HP 보안 감사 솔루션(Gate One)

Date: Sep. 19 (Wed.)

황완식/차장
한국HP TS/IS

HP Solution World 2007

IT transformation to BT

목 차

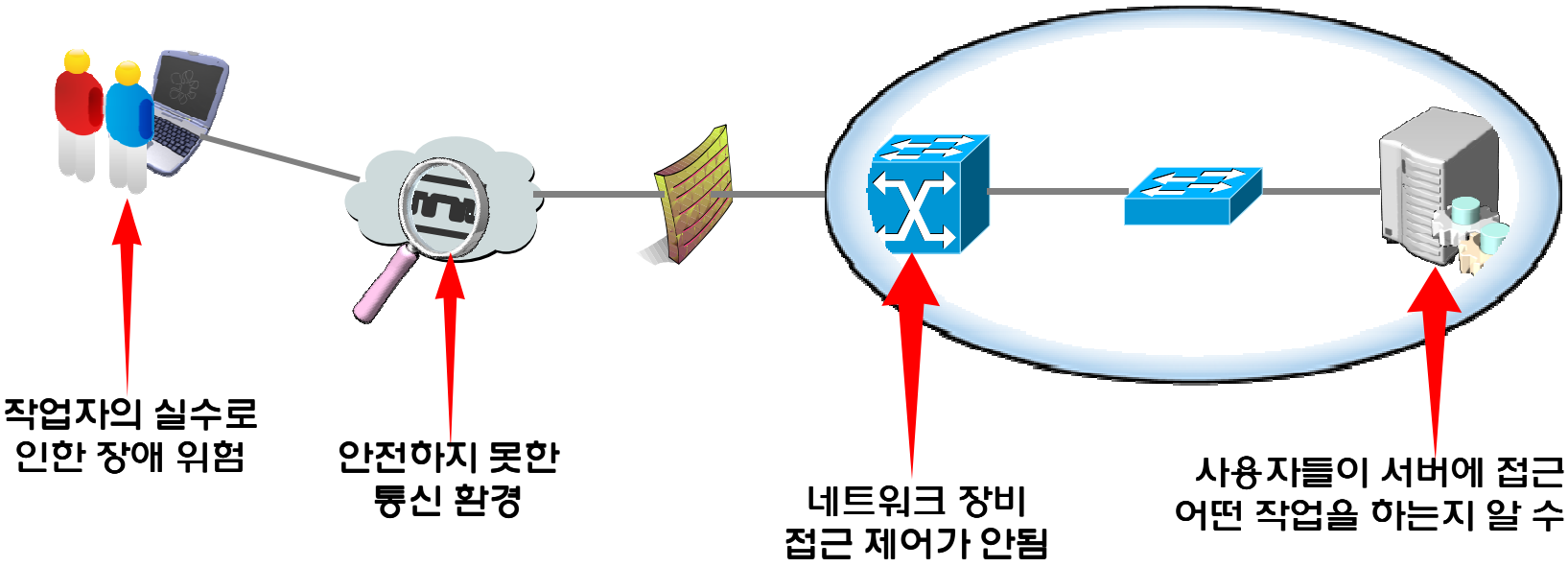
개 요

HP 보안 감사 솔루션은 Shell (TELNET, FTP, SSH, SFTP)에 대한 접근제어 및 감사 기능을 제공 합니다.

솔루션 등장 배경

문제점 인식

- Human error 대비책 부재
- 인증 받은 사용자의 작업 이력 관리 부재
  (보안감사 추적 및 이력 관리 어려움) ➔ 작업내용 보안감사 로그 필요성 증대
- 장애발생시 Fast Recovery 위한 로그 추적 기능 필요성 발생
- 기업 내부의 중요정보, 고객정보 유출에 따른 막대한 경제적 손실 및 기업 경쟁력 약화 등을 원천 차단하기 위한 시스템의 필요성 등장



솔루션 등장 배경(내부보안사고)

내부 보안사고 이슈

발췌 : 한국정보보진흥원 정보보호뉴스 2007년6월호

- 내부자 공격으로 인한 피해 정도는 외부 사용자에 비해 8배 이상 심각.
- 미국 내 한 금융 분야에서 내부자에 의한 사기 사건이 발생, 그로 인해 7억 달러의 손실 발생.
- 내부 엔지니어에 의해 작성된 논리 폭탄으로 인해 1,000만 달러의 손실과 약 80여명의 근로자들이 해고 됨.

내부 보안 사고 비율

발췌 : CERT, CSO 매거진, Secret Service의 'eCrime Watch Survey

- 미국 내 기업에서 발생하는 정보보호 관련 사고 중 전체 온라인 범죄 68%가 내부 소행 이며 나머지 32%는 외부 사용자에 의해 발생.
- 일본 내 기업에서의 내부 보안사고 비율은 60% 이며 국내 기업의 경우는 82%정도가 내부 보안사고 비율 임.

내부 보안사고 경로

- 서버에 접근 허가 받은 사용자들의 telnet, ftp와 같은 shell을 이용한 직접 자료 유출.
- telnet, ftp 처럼 보안이 취약한 프로그램의 약점을 이용해 내부의 다른 사용자가 해킹 시도.
- 네트워크 장비 경우 처럼 작업 내용을 알 수 없는 약점을 이용한 장비 Shut down 이나 인증 받은 내부사용자가 서버에 논리 폭탄 등을 이용한 서비스 다운 등.

솔루션 등장 배경

LG파워콤, 시스템 접근 차단 및 교육 강화

[입력날짜: 2007-04-23] 발췌 -보안뉴스-

가입자 정보보호 강화... LG파워콤

얼마전 법원은 국민은행의 인터넷복권 가입자 3만여 명 개인정보 유출 사건에 대해 집단소송을 제기한 피해자들에게 10만원의 위자료를 지급하라는 판결을 내린 바 있다. 또한 고객의 정보가 유출되면 기업에도 상당한 이미지 손실이 발생하기 때문에 기업들이 개인정보유출을 막기 위해 다양한 노력을 기울이고 있다. 특히 통신사업자들은 엄청난 고객정보를 보유하고 있는 관계로 이 부분에 신경을 쓰지 않을 수 없는 상황이다. 여기서는 각 통신사별로 어떠한 고객정보 보호 시스템을 구축하고 있는지 자세히 알아보도록 하겠다.

LG파워콤은 개인정보 보호를 위해 관련 조직을 구성해 운영하고, 정보보호 교육을 실시하고 있으며, 시스템 접속 현황에 대해 실시간 모니터링을 수행하여 시스템 접근에 대한 관리를 엄격하게 통제하는 등의 활동을 실시하고 있다.

입사시 고객정보보호, 시설보안, 시스템 보안의 내용이 포함된 보안각서를 작성하도록 하고 있으며, 직무와 직급에 따라 내부 전산망 접근권에 엄격한 차등을 두고 있다.

관리적 조치 외에도 LG파워콤은 시스템에 대한 접근 관리를 강화하는 등 기술적 조치들도 병행하여 시행하고 있다.

내부자에 의한 정보유출 차단효과 및 정확한 사후조사가 가능하도록 하고 있으며, 고객정보의 집중 다운로딩 발생에 대한 모니터링 기능을 개발하여 정보유출관련 모니터링 체계를 구축했다.

최근에는 기존 시스템의 미비점을 보완하여 새롭게 내부 전산시스템을 정비하면서 로그인 인정절차를 대폭 강화하여 허가되지 않은 직원의 시스템 접근을 차단했으며, 해킹 등 외부 접근이 불가능하도록 시스템 보안기능을 더욱 강화했다.

LG파워콤 관계자는 "향후에는 개인정보보호 교육을 확대, 강화해 나가는 관리적 보호조치 강화와 함께 기술적 미비점을 지속으로 보완해 나가면서 시스템 접근권 강화와 같은 기술적 보호조치를 더욱더 강화해 나갈 것"이라며 "특히 개인정보DB 접근통제 강화, 개인정보보호 교육 등을 통해 대리점과 같은 사외업체에 대한 관리를 강화해 나갈 계획"이라고 밝혔다.

WiBRO 해외유출 일당 검거

[입력날짜: 2007-05-21] 발췌 –디지털타임스-

15조원대 핵심기술 미국 통신사에 판매시도 / 검찰, 포스 데이타 전 · 현직 연구원 4명 구속

우리나라가 세계 최초로 개발한 차세대 휴대인터넷 와이브로(WiBro)의 핵심기술을 해외로 유출하려던 일당이 붙잡혔다.

이 회사 전직 연구원인 정씨는 지난해 10월 회사의 와이브로 기술메모(TM)와 디자인 문서(DD), 성능평가자료(PD) 등을 외장 하드디스크에 담아 회사 밖으로 유출했다. 공모자 박씨와 이씨도 각각 이 회사의 기지국 채널카드 MAC 소스프로그램을 외장 하드디스크에 담아 인쿼드론의 국내 연락사무소에 제공하거나 와이브로 장비 세부기술 디자인 설계문서 등을 개인 이메일로 유출한 혐의를 받고 있다.

이들이 빼돌리려던 문서는 와이브로 인프라인 기지국(RAS)와 기지국 제어기(ACR), 단말장치(PSS), 망관리장치(EMS) 등 와이브로 핵심 기술 전반에 걸쳐 있다.

포스데이타는 "금년 초부터 퇴직 직원들의 기술유출 시도를 포착해 전문업체를 고용해 증거를 확보했으며, 해당업체인 인쿼드론을 상대로 미국 캘리포니아 주법원에 민사소송을 제기하는 한편 형사고소도 추가할 예정"이라고 밝혔다. 포스데이타는 또 이번 기술 유출 시도로 인한 회사측의 피해는 미미하며 진행중인 연구개발에도 큰 차질이 없을 것이라고 덧붙였다.

하지만 당국에 따르면 포스데이타측이 중요 기술에 대한 열람제한이나 통제 등 초보적인 보안관리가 허술해 사건 연루자들이 핵심기술 자료를 손쉽게 공유하는 등 사건의 빌미를 제공했다는 지적이다.

보안 감사 솔루션의 필요성

많은 기업들이 안정적인 시스템 운영과 정보유출 차단에 집중

hp invent

최선의 해결책은?

Real-time Audit trail & Monitoring & Backup & Recovery

- Practice 1 : 전사적 차원의 주기적인 위험평가 수립
- Practice 2 : 모든 직원들을 대상으로 한 주기적인 보안수준 제고 교육
- Practice 3 : 의무와 최소한의 특권 구분
- Practice 4 : 엄격한 패스워드와 계정관리 관리 정책 이행
- ⇨ **PRACTICE 5 : 내부 직원의 온라인 활동에 대한 로그, 모니터링, 그리고 감사**
- ⇨ **PRACTICE 6 : 시스템 관리자와 특수한 사용자에 대한 이중의 경보 시스템 적용**
- Practice 7 : 악의적인 코드에 대한 적극적인 대처
- Practice 8 : 원격 공격에 대비한 다층 방어(Layered Defense)
- ⇨ **PRACTICE 9 : 의심스러운 행위와 파괴적인 행위에 대한 모니터링과 대응**
- ⇨ **PRACTICE 10 : 계정 만료에 대한 컴퓨터 접근 해지**
- ⇨ **PRACTICE 11 : 수사에 사용될 수 있는 데이터 수집 및 보관**
- ⇨ **PRACTICE 12 : 안전한 백업과 복구 프로세스 수립**
- Practice 13 : 내부 위협 통제에 대한 명확한 문서 보유

GATEONE

GATEONE

발췌 : www.cert.org/archive/pdf/CommoselsierThreatsV2.1-1-070118.pdf)

hp invent

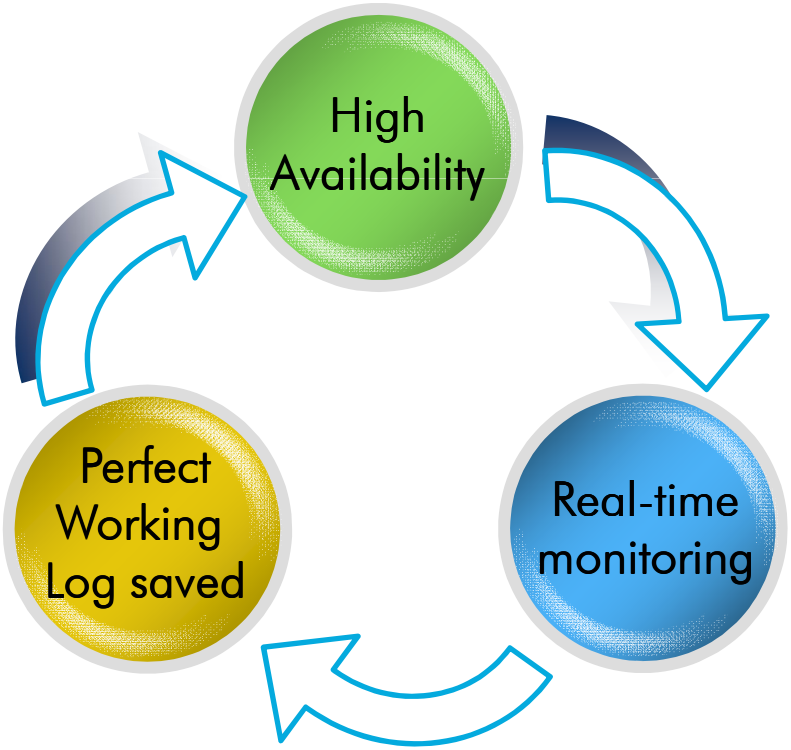
HP 보안 감사 솔루션(Gate-one Series)

보안 감사 솔루션의 필수 요건

신속한 의사판단 지원 여부

감사솔루션의 기준점은 실시간 모니터링이 얼마나 빠른 시간에 이루어지며 보호 받는 장비들의 장애를 감소시켜 가용성이 얼만큼 지속 되는가와 장애 발생시에 추적 가능한 로그를 완벽하게 저장되는지가 핵심

장애감소 및 가용성 보장과 증대	서버 및 네트워크 장비의 장애를 감소시켜 가용성 보장하고 증대 시켜야 함
실시간 모니터링	사용자의 행위가 관리자의 실시간 모니터링 화면으로 빠르게 보여줘야 함
완벽한 작업 로그저장	단순한 명령어나 결과값만 저장하는 것이 아닌 모든 행위 값을 저장



Non-Agent 방식의 보안 감사 솔루션

서버와 클라이언트에 Agent 미 설치

서버 Agent 설치 문제점

- Agent 설치로 인한 시스템 과부하 현상 초래
- 타 Application과 충돌 발생
- Agent 버전 업데이트 시 시스템 별로 각각 적용해야 함
- OS 버전 별 설치 어려움
- 서버용 Agent 자체 버그는 해킹 제 1의 취약점 대상

PC Agent 설치 문제점

- PC 성능 과부하 현상 초래
- Window OS의 경우 OS버전에 따른 Agent 오 동작 위험 존재
- 타 Application과 충돌 발생
- Agent 버전 업데이트 시 사용자 PC에 개별적 업데이트
- 스파이웨어 또는 해킹에 의한 Agent 유출

Agent 사용시의 단점

- Agent로 인한 관리의 어려움 증가
- 100% 모니터링이 안됨

Non-Agent 방식 구현

hp invent

세부 기능

GATEONE Core

- 세계 최초 네트워크 장비 접근제어 및 실시간 모니터링 감사 장비
- 세계 최초의 상용화 한 Gateway 방식의 보안감사솔루션(특허출원)
- telnet, ftp, ssh, sftp 등으로 접속하는 사용자들에 대한 100% 감사
- 명령어제어(금지명령어 및 사용자 실수에 의한 명령어 실행 차단)
- 세션제어(세션 Time-Out 기능, 세션 Kill 기능 등)
- 접근제어(서버 및 네트워크 접근 시 권한에 따른 접속제어)
- 권한제어(인증 받은 사용자이더라도 한 서버에서 다른 서버 접속 시 제어)
- 다양한 인증 연동(PKI 인증 연동, RADIUS 인증 연동)
- 한번의 로그 인으로 여러 서버 동시 접속 기능
- 실시간 모니터링(동시 접속자들에 대한 모든 실시간 모니터링 작동)
- 감사로그(사용자들의 모든 로그 저장 및 명령어 저장, 정책위반 저장)
- 장애 발생 시 복구를 위한 로그 제공

기대 효과

- 시스템 가용성 증대로 인한 시스템 유지 비용의 절감
- 시스템 장애로 발생하는 영업기회 비용의 절감(Zero(%))에 가까운 무 장애 서비스를 운영할 수 있는 기반 시설 제공으로 높은 ROI를 구현

- 보안사고 발생시 강력한 Evidence화 할 수 있는 상세 통계 제공

- 명령어제어/세션제어를 통해 Human error의 방지로 시스템 및 네트워크 장비의 가용성 증대
- 장애 발생시 빠른 복구

- 정책 및 로그 감사, 실시간 모니터링 등의 기능을 이용하여 사용자의 휴먼에러 차단
- 개발 소스 및 자료 유출 경로 추적
  → 인가자(사용자, 개발자)의 경우 서버에서 복사한 소스 자료의 유출 경로 추적
  → 자료유출 경로 추적에 따른 추가 사건 발생 방지 효과

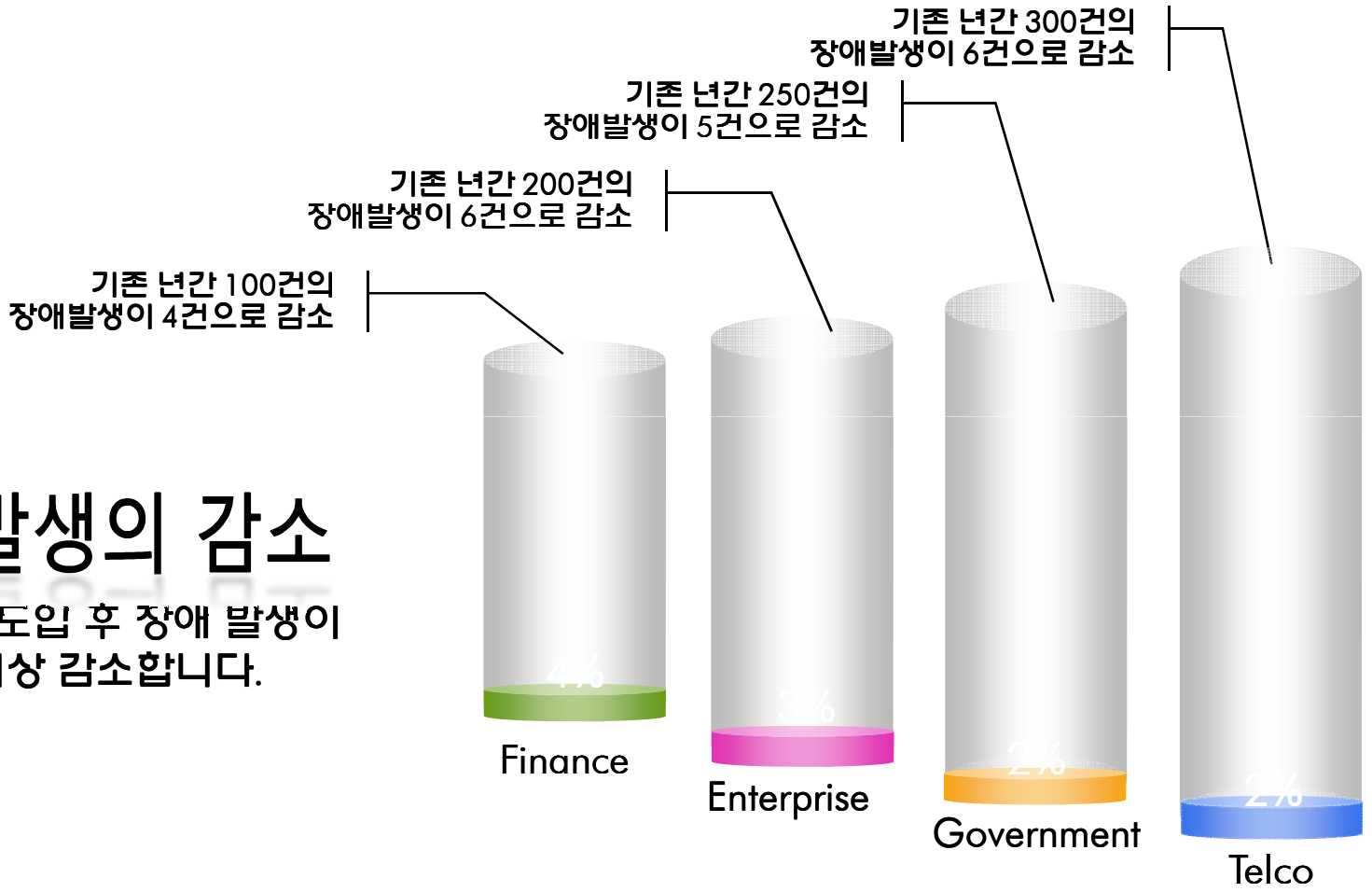
- 통합적인 사용자 관리를 통한 관리자 업무효율 증대
- 센터의 전산 통제 권한 강화
- 방화벽 rule의 감소에 따른 성능 향상 효과 기대

- 사용자들에 대한 보안정책 강화로 시스템의 안정성 확보
- Access time control로 작업자들의 작업시간 준수에 대한 강제성 확보-> 서비스 지연을 방지.

기대 효과 (솔루션 사용 고객 대상)

내 용	설 명
휴먼에러 방지에 따른 장비들의 무 장애 서비스 실현	- 명령어 제어 및 세션제어에 따른 Human error를 사전에 방지하여 고 가용성 실현
장애 발생시 굉장히 빠른 복구 방안 제시	- 작업자들에 의한 시스템 장애 발생 시 작업로그의 빠른 추적에 따른 복구 방안 제시
개발 소스 및 자료 유출 경로 추적	- 인가자(사용자, 개발자)가 서버에서 복사한 소스 자료의 유출 경로 추적 - 자료유출 경로 추적에 따른 추가 사건 발생 방지 효과
비 Agent방식에 따른 관리자의 업무 부담 감소	- 기존에 Agent방식의 보안감사 솔루션은 서버 및 클라이언트 agent 설치에 따른 관리자의 업무 부담 증가 - GATEONE은 비 agent방식을 구현하여 관리자의 보안감사 업무에 따른 작업량 및 관리 영역 감소
Access time control에 따른 작업 계획서상의 시간 준수	- 기존 유지보수 업체들이 작업시간을 정확히 준수하지 않음에 따른 서비스 지연을 방지 하는 효과 발생
실시간 모니터링 기능으로 즉각적인 작업 지시 및 사고 방지	- 작업자들의 세션을 관리자가 실시간으로 모니터링 함에 따라 즉각적인 작업 지시 변경, 중지, 차단하여 고 가용성 보장
웹 인터페이스 접근 방식에 따른 자유로운 네트워크 장비에 설치	- 기존 방화벽이나 IPS 처럼 특정한 위치가 아닌 네트워크 장비의 어느 곳이나 설치 가능하여 내부 네트워크의 변경 작업 불필요
완벽한 권한 관리에 따른 Access Control	- 사용자별 장비의 접근 권한에 따른 작업 수행으로 작업자 관리가 용이

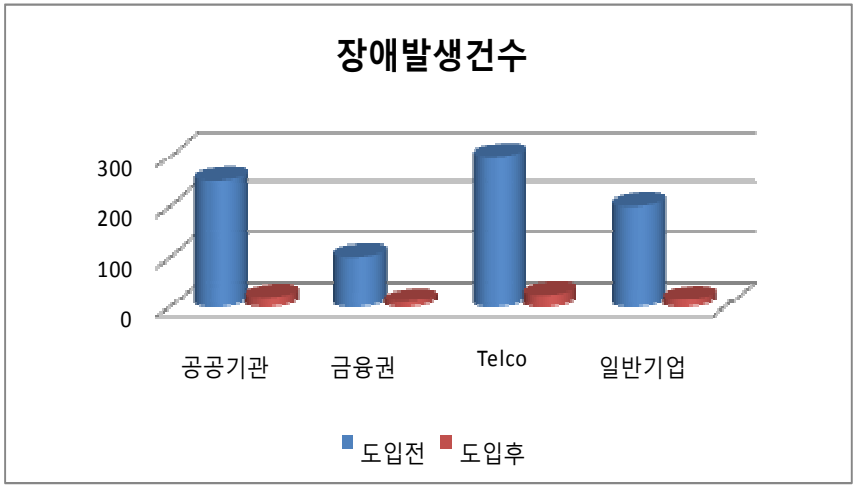
장애 감소 효과

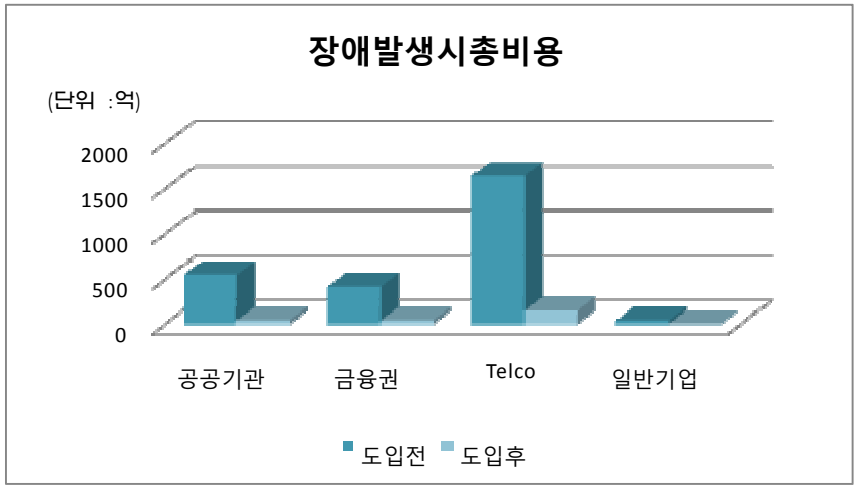


장애 발생의 감소

GATEONE 도입 후 장애 발생이
96% 이상 감소합니다.

장애감소효과(ROI 분석표)

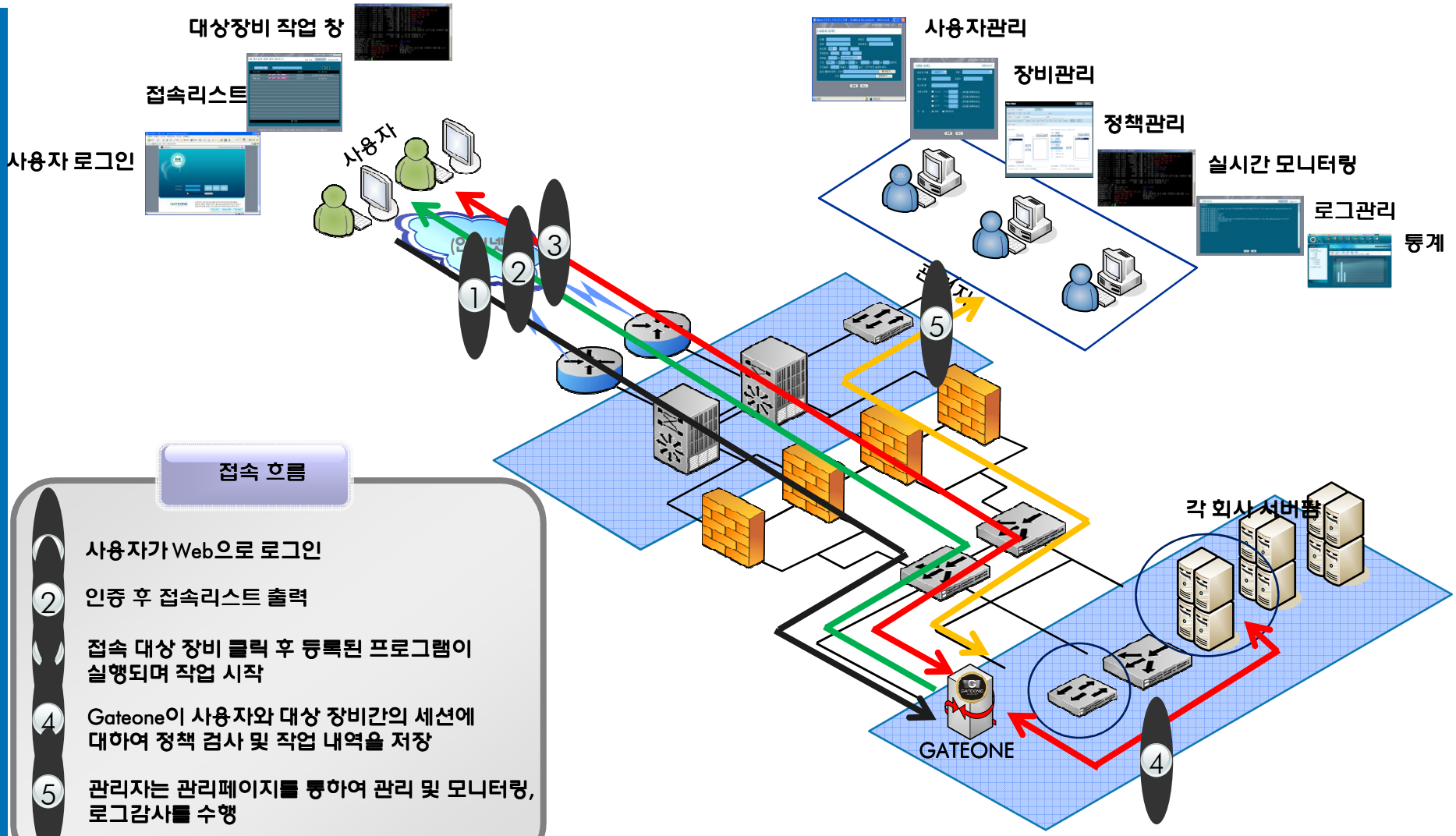




(단위 : 원)

구 분		공공기관	금융권	Telco	일반기업
보안감사 솔루션 설치 전	장애시간당 영업손실 비용	222,000,000	420,000,000	600,000,000	1,1240,000
	년간 장애발생건수	250	100	300	200
	장애복구시간	2	1	1	3
	장애복구 투입인력	2	3	3	1
	투입인력 시간 단가	19,245	19,245	19,245	19,245
	장애발생시 총비용	55,500,115,470	42,000,057,735	180,000,057,735	2,248,057,735
보안감사 솔루션 설치 후	장애발생건수	20	10	25	15
	장애 감소 비율	92%	90%	92%	90%
	장애발생시총비용	4,440,115,470	4,200,057,735	15,000,057,735	168,657,735
비용 절감 효과		51,060,000,000	37,800,000,000	165,000,000,000	2,079,400,000

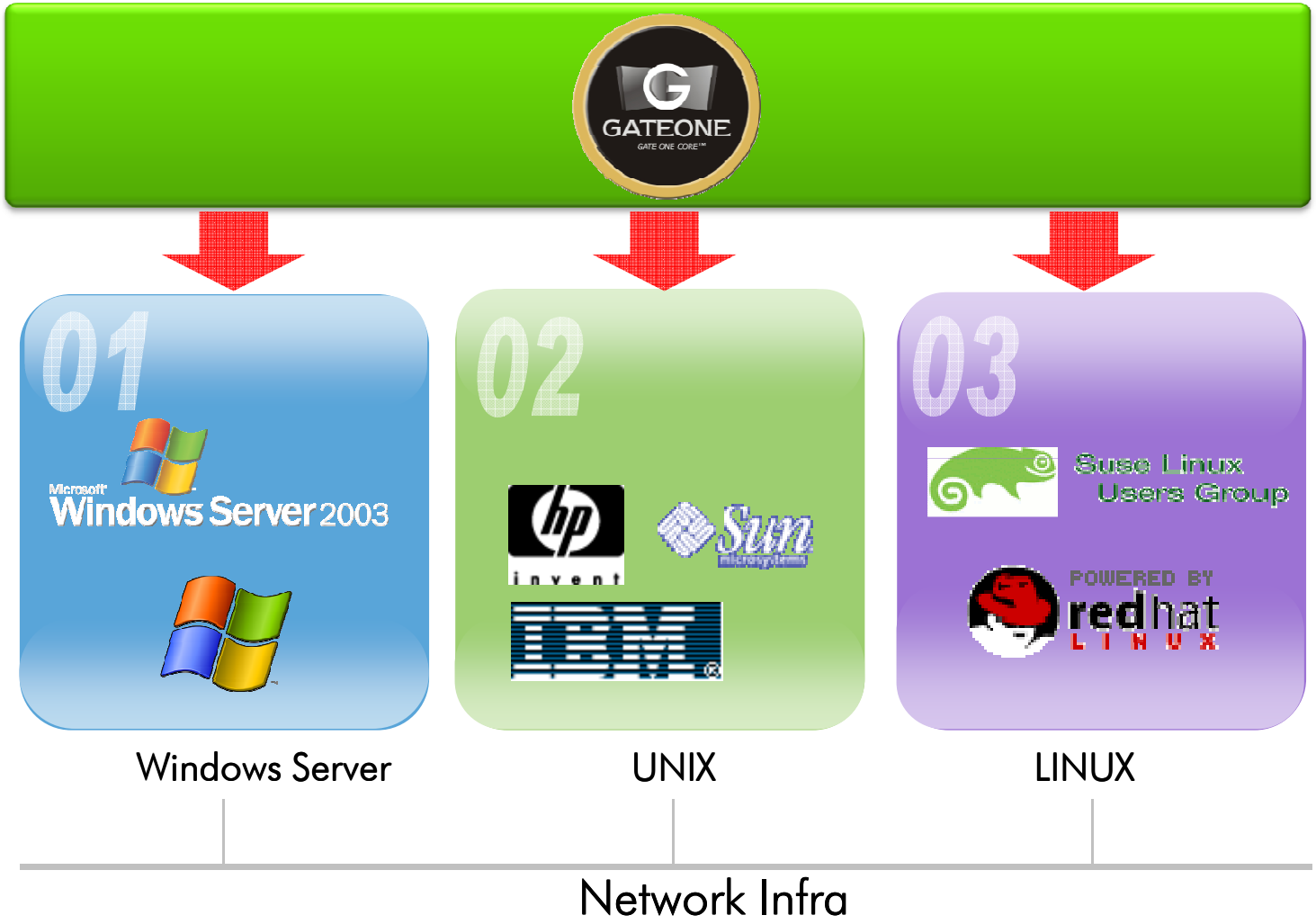
구성도



접속 흐름

1. 사용자가 Web으로 로그인
2. 인증 후 접속리스트 출력
3. 접속 대상 장비 클릭 후 등록된 프로그램이 실행되며 작업 시작
4. Gateone이 사용자와 대상 장비간의 세션에 대하여 정책 검사 및 작업 내역을 저장
5. 관리자는 관리페이지를 통하여 관리 및 모니터링, 로그감사를 수행

지원 플랫폼



- Windows 원격 터미널은 제외
- 2007년 9월22일부터 GATEONE-W에서 지원

hp invent

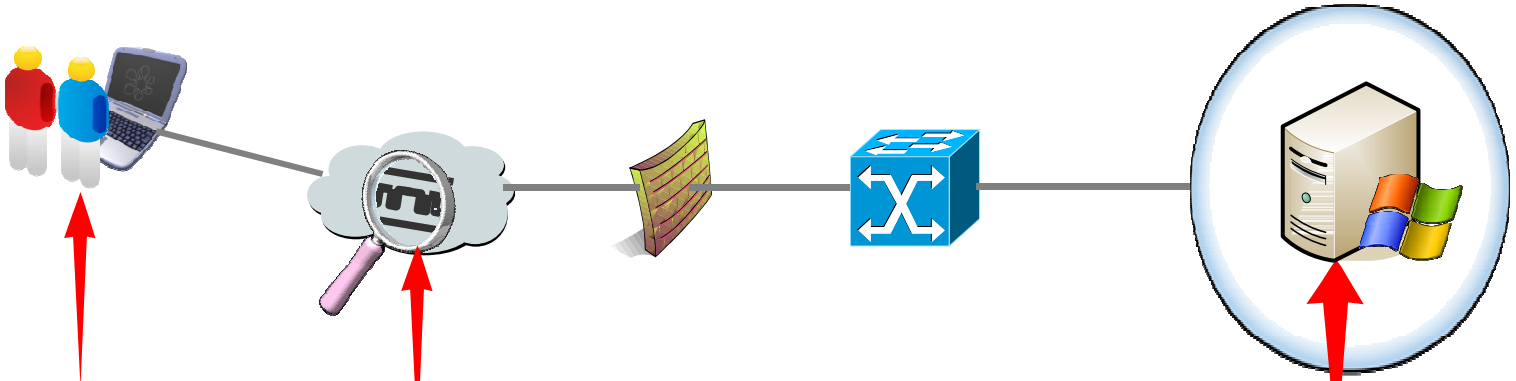
GATEONE-W 개요

GATEONE-W Series는 Windows서버에 대한 원격 접근제어 및 감사 기능을 제공합니다.

솔루션 등장 배경

현실적 문제점 인식

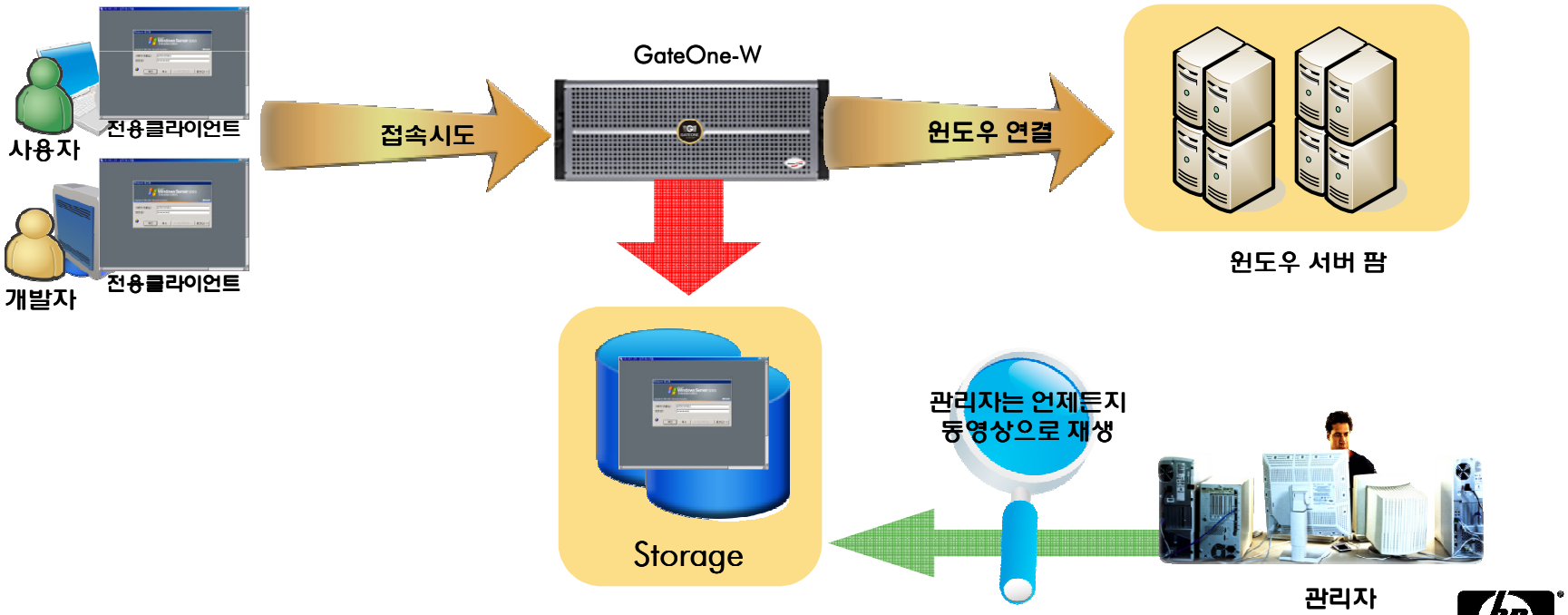
- 사용자 작업에 의한 Windows 기반의 시스템 장애 발생이 빈번함
- 개발자 및 운용자가 윈도우 시스템 사용시 Windows Terminal 작업 세션 제어 불가
- Windows Terminal 작업으로 인한 장애 발생시 복구하는데 많은 인력과 시간을 소요
- Windows Terminal 작업에 대한 감시 관리 시스템 부재
- 인증 받은 사용자가 서버에 접속 시 어떤 작업을 하는지 감사추적이 불가능



GATEONE-W 핵심기능

GATEONE-W 핵심기능(계속)

- 클라이언트와 Windows Server간 Windows 원격터미널 접속 시 GateOne-W가 다중 사용자의 접속을 원활히 중개
- Windows 원격접속부터 Logout시점까지 동영상 녹화
- Windows 원격접속 명령어 제어는 지원하지 않지만 녹화 재생 기능을 지원하여 장애 발생시 빠른 원인 추적 제공
- 동영상의 저장 로그가 작게 sizing 되어 storage의 부담을 줄임

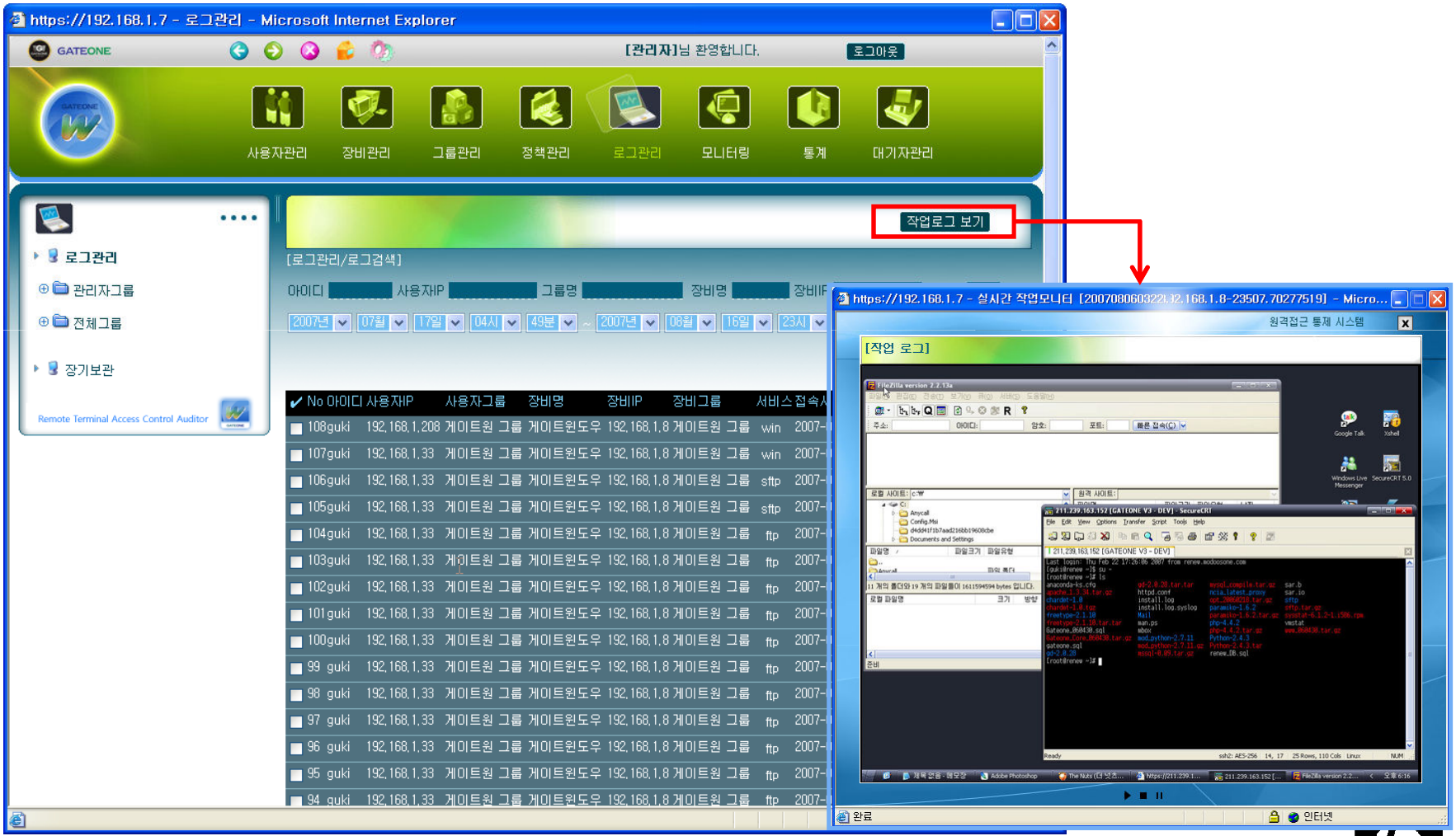


세부기능 – 로그인 화면

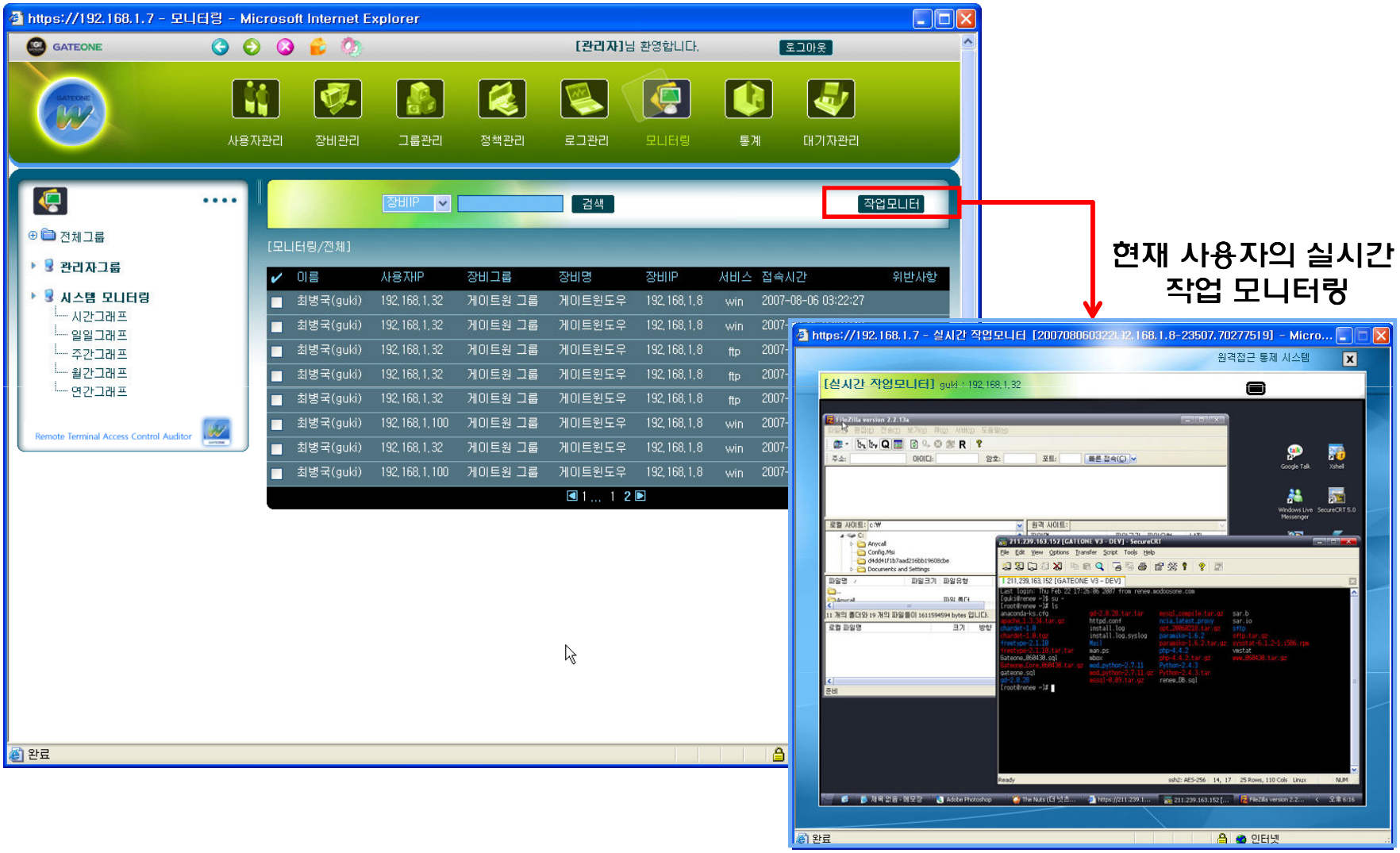

https://192.168.1.7 - 원격접근통제시스템 - Microsoft Internet Explorer
서비스팩2 이상 사용자들은 인터넷 옵션->도구->팝업차단설정에서 본 사이트의 팝업을 허용해 주세요.
GATEONE
Modoosone Network Management System
GATEONE
Windows
Remote Terminal Access Control Auditor
패스워드 5회 오류시 계정사용이 중지 됩니다.
아 이 디 :
패스워드 :
로그인
인증서
CLIENT DownLoad
DownLoad
GateOne
GATEONE W (윈도우즈 보안 감사 솔루션)은 모두스원의 보안감사 핵심기술력을
바탕으로 사용자의 네트워크 장비 및 접속사용 로그를 분석하여 보안사고 발생 시
강력한 증거자료를 제시할 수 있는 세계 최고의 완벽한 보안감사 솔루션 입니다.
가입 신청
가입처리 확인
문의 메일
Copyright @ 2007 Modoosone Co.,LTD Ver. GATEONE W 1.0.1
본 페이지는 1024*768 과 1280*1024 해상도에 최적화 되어 있습니다.
javascript:login()
인터넷

세부기능 – 로그관리(동영상 로그보기)

- 동영상 윈도우 로그 저장, 로그 기록 검색 및 내용 검색



세부기능 – 실시간 모니터링



현재 사용자의 실시간 작업 모니터링

공공기관 도입 사례

발췌 : 정보보호21C 9월호 & Security News

통합전산센터, 시스템 안정화 '완벽'

HP 보안감사솔루션 'GATEONE' 도입해 보안 강화

정부는 지난 2006년 10월 행정자치부, 재경부 등 24개 기관 1555대 등 총 3584대 시스템을 대전 제1통합전산센터로 이전해 통합, 운영해오고 있다. 정부통합전산센터(센터장 강중협)는 국가 정보자원의 효율적 관리와 안정적 운영을 책임지고 있으며, 그간 각 정부 기관별로 분산 구축·운영되던 정보자원을 통합하고 국가 차원의 백업시스템을 구축해 모든 공공기관에 고품질, 고보안성의 인터넷 서비스를 제공하는데 주력해 왔다. 이런 가운데 최근 보안감사솔루션을 도입해 보안에 완벽을 기하고 있다. 글·김민권 기자

> 정부 전산망 통합이후 장비당 월평균 장애시간이 통합 전 67분에서 통합 후 2분으로 감소

계 사업도 올해 안에 완료할 계획이다.

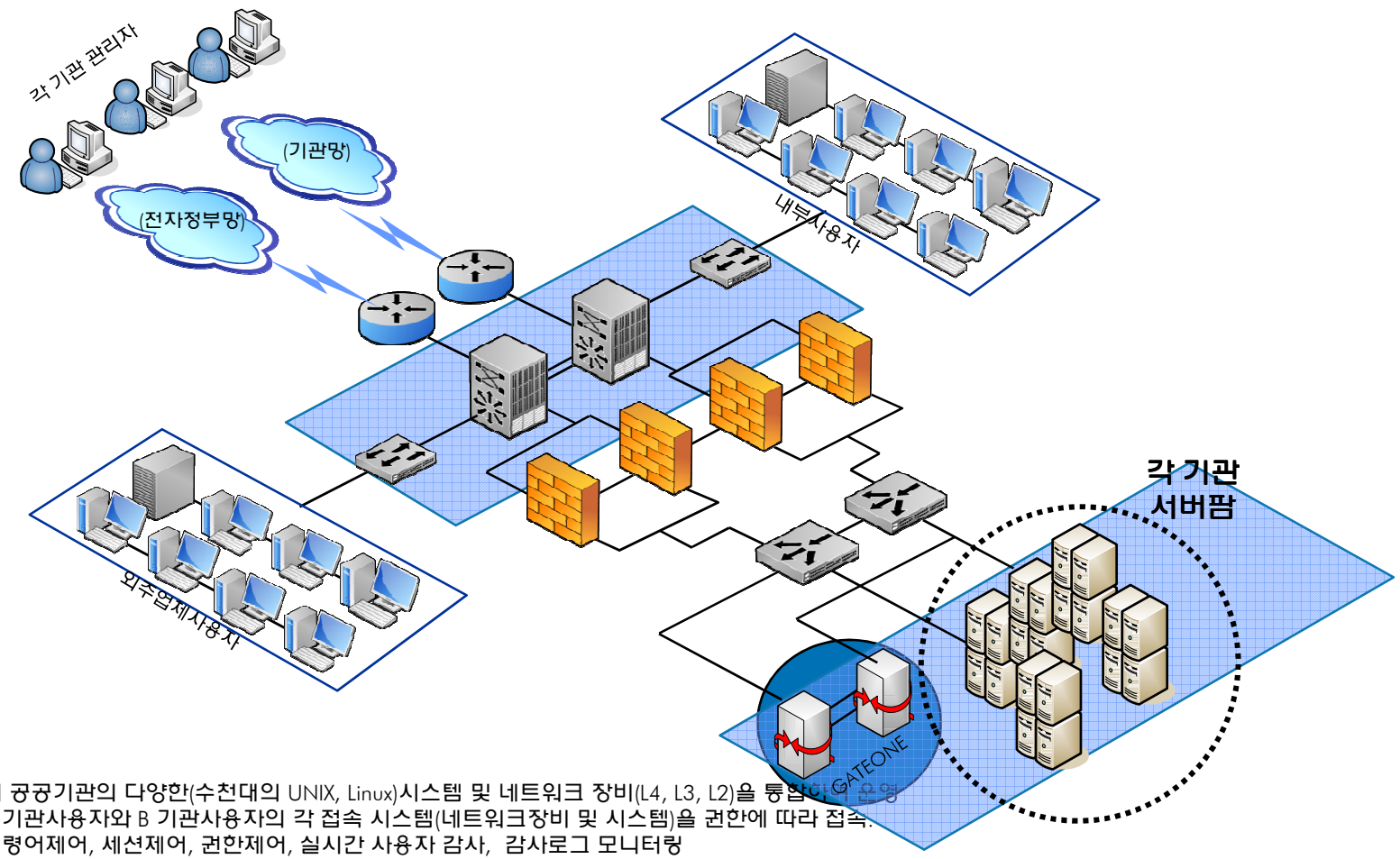
통합전산센터 관계자는 "정부 전산망 통합 이후 장비당 월평균 장애시간이 통합 전 67분에서 통합 후 2분으로 감소했으며, 이에 따른 시스템 가동률도 통합 전 99.8%에서 통합 후 99.99%로 개선됐다. 또한 해킹 공격에 대비 24시간 365일 대응체계를 구축해 서비스 안정성을 크게 향상시켰다"고 밝혔다. 정부는 올해 말까지 광주 제2센터

Reference

외 50 Site

hp invent

XXX 공공기관 GATEONE 구축사례

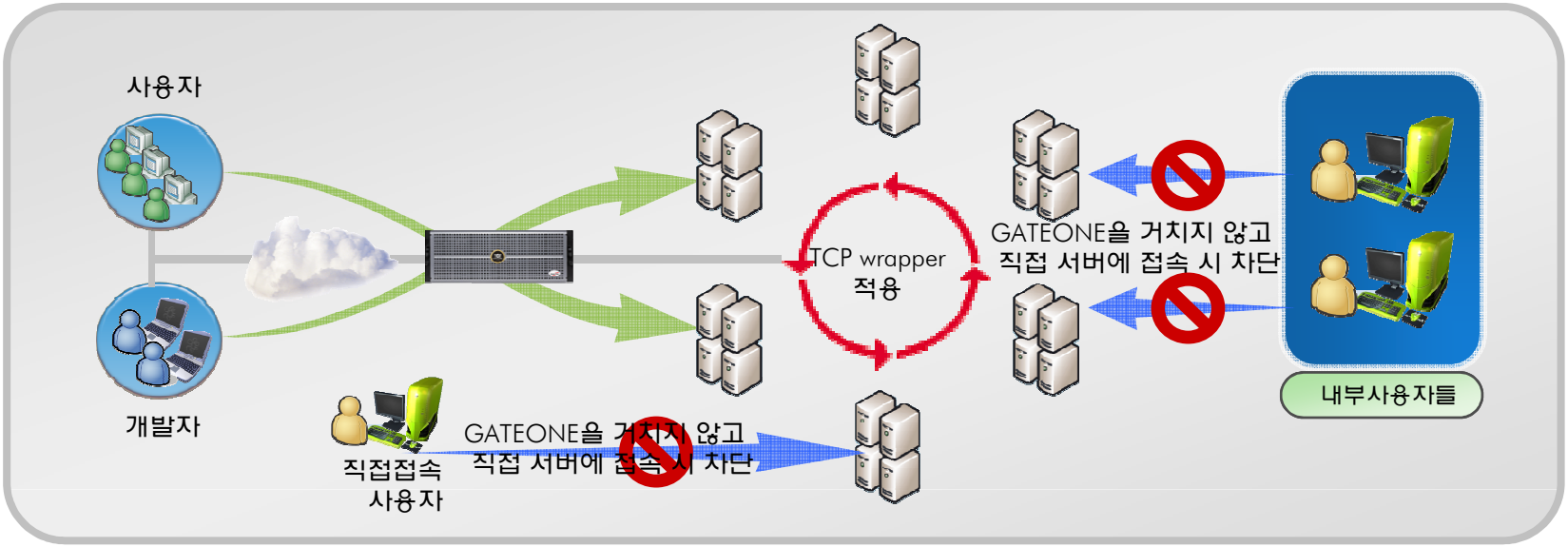


Ⅰ. 전산환경 : 여러 공공기관의 다양한(수천대의 UNIX, Linux)시스템 및 네트워크 장비(L4, L3, L2)을 통합[illegible]

Ⅱ. 조　　건 : ① A 기관사용자와 B 기관사용자의 각 접속 시스템(네트워크장비 및 시스템)을 권한에 따라 접속.
② 명령어제어, 세션제어, 권한제어, 실시간 사용자 감사, 감사로그 모니터링
③ 사용자 접속은 전용 sftp, ssh 클라이언트 프로그램을 이용하여 접속
④ 접속자수 : 4,000명

Ⅲ. 원격접속통제 보안감사시스템(GATEONE장비)의 역할
각 기관의 사용자들은 원격접속통제시스템으로 접속하여 자동으로 권한에 따른 시스템 접속을 연결하여 주고 사용자별 명령어, 세션, 권한을 실시간 제어함으로써, 미연에 있을 휴먼에러를 방지하고 향후 발생할 보안 사고를 대비한 감사 로그(이력관리)를 저장

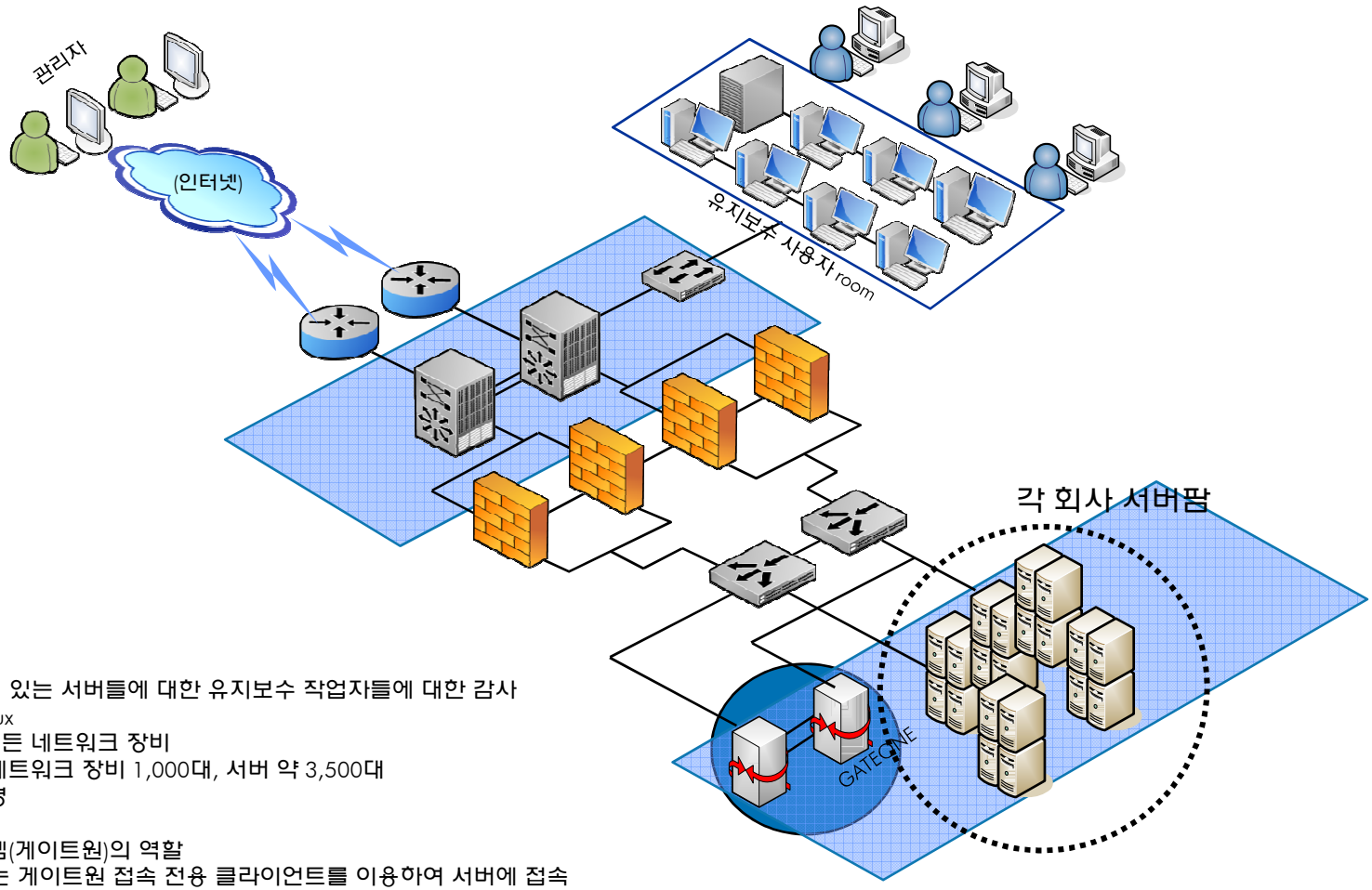
통신사 GATEONE 구축사례



Ⅰ. **전산 환경**
- **네트워크 전산센터 내에 산재해 있는 네트워크 장비 및 서버의 운영**
- **시스템** : UNIX, Linux
- **네트워크 장비** : Cisco, L3, L4, L2
- **관리 장비 수량** : 네트워크 장비 약 100대, 서버 약 500대
- **접속자 수** : 100명

Ⅱ. 원격접속통제시스템(GATEONE)의 역할
- **원격사용자 및 본사 사용자의 인증 시 접속권한리스트를 부여.**
- telnet, ftp 접속에 대한 작업로그(이력관리)를 저장.
- **허용하지 않은 명령어 실행 시 자동적으로 세션을 끊음.**
- **지정한 시간에 따라 접속을 허용함으로써 작업시간 준수.**
- TCP wrapper를 적용하여 서비스 하는 프로토콜에 한해서는 모든 서버들이 GATEONE시스템에 대해서만 응답.

IDC GATEONE 구축사례



Ⅰ. 전산 환경
- IDC 센터에 입주해 있는 서버들에 대한 유지보수 작업자들에 대한 감사
- 시스템 : UNIX, Linux
- 네트워크 장비 : 모든 네트워크 장비
- 관리 장비 수량 : 네트워크 장비 1,000대, 서버 약 3,500대
- 사용자수 : 2,000명

Ⅱ. 원격접속통제시스템(게이트원)의 역할
- 각 유지보수 업체는 게이트원 접속 전용 클라이언트를 이용하여 서버에 접속
- telnet, ssh, ftp로 접속하여 장비에 대한 작업로그(이력관리)를 저장.
- 허용하지 않은 명령어 실행 시 자동적으로 세션을 끊음.
- 지정한 시간에 따라 접속을 허용함으로써 작업시간 준수.
- 관리자는 원격 작업 관리하여 장애 발생을 대비한 감시.

hp invent

Demo Scenario

사용자 접속	• 사용자가 정상적으로 로그인하여 대상 서버에 접속하여 작업하는 화면을 시연
실시간 모니터링	• 관리자로 로그인하여 사용자의 작업 세션을 실시간 모니터링
정책위반	• 사용자가 금지명령어 실행으로 정책위반 발생 • 관리자 화면에서 경보음이 발생하고 명령어가 실행이 되는 않는 상황 시연
강제 세션차단	• 관리자가 사용자 세션을 강제로 차단
정책설명	• 사용자 정책 화면에서 사용자 관리 정책을 설명
로그 보기	• 사용자 로그를 다양한 검색조건으로 검색 • 로그의 내용을 설명
정책위반로그보기	• 정책위반 로그에서 사용자 정책을 보는 부분을 설명 • 정책위반 내용을 설명

hp invent

SHOW DEMO

(GATEONE-C Series)

Q & A

HP Solution World 2007

IT transformation to BT