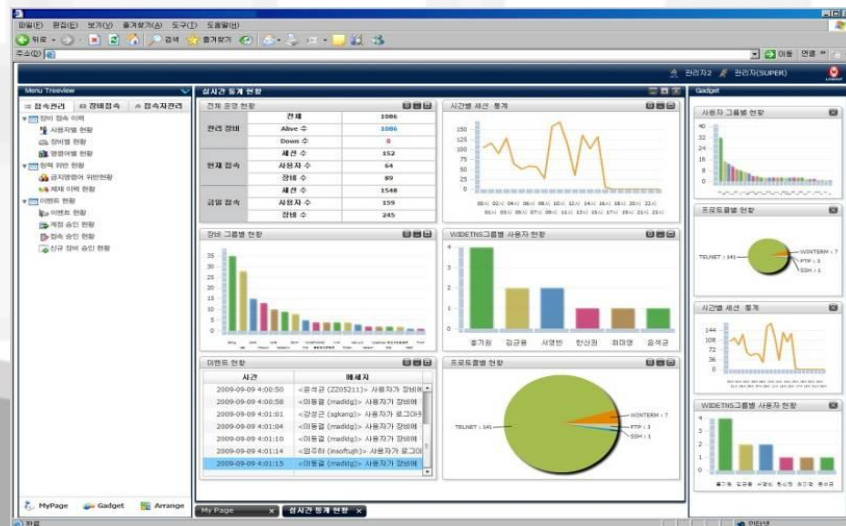
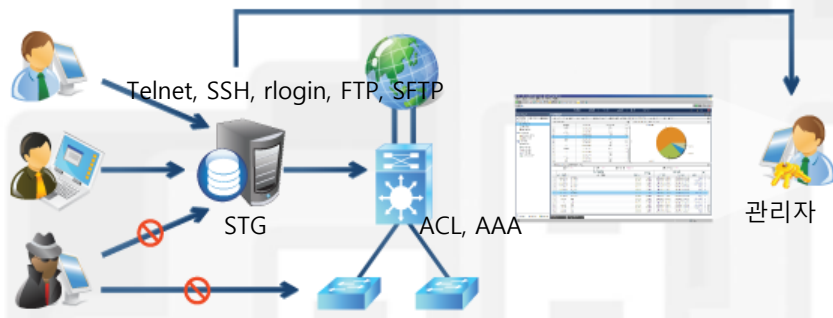
- HI-Ware 의 가장 큰 성능적 핵심은 사용자 계정의 관리, 로그저장, 로그조회, 동시접속 세션, 장비의 수 입니다.
- HI-Ware 제품 군은 이 모든 사항을 고객사에서 이미 검증하여 최대 효율성을 제공하고 있는 안정적인 제품입니다.



HI-Ware 제품 구성도



■ 자사의 대표적인 솔루션으로 네트워크 및 서버 등의 인프라 운영시스템의 원격 접속 시 CLI (Telnet, SSH, FTP, SFTP, rLogin)등의 접속을 제어 및 관리하고 다양한 계정 연동 정책을 통해 접속에 대한 정책을 구현할 수 있는 시스템 입니다. STG는 강력한 보안감사 기능 및 자동화 기능을 제공하며, 패스워드의 자동변경 및 장애 발생 시 사후 추적이 매우 용이한 차세대 원격접속 관리 시스템 입니다.

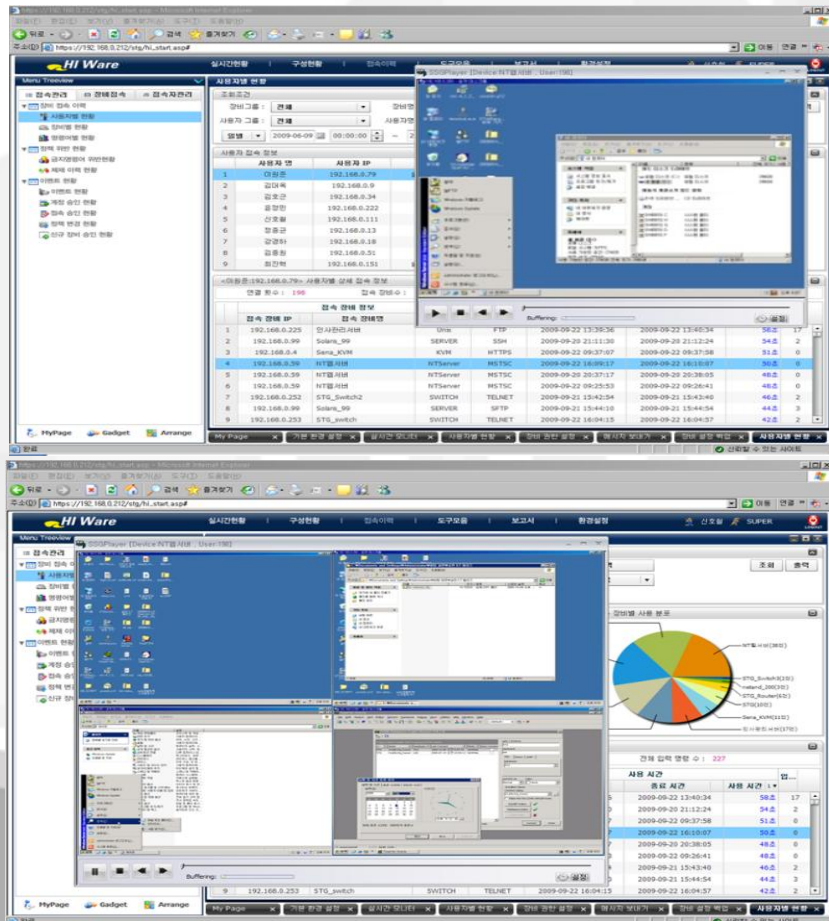


원격접속 내역 감사 및 자동화 시스템 구현

• 기능 요약 (Secure Terminal Guard)

- Web2.0 Flex 기반의 Web UI와 Https 보안 접속 기능 제공
- 서버 시스템 및 네트워크 시스템의 완벽한 호환성 제공
- CLI (Command Line Interface)로 구동되는 모든 벤더의 모든 장비 지원
- 세션의 접속 허가 및 요청/승인 프로세스 제공
- 사용자 별, 장비 별, 명령어 별로 접속 사용자의 작업 로그를 저장 조회
- 조회 필터를 통하여 기간별, 그룹별, 조회 기능 제공
- 관리자의 PC에서 실시간 작업 내역을 모니터링 할 수 있는 기능 제공
- 금지 명령어에 의해 위반 시 통보 및 자동 세션 제어 기능 제공
- 적용된 명령어의 초 단위 로그 관리 기능 제공
- 적용된 전체 작업 로그의 재생 기능 제공
- Web에 의해 적용된 Web 조회 및 관리자 Emulator에서 기능 조회
- 관리자 이벤트 메시지에 작업자 로그인 시 알람 기능 제공
- 정책에 의한 재 접속 방지 방지 정책 구현
- 다양한 보고서 기능 제공

Windows Terminal Service에 접속 시 사용되는 mstsc /(option)의 접속 경로를 일원화 하여 접속 내역에 대한 작업 로그를 동영상 형식으로 저장하여 장애 발생 시 재생이 용이하도록 하는 차세대 터미널 감사 시스템 입니다. 이러한 GUI 형식의 접근은 IP, Mac, 계정권한, 장비권한, 시간 등의 다양한 정책을 통하여 관리되며 모든 작업내역은 실시간 저장 및 관리 됩니다.



GUI 형식의 시스템 보안감사

• 기능 요약 (Secure Snapshot Guard)

- Web2.0 Flex 기반의 Web UI와 Hhttps 보안 접속 기능 제공
- 서버 시스템 및 네트워크 시스템의 완벽한 호환성 제공
- 세션의 접속 허가 및 요청/승인 프로세스 제공
- Windows Terminal Service의 자동 로그인 기능 제공 (패스워드 보호정책)
- 조회 필터를 통하여 기간별, 그룹별, 조회 기능 제공
- 관리자의 PC에서 실시간 작업 내역을 모니터링 할 수 있는 기능 제공
- 공지 사항 및 인증 접속 프로세스 제공
- 다양한 재생(화면분할) 및 스냅샷 저장기능 제공
- 재생 프레임 퀄리티 조정 가능
- 빨리 보기 (X2, X4 ...) 기능 및 버퍼링 기능 제공
- 다양한 보고서 플랫폼 제공
- HI-STG의 모든 편이 기능 제공

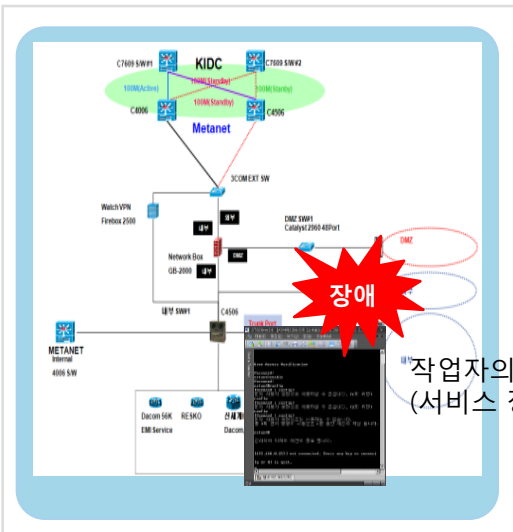
가정 #1 - 원인을 알 수 없는 장애로 서비스의 문제가 발생할 수 있는 구조.

- 운영 망 중 KIDC의 서비스에서 장애가 발생
- 서비스 장애 시간은 30분 발생
- 서비스의 장애로 장애 비용 및 대 고객 신뢰도에 문제 발생

- 유지보수 운영 팀에서는 DDos의 공격에 의한 일시적인 트래픽 폭주 현상으로 장애보고
- IPS, IDS 등의 업그레이드와 보안 제품이 신규 투자 보고

- Cisco에서는 2006년 이러한 장애의 65% 이상은 작업자의 명령어 Script 오류에 의한 장애로 보고됨
- 관리자는 어떠한 이력정보도 없기 때문에 보고서에 100%의존
- Script에 의한 시스템 장애였다면 신속한 장애 복구 및 명확한 책임소재가 이루어져야 중복 투자의 위험성도 제거 될 수 있음

A유지보수



원인 규명 요청

장비 노후 및 DDos에 의한 장애 보고

- 추가 장비 구매요청
- 보안 대비책 제안

작업자의 실수
(서비스 장애 발생)

예산 손실



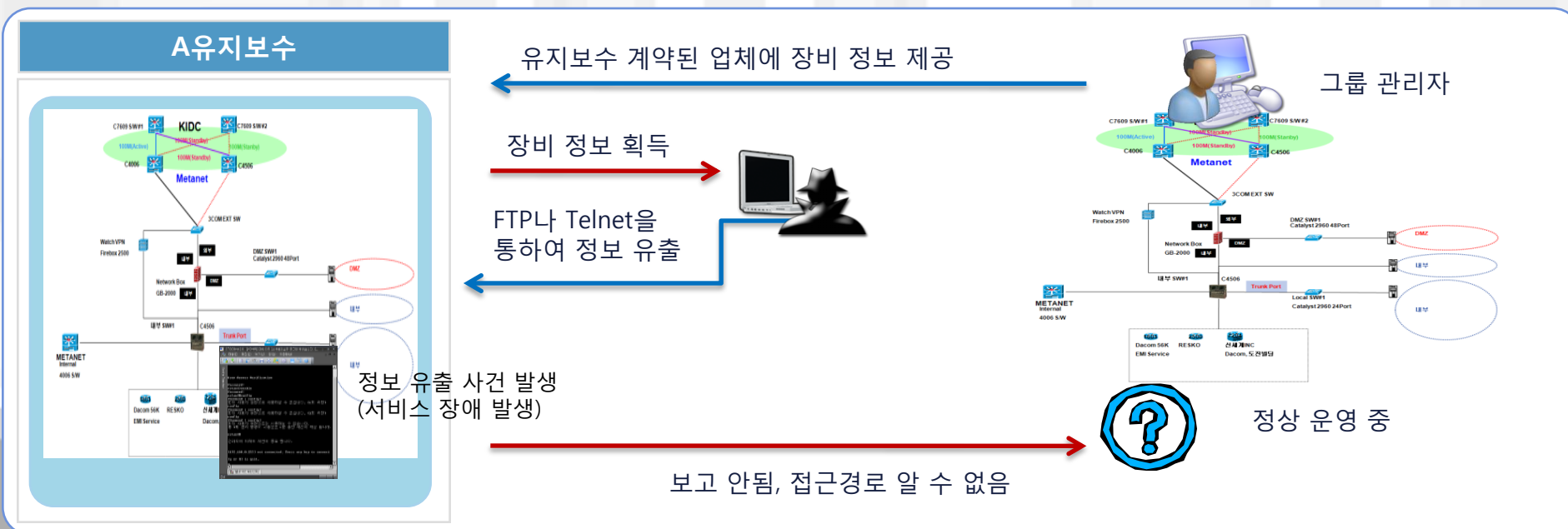
그룹 관리자



- 근거에 의한 집행 어려움
- 적용 히스토리 관리 부족

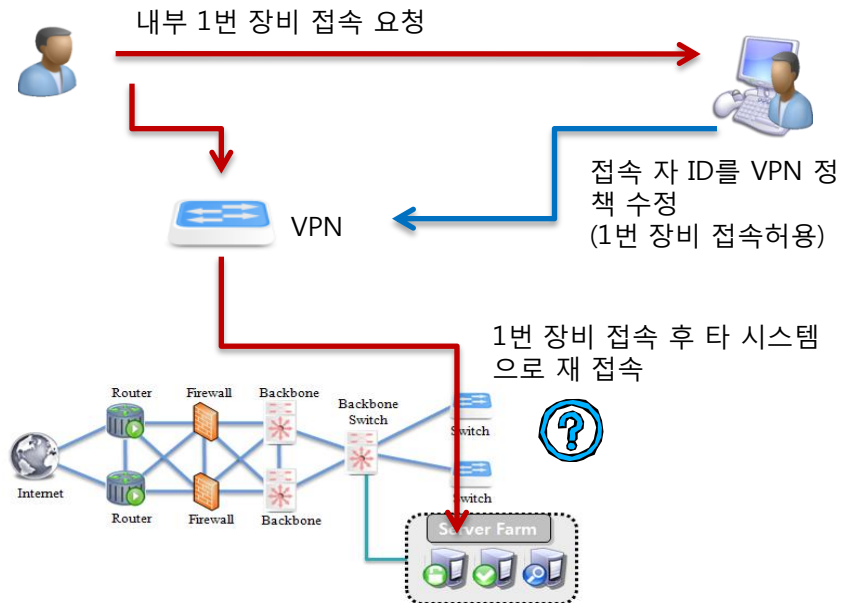
가정 #2 - 1차 적인 내부 정보가 유출되는 경우의 구조.

- 개별 유지보수 업체에 모든 사용 정보를 통보하고 유지보수 작업을 진행할 수 밖에 없는 구조임
- 관리자는 유지보수 업체에게 장비의 ID/Password를 통보할 수 밖에 없음
- 모든 보안 성을 유지하였던 제안사의 고객사인 (G정유그룹)은 원초적인 ID/Password의 유출을 통하여 정보가 유출
- 정보보호진흥원은 보안사고 통계치의 90%이상이 ID/Password에 의한 내부 접근자의 유출이라고 보고됨
- ID/Password를 보호 하였다면 이러한 문제로부터 관리자는 해방될 수 있으며 중앙 집중 식으로 관리가 가능

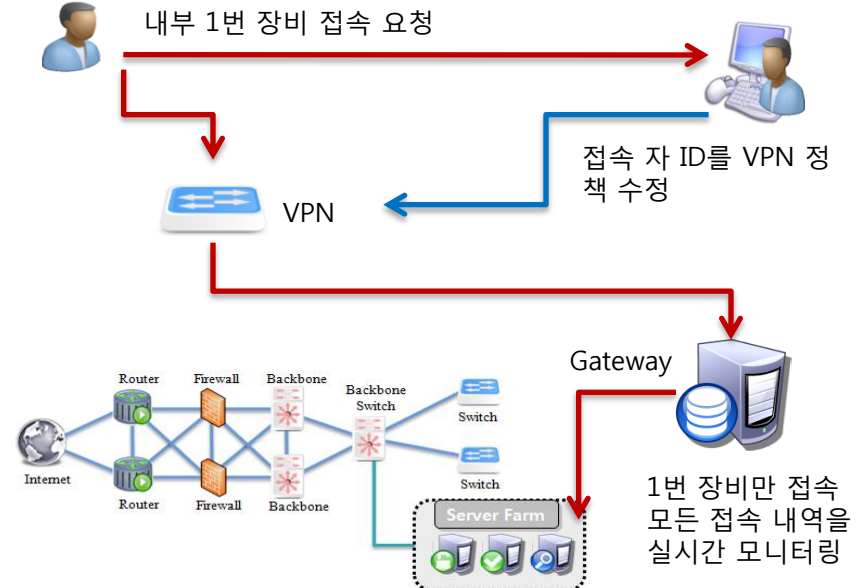


■ 대규모의 망을 운영중인 금융기관(A공공)에서는 SSL VPN을 통하여 내부 운영 서버 접속 시 해당 관리자가 VPN에 접속할 계정을 생성하여 접속할 대상 서버 IP를 개별 적으로 등록하여야 했습니다. 이러한 망 접속 구조는 해당 서버의 권한으로 접속한 사용자가 타 서버로의 재 접속을 하면서 발생 하는 운영적, 보안적 이슈 사항에 대한 대비책을 전혀 갖추지 못하고 있는 구조로 운영되고 있었습니다.

적용 전 운영 사례

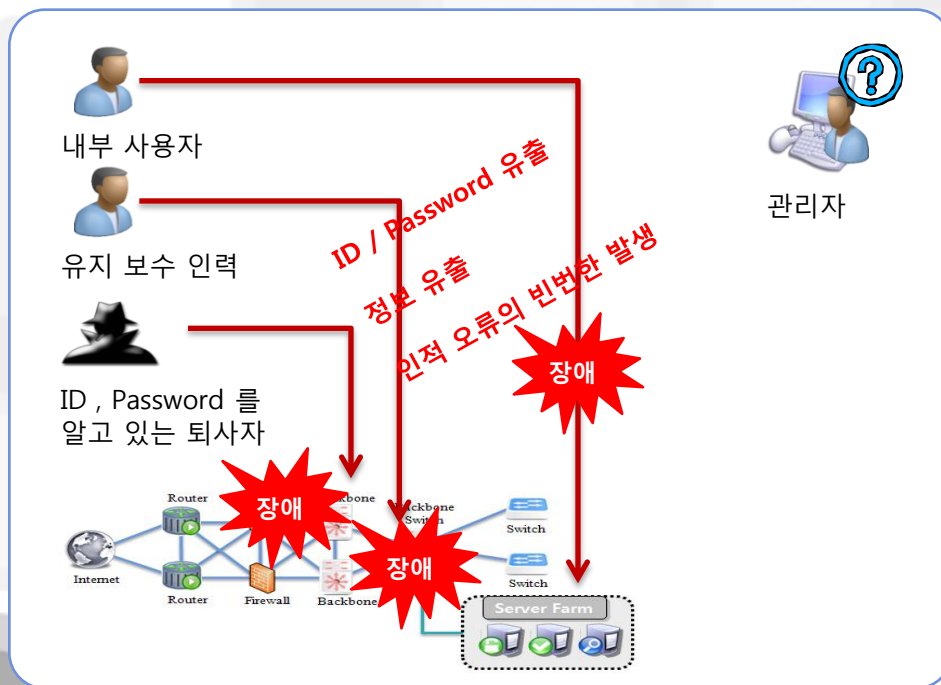


적용 후 개선 사례

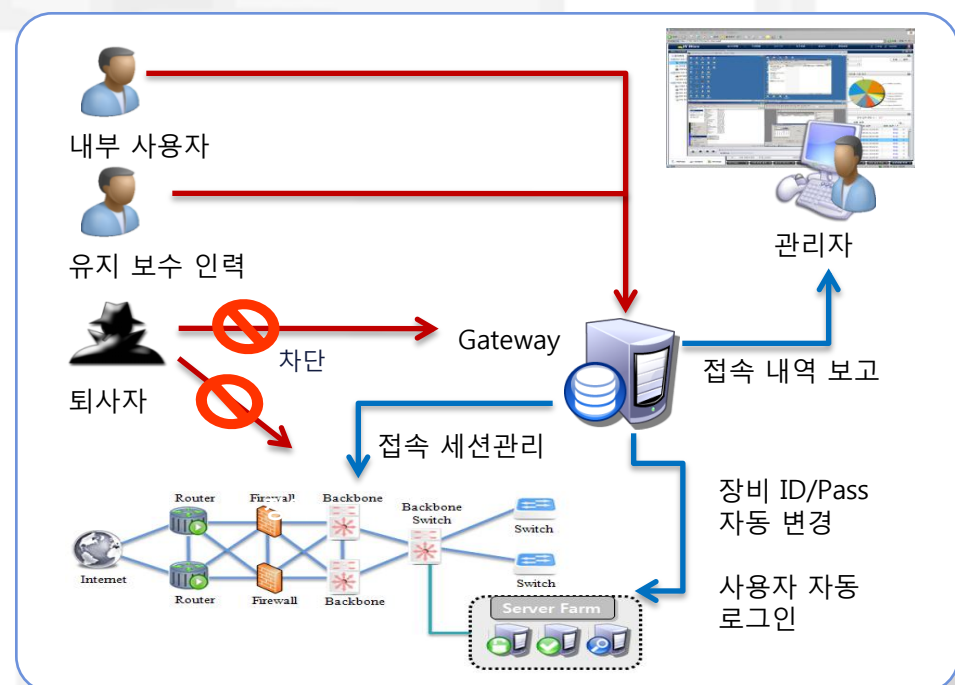


■ 국내 최대의 인프라를 보유하고 있는 K통신사는 지역별로 산재한 장비에 대하여 접속 권한을 지역 유지보수 업체와 공유하고 있었습니다. 따라서 지역 업체의 변경 및 사용자 변경 시에 미 인가 작업자의 접속을 통제 할 수 있는 방안이 전무한 상태였습니다. 이는 K통신사 인프라에 누구나 접속이 가능하다는 중요한 이슈이기도 하였습니다.

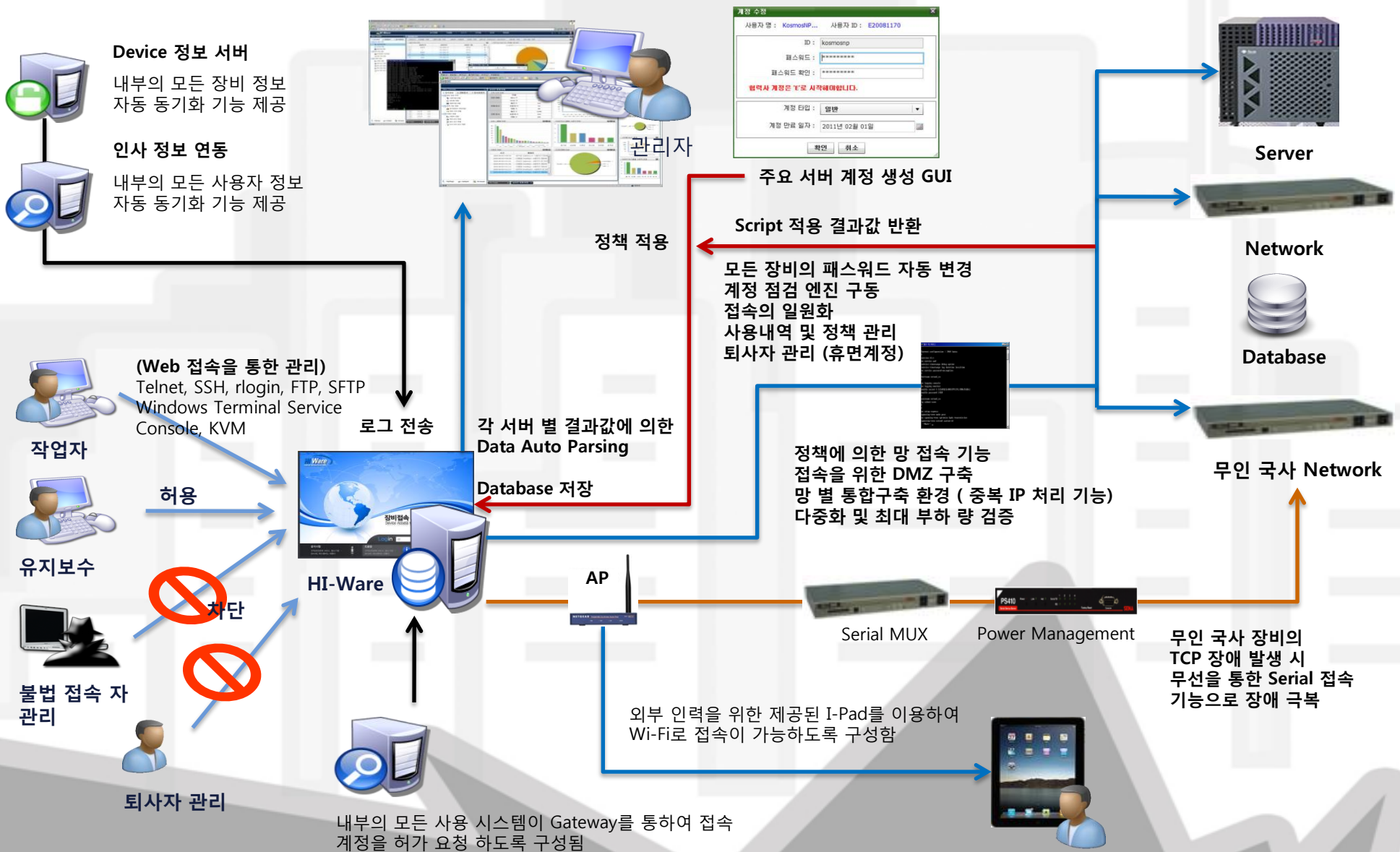
적용 전 운영 사례



적용 후 개선 사례



고객 사 네트워크 및 서버 운영 방식 예제



감사합니다

최적의 제품을 최선을 다해 보답하겠습니다

<http://www.netand.co.kr>



솔루션사업본부 / 과장

이 원 준

(주)넷앤드 휴먼인터페이스

E-mail : lwj216@netand.co.kr

H . P : 010-6267-5115

150-890 서울시 영등포구 여의도동 44-2 태양빌딩 802호

TEL : 02-2661-1410 FAX : 02-2661-1420

NMS / TMS / RTMS / STG - 최상의 관리시스템 및 작업인증 솔루션

<http://www.netand.co.kr>



솔루션사업본부 / 과장

이 병 강

(주)넷앤드 휴먼인터페이스

E-mail : bkleee@netand.co.kr

H . P : 011-9013-9121

150-890 서울시 영등포구 여의도동 44-2 태양빌딩 802호

TEL : 02-2661-1410 FAX : 02-2661-1420

HI-Ware(STG,SCG,SSG,EVS) Soutlution