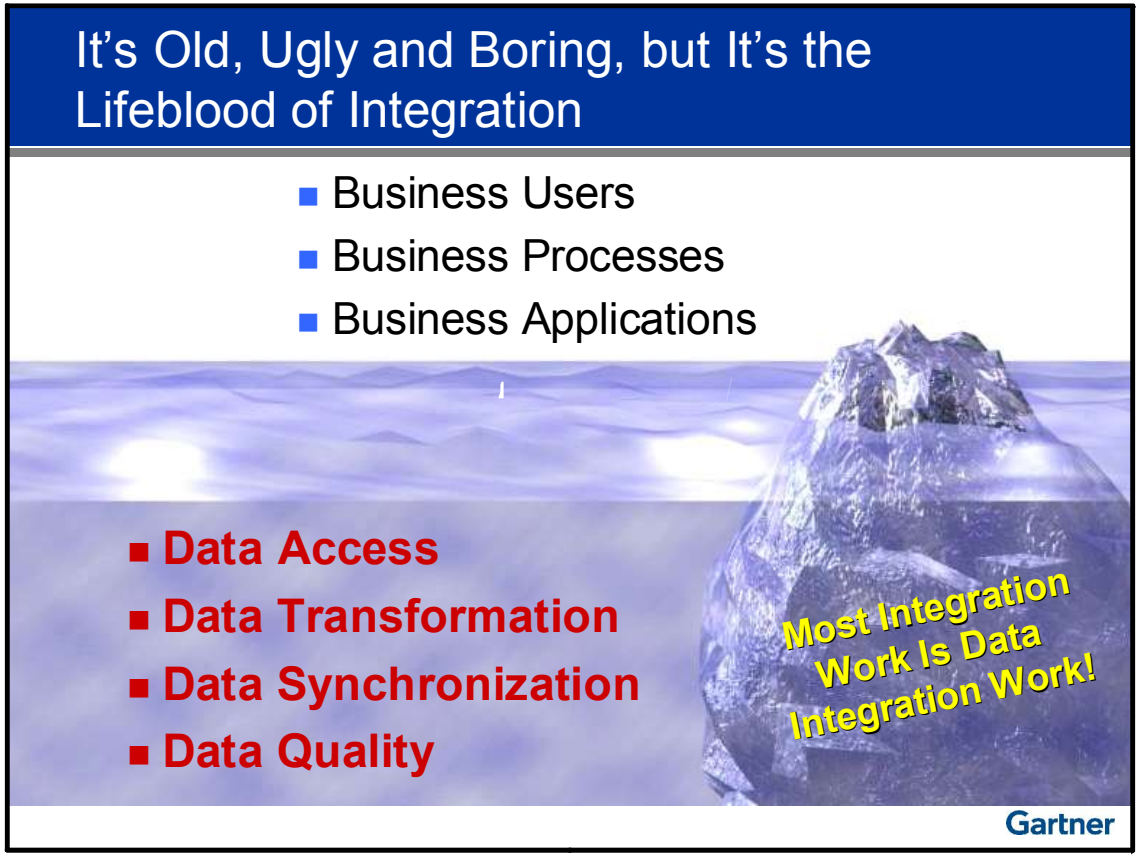
Industry Solutions

Sterling Commerce Enterprise MFT Solutions

Sterling Commerce

1

파일전송오래 전부터 사용되었으며, 여전히 사용되며, 더 많이 사용되고 있는 기술



80 percent of data exchange today is accomplished through movement of files

-

Gartner

© 2011 IBM Corporation

데이터 전송의 해결해야 할 과제

- 보안(Security)
  - 전송중인 **파일에 대한 보안이 각종 규제정책 및 정보보호와** 관련하여 CIO와 담당자의 관심사항으로 부상 (예: 개인정보보호법, PCI등)
  - 민감한 내용(예:고객정보,내부 기밀정보,영업정보, 도면등)의 **데이터가 암호화 되지 않고 전송**. 기밀정보의 기업 내,외부로의 유출에 대한 우려 증가.
  - FTP의 보안 취약성
    - DMZ내의 FTP서버는 외부 **해커등의 공격에 노출되어** 있음
    - 보안 취약성 보고에 대응한 정기적인 FTP 서버 패치등의 미흡
    - 조직내의 특히 각종 업무팀내에 보고하지 않는/혹은 **중앙 관리되지 않는 FTP서버들** 존재.
    - 내부 FTP서버 계정 아이디/패스워드가 스크립트내에 하드코딩되어 있음.
    - 내부 FTP서버 계정 아이디/패스워드가 암호화 되지 않고 네트워크를 통하여 전송되고 있음.
  - 기업 내,외부를 통하여 데이터의 전달 경로 및 접근자에 대한 정보에 관심이 증대하고 있음.
  - 많이 기업들이 내부 네트워크내에서 **보관중이거나 이동중인 데이터 파일에 대한 암호화를** 고려하고 있음.
  - 다수 개발프로젝트/ 운영조직의 결과로 IT관련작업이 분산적으로 수행되며 **노력과 비용이 중복 투자됨**

© 2011 IBM Corporation

Connect:Direct 기능상세 - 보안

▶ **CC 인증 제품**

데이터 암호화 전송을 담당하는

Connect:Direct Secure+ Option 이

CC(Common Criteria : 정보보호제품

국제 공통평가기준) 인증을 획득함.

※ 참조 : Common Criteria

CC(국제공통평가기준)는 세계 여러 국가에서 개발·생산되고 있는 정보보호제품에 대한 평가기준을 국제적으로 표준화한 것이다. 즉 세계적으로 유통되는 정보보호제품에 대한 단일화된 평가기준을 마련해 관련 시장에서 해당 제품들에 대한 신뢰성을 보장하는 것

Certification Report

EAL 2+ Evaluation of Sterling Commerce Inc.,

Connect:Direct® with Secure+ Option

v3.7 running on UNIX and v4.2 on Windows

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© 2006 Government of Canada, Communications Security Establishment

Document number:	383-4-48-CR
Version:	1.0
Date:	15 September 2006
Pagination:	i to v, 1 to 9

© 2011 IBM Corporation

데이터 전송의 해결해야 할 과제

- **파일 전송량 증가(File Transfer Volume Growth)**
  - **파일 전송의 볼륨이 해를 거듭할수록 지속적으로 증가할** 것으로 예측되며, 그것은 전송되는 횟수 뿐만 아니라 파일 자체의 크기(Mb->Gb)가 증가하고 있음.
  - 파일 전송은 이질적인 시스템간에 약한 결합성(loosely coupled)을 가진 연계의 장점을 가진 수단으로 애용되고 있으며, 특히 **배치형태로 운용되고** 있음. 특히 기업간(혹은 조직간)에는 상당부분의 정보가 파일전송형태로 교환되고 있음.
  - 기업간의 인수.합병의 증가로 **절대량의 데이터가 증가하고** 있음.
  - 파일 전송이 지속적으로 증가함에 따라 **작업량과 강도는 높아지고 있지만** 상응하는 시스템과 관리 자원은 고정되어 있음.
  - 전송된 파일의 불안전한 위치정보 혹은 전송실패, 전송지연등으로 고객사/파트너사의 업무지장을 초래하고 있으며, 신뢰 및 매출에 영향을 미치기도 함.
  - 고객사/파트너사 선택할 수 있는 **전송프로토콜이 제한적.**

© 2011 IBM Corporation

데이터 전송의 해결해야 할 과제

- 가시성/관리(Visibility/Management)
  - 크고 작은 파일 전송에서 **고객사/파트너사에게 가시성(파일전송에 대한 상태, 완료여부등의 파악)제공은 중요한** 것으로, 이것은 신뢰성있는 비즈니스를 위한 핵심내용이다. 가시성의 제공은 파일크기와 상관없이 필요한 부분이다.
  - 파일전송은 고객에 대한 Service Level Agreement (SLA) 의무를 만족시키는 핵심 역할에 복무한다. SLA관리의 제공은 고객사 만족을 가능하게 하는 핵심사항이다.
  - SLA는 또한 IT조직자체가 내부업무팀에 제공하는 **서비스의 수준을 측정하는 지표로** 사용될 수 있다.
  - 고객사/파트너사에게 제한적은 가시성을 제공하거나 아예 제공하니 못함.
  - 각기 다른 가지 각색의 기능을 제공하는 다양한 형태의 **복수 FTP 인프라를 운영하고** 있으며, 이것은 **효율적인 운영관리를 저해하고** 있음.
  - 복수의 조직에서 관리 되는 FTP서버를 통한 파일 전송은 **전송내역에 대한 단편화된 정보만을** 제공한다.
  - 파일전송의 실패는 그 것을 해결하기 위한 시간 및 개인의 노력과 비용이 요구되며, 고객사/파트너사의 불만족을 초래.
  - **FTP자체로는 관리, 암호화, 자동화 기능 등을 포함하고 있지 않아** 필요할 때마다 써드파티기능을 추가하고 있음.

© 2011 IBM Corporation

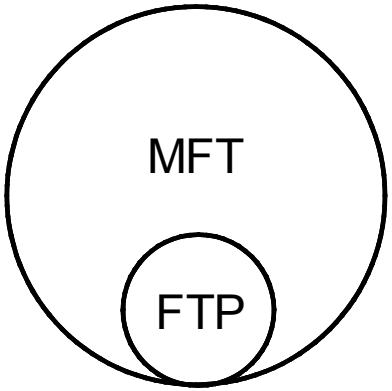
데이터 전송의 해결해야 할 과제

- **고객/파트너 연결하기(Customer/Partner Onboarding)**
  - 많은 기업들이 고객사/파트너사/공급사등을 주어진 시간안에 **신규로 연결(on-boarding)하는데 어려움을** 가지고 있음.
  - 신규 **고객 연결(on-boarding) 지연으로** 인한 수익 및 고객 만족도에 영향을 미침.
  - 신규 **파트너 연결(on-boarding) 지연으로** 인한 비용절감 기회 손실.
  - 신규 **공급사 연결(on-boarding) 지연으로** 인한 물자 및 서비스 공급에 차질 초래.
  - 그 외 다양한 이슈들이 존재.
    - 특정 프로토콜에 맞추어 복수의 파일전송 인프라(예: FTP 서버, SFTP 서버등) 존재. 어떤 경우 직접 개발(In-house development)하거나 여러 종류의 제품을 사용함으로써 **상당부분 수작업을** 수반함.
    - 신규 연결시점에서 보안과 관련하여 네트워크나 방화벽의 설정변경을 동반하는 경우 보안정책변경과 관련하여 **상당한 기간이 소요**하는 경우가 발생한다. 또한 고객사/파트너사의 기술적 준비정도나 IT인프라가 상이함으로써 더 많은 기간이 요구되는 경우도 발생함.
    - 대부분의 경우, 신규 고객사/파트너사/공급사 연결시 시스템관리자는 연계시스템의 고객정보(계정,암호등)를 설정하게 되며, 이러한 작업은 연계 작업시 추가 소요시간을 필요로 함.
    - On-boarding 처리 절차에서 고객사/파트너사/공급사와 연결과 관련하여 이메일이나 전화를 이용하여 수많은 정보를 교환하며, 연결 테스트작업에서도 많은 시간을 필요로 한다. 이 작업이 On-boarding 처리에서 대부분의 시간을 소요되는 부분이다. 이때 정보의 교류가 부정확하거나 지연되는 경우가 다수 발생한다.
  - 많은 기업들이 이러한 on-boarding 처리절차에서 고객 스스로가 각자의 정보를 스스로 등록관리(self-service mode)할 수 있는 솔루션을 추구한다.

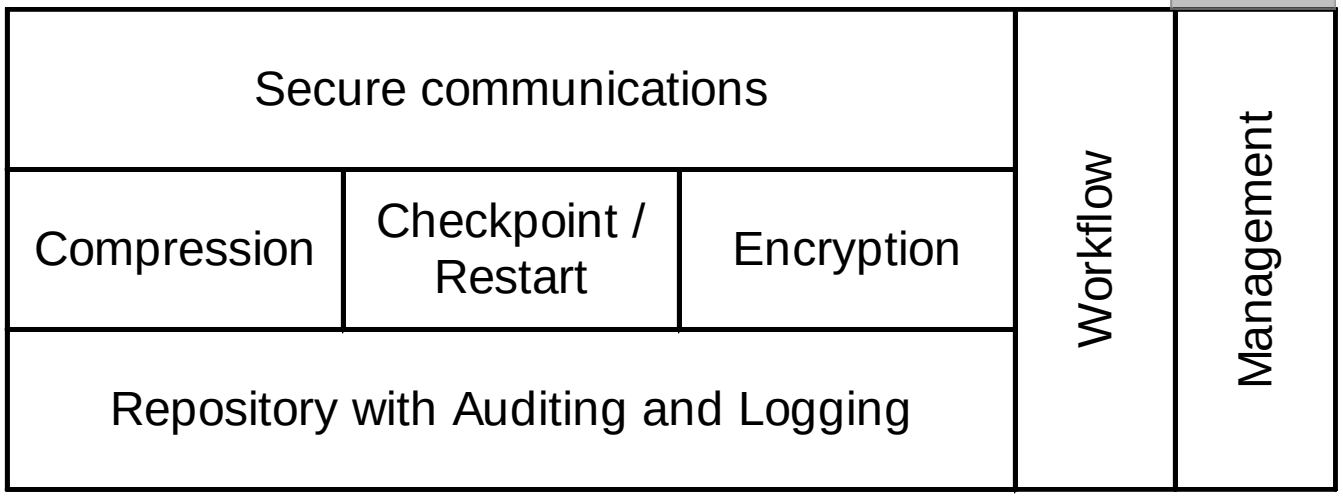
© 2011 IBM Corporation

해결을 위한 솔루션

- **MFT (Managed File Transfer) 개요**
  - 기존 FTP의 불완전에 기능을 대체하는 전용 솔루션
  - 안전한 파일전송기능 (장애 시 자동복구를 통한 전송보장)
  - 전송 성능을 위한 압축, 보안 전송을 위한 암호화 전송
  - 파일 전송에 대한 감사 및 로깅을 위한 중앙집중식 레파지토리
  - 어플리케이션의 업무 프로세스와 연계를 통한 자동화 구현
  - 중앙집중식 관리기능

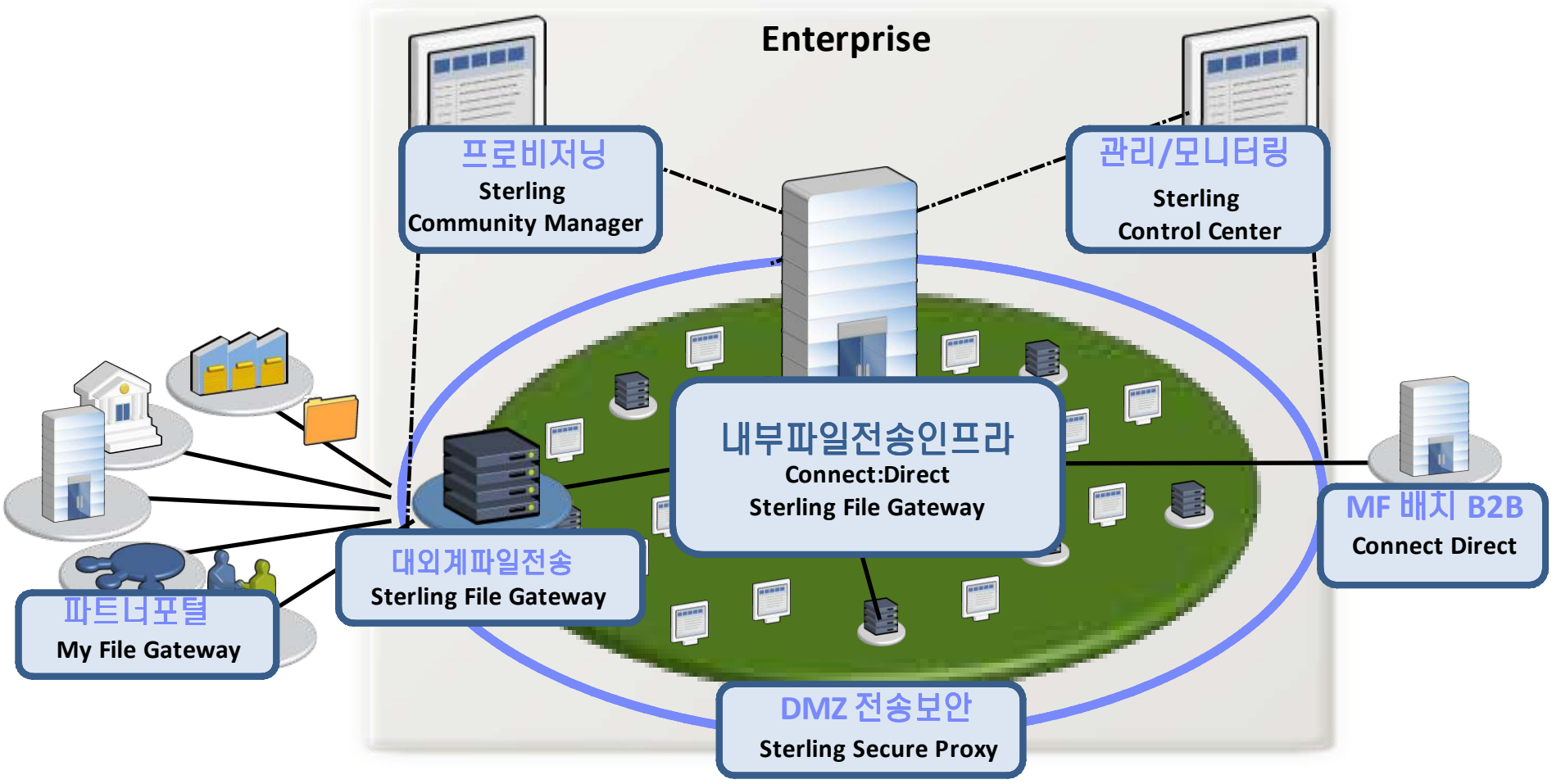


Gartner



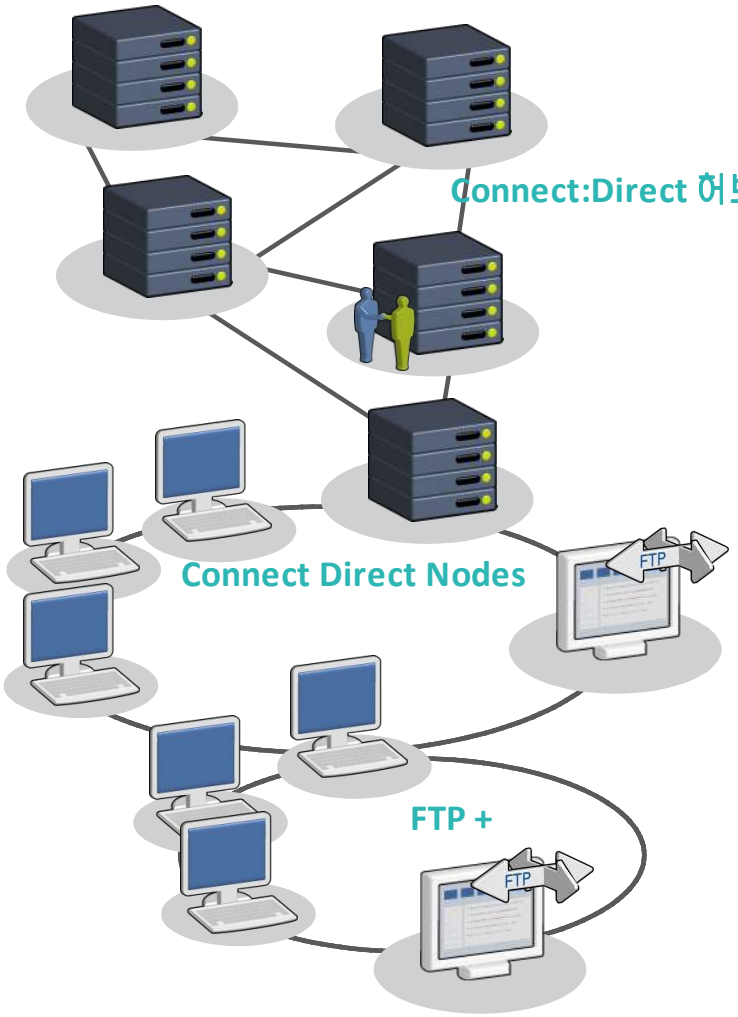
© 2011 IBM Corporation

Sterling MFT 제품군 구성



© 2011 IBM Corporation

내부 파일전송 : Sterling Connect:Direct / FTP+

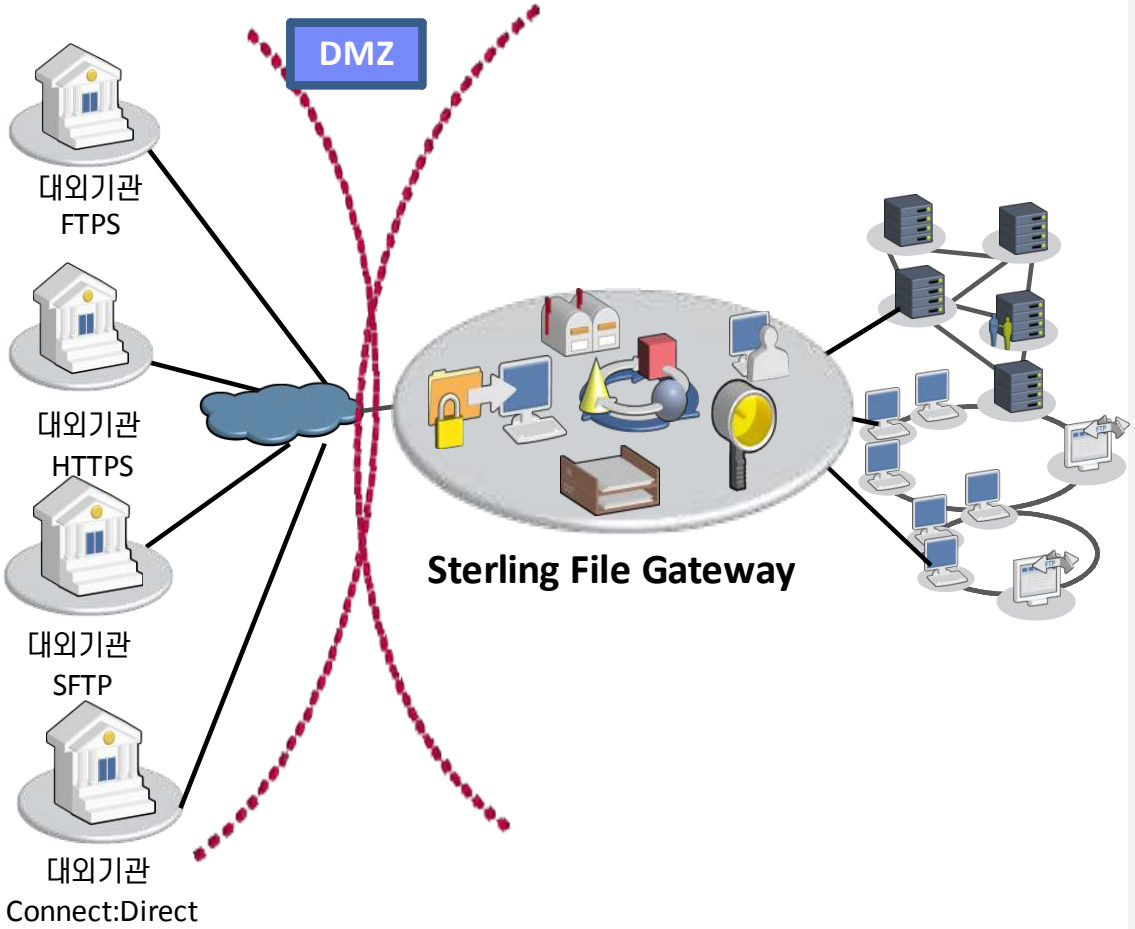


- 엔터프라이즈 파일전송을 위한 견고한 아키텍쳐
- z/OS, i-Series, Unix, Linux & Windows등 다양한 OS지원
- 이질적 시스템간(z/OS<->Unix) 데이터 코드페이지 자동변환
- 상용 Job Scheduler등과 연계를 통한 작업자동화
- 에러 자동복구 및 Checkpoint restart
- 평균 > 99.999% 의 가용성
- 100Gb가 넘는 대용량 파일전송 지원
- FTP+는 클라이언트제품으로 기존FTP스크립트를 재사용하여 C:D기능을 사용가능

© 2011 IBM Corporation

대외기관 파일전송 : Sterling File Gateway

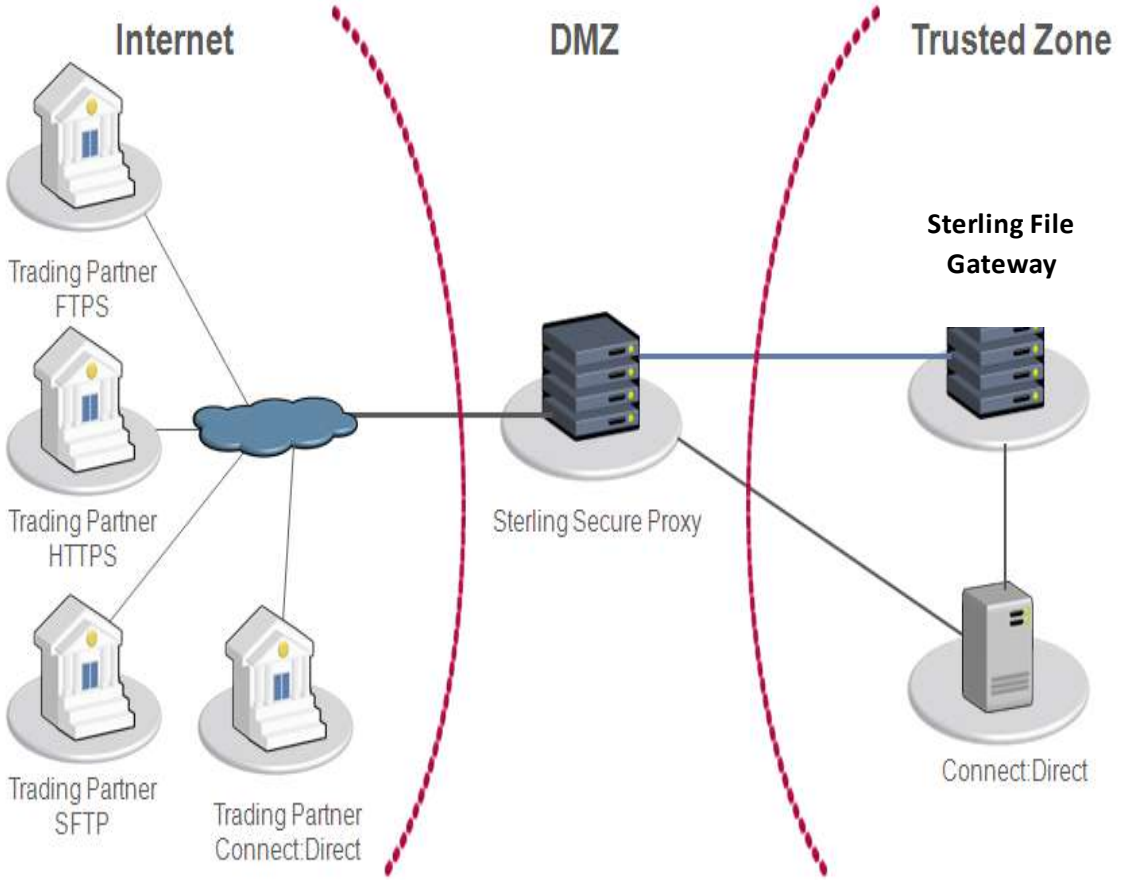
다양한 대외기관 연계를 위한 단일 플랫폼



- 다양한 전송 프로토콜을 지원하는 단일 플랫폼
- 신속한 고객사/파트너사/공급사 연계 지원
- 안전한 Mailbox 기능
- 지원 프로토콜: C:D, FTP(/S), HTTP(/S), AS2, AS3, SWIFT, SFTP
- 수평/수직적 확장성 제공
- 다양한 Back-end 시스템 연계 EAI Adapters (예:Web Services, MQ, JMS, JDBC, SAP)
- EDI, ACH Payments, SWIFT 표준지원
- Any-to-Any 데이터 변환 및 규칙 지원
- 보안을 위한 Best Practices

© 2011 IBM Corporation

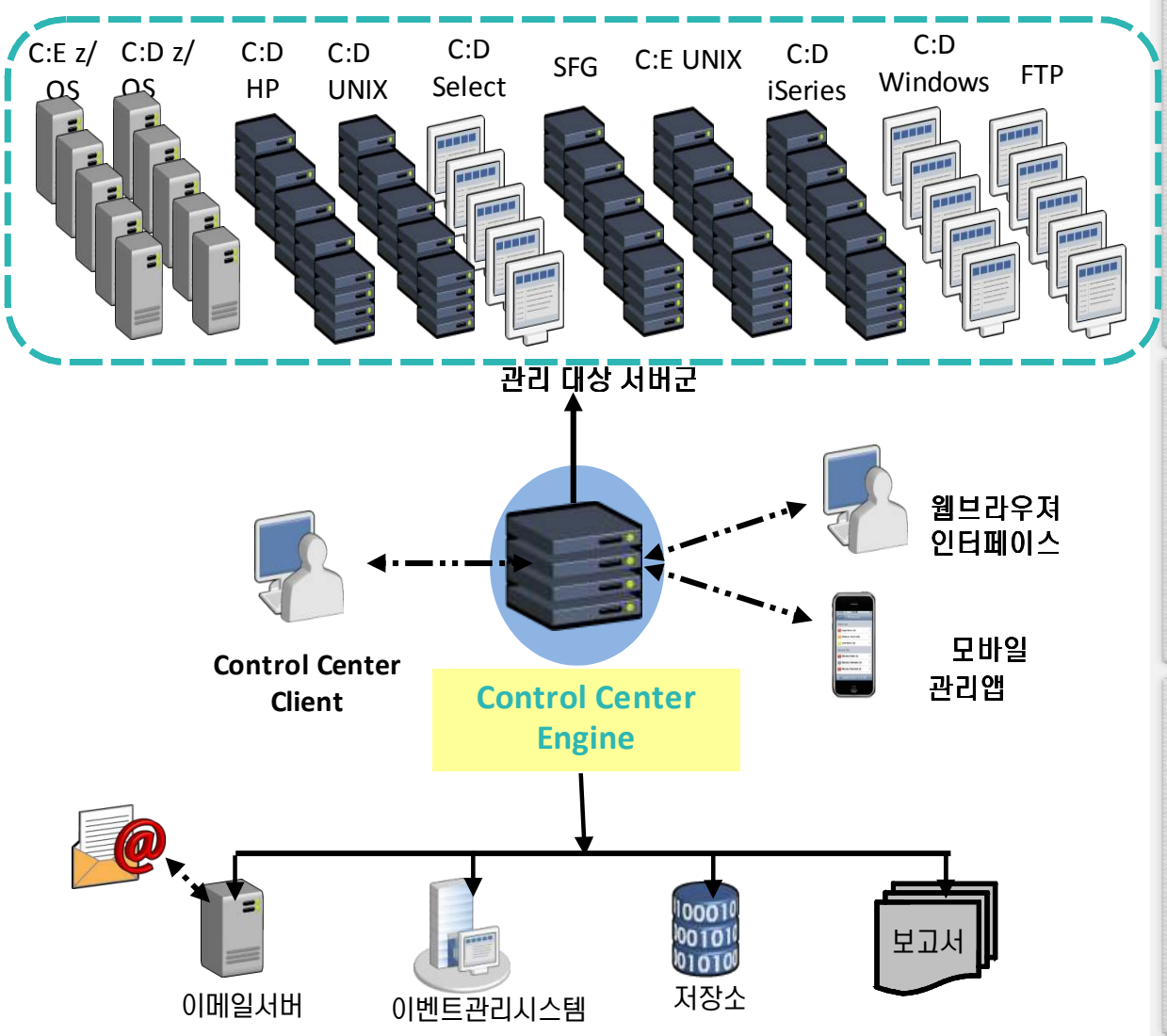
대외기관 DMZ 보안 : Sterling Secure Proxy



- Reverse Proxy 기능을 이용한 고수준 DMZ 보안
- In Bound 방화벽 포트 오픈 불필요
- Connect:Direct와 완전한 연동
- 지원 보안 알고리즘
  - SSL ,TLS, STS, DES,3DES,
  - SHA, AES, DSA, RC4
  - PGP Integration & Key Mgt
- 다중절차 인증(Multifactor Authentication)
- DMZ 세션 Termination
- DMZ에 어떠한 데이터도 저장되지 않음
- SSP를 위한 설정정보는 내부시스템에 저장됨
- 보관 데이터 암호화
- 역할기반 접근제어

© 2011 IBM Corporation

중앙집중 관리/모니터링 도구 : Sterling Control Center



Service Level Manager

파일전송 상황에 대한 SLA관리

- 예외상황 관리
- 능동적인 알림 기능
- 규칙, 이벤트, 스케줄링
- 보고서

CD Asset Manager

중앙 집중 관리 및 모니터링

- 라이센스 키 보관 및 분배
- 제품 설치 노드 찾기 및 파일전송 네트워크 매핑

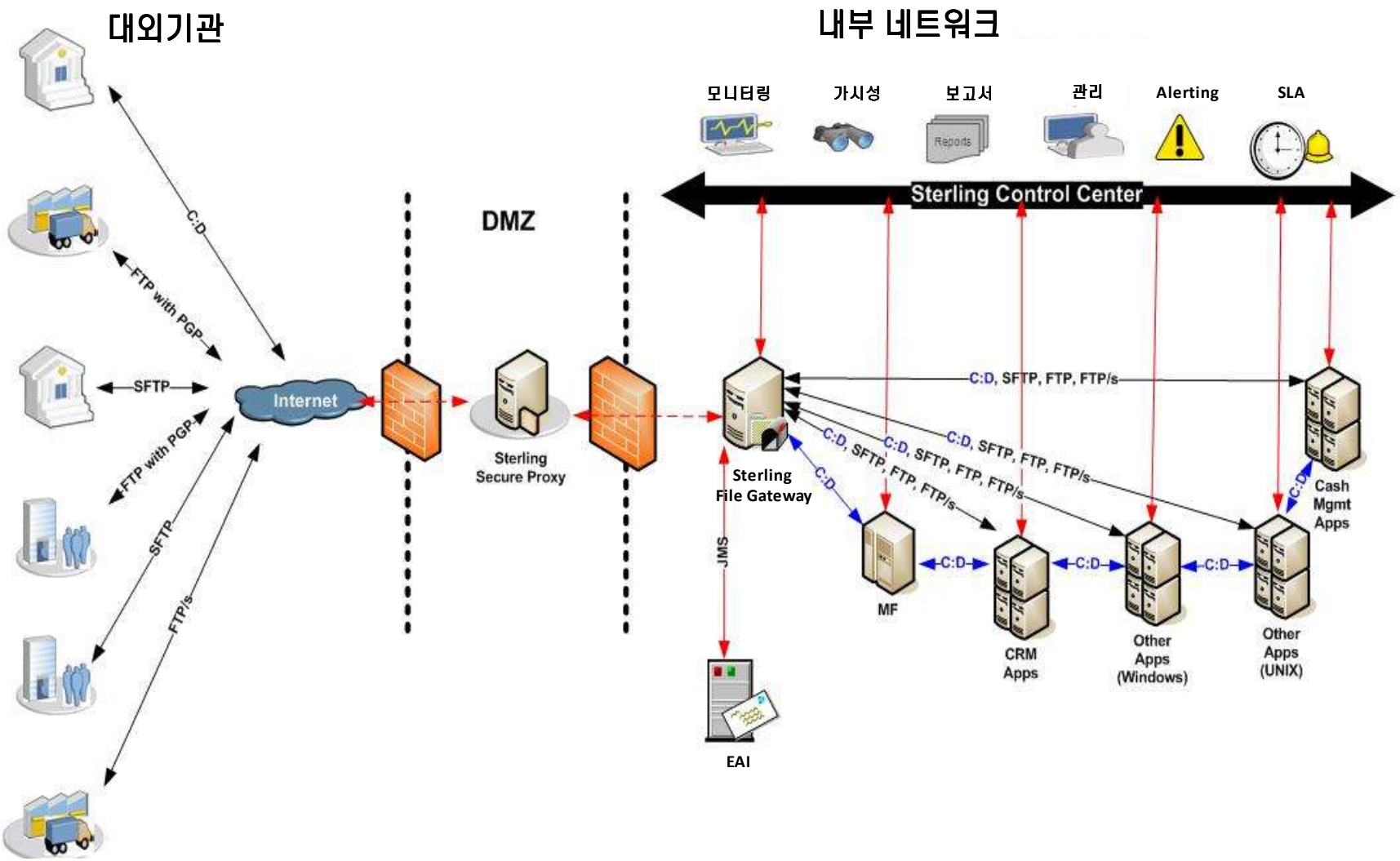
CD Configuration Manager

환경설정, 감사정보, 배포정보의 중앙관리

- 커뮤니케이션 패스 와 프로토콜 설정 값.
- 접속 및 보안 권한관리Secure+ 관리

© 2011 IBM Corporation

Sterling MFT 제품군 활용 예시



© 2011 IBM Corporation

산업군별 활용영역

A2A: Application to Application,내부 시스템 연계
B2B: Business to Business,대외기관 연계

분류	A2A (Connect:Direct,FTP+,Control Center)	B2B (Sterling File Gateway, Secure Proxy)
금융권 (은행,카드사,보험사,금융기관등)	◦메인프레임를 중심으로 한 주요 업무서버(UNIX,Windows) 연계를 위한 **표준 파일전송 인프라로 활용** 고객사례 : 국민은행등 •차세대등 신규프로젝트 진행 시 EDW,CRM등 파일전송이 꼭 필요한 업무시스템 구축 시 활용 • •카드사, VAN사(예:NICE,KICC,KSNET), 대형가맹점은 PCI-DSS규제를 받음. (PCI-DSS:신용카드 정보에 대한 보호규제) •개인정보보호법등 개인정보보호를 위하여 금감원등에서 내부데이터 보안에 대한 기술적 준비를 권고하고있음. 내부시스템간에도 중요한 내용의 **파일전송시 암호화하여 전송할** 것등	◦ 파일 전송을 통한 대외기관 연계 * 업무팀 단위로 FTP서버나 Socket으로 되어 있음(전송속도, 관리, 신규추가 시 과도한 시간,보안이슈등) * 은행 <-> 카드사, 은행<->금융기관,카드사<->VAN사, 카드사<->대규모 가맹점(xx마트)등 파일연계가 많음 * 전송내용은 다양함

© 2011 IBM Corporation

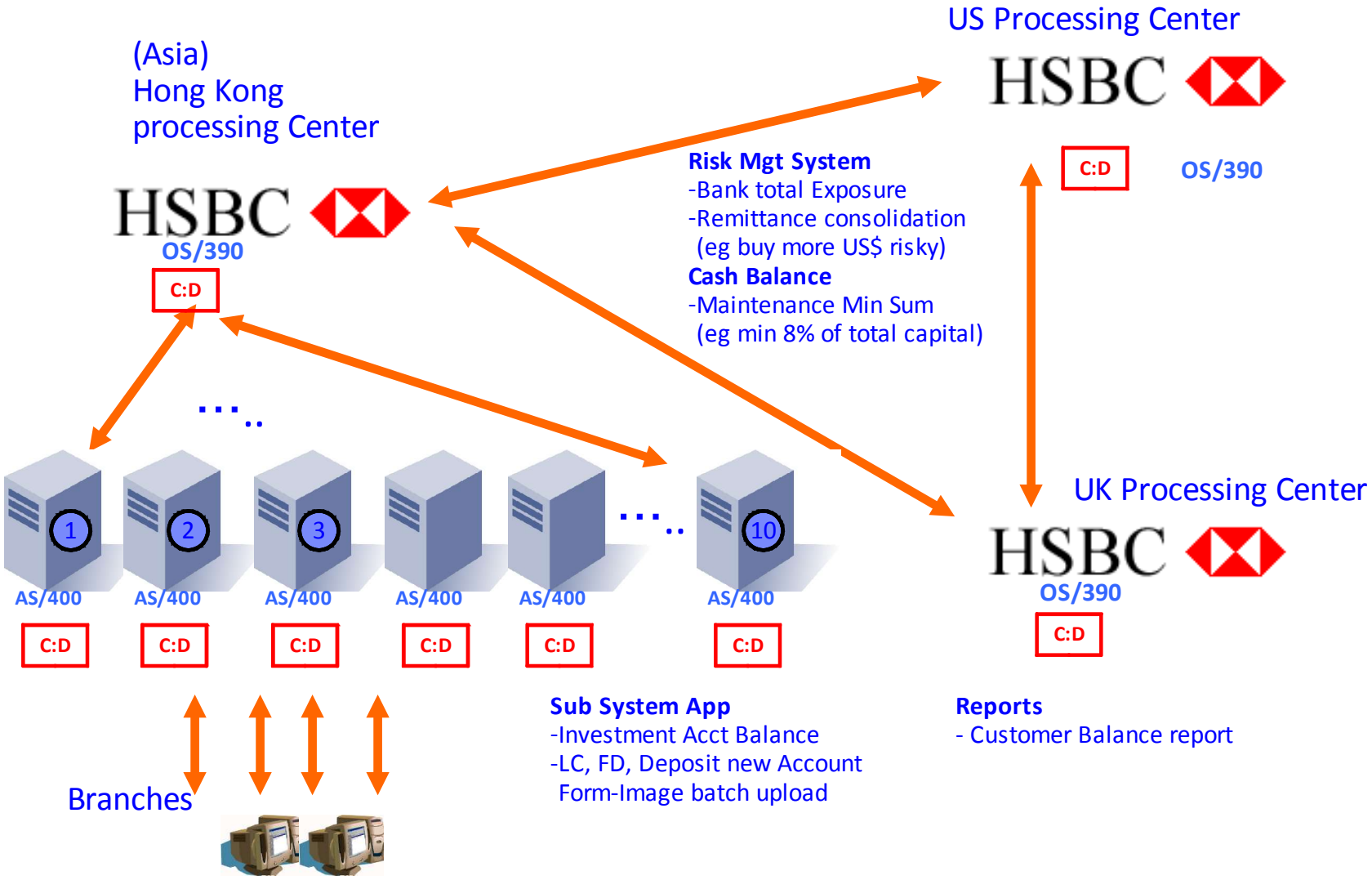
산업군별 활용영역

A2A: Application to Application,내부 시스템 연계
B2B: Business to Business,대외기관 연계

분류	A2A (Connect:Direct,FTP+,Control Center)	B2B (Sterling File Gateway, Secure Proxy)
통신,전력	M/F(z/OS)를 중심으로 한 주요 업무서버 (UNIX,Windows) 연계를 위한 **표준 파일전송 인프라 제품으로 활용** 차세대등 신규프로젝트 진행 시 EDW,CRM등 파일전송이 불가결한 업무시스템 구축 시 제안 빌링정보의 어플리케이션간 전송(DW,CRM,빌링, 등)	청구서인쇄를 위하여 아웃소싱업체에 청구정보 전송 (대량데이터, 보안유지)
제조(자동차,전자,반도체등등)	대기업군인 경우 상당히 많은 서버군을 보유하고 있으며 서버간 파일 업무연계가 다양함. 통합관리, 보안, 전송모니터링, 감사등을 위한 목적으로 **표준 파일전송 인프라 제품으로 활용** 차세대등 신규프로젝트 진행 시 EDW,CRM등 파일전송이 불가결한 업무시스템 구축 시 제안 CNC Machine 데이터 수집 전송 제조 공정 모니터링 데이터 수집전송 대용량 BOM, CAD 파일 송수신	협력사, 고객사 등과 각종 파트도면, 고장수리 매뉴얼, 제품 카달로그 데이터, 가격정보등 정보교환 Global 기업의 경우 해외 협력사/고객들과 저속인터넷망을 이용하여 송수신-전송속도 향상 보안 이슈가 있는 고객

© 2011 IBM Corporation

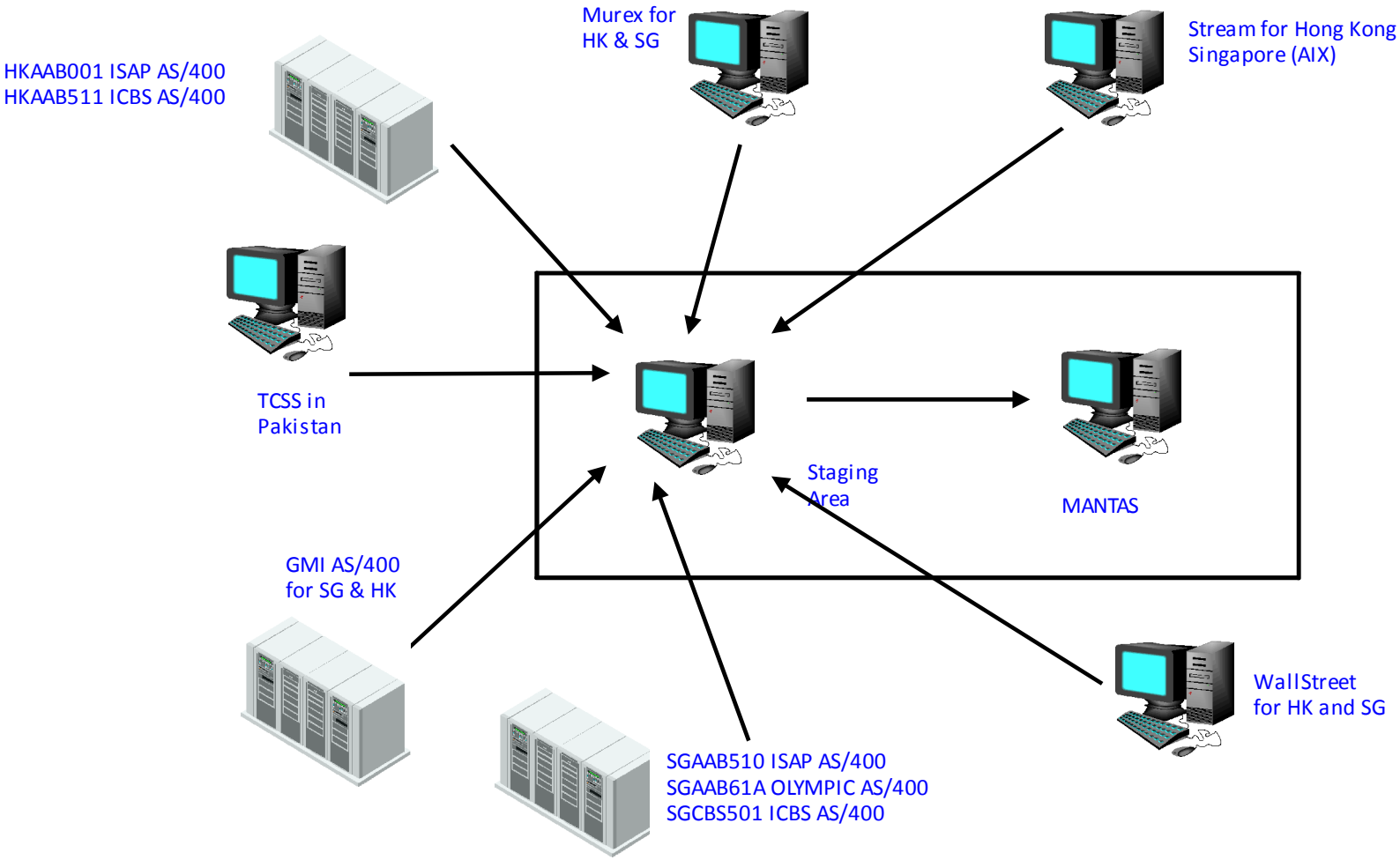
Connect:Direct Case Study – 해외(HSBC Global deployment)



© 2011 IBM Corporation

Connect:Direct Case Study – 해외(ABN-AMRO)

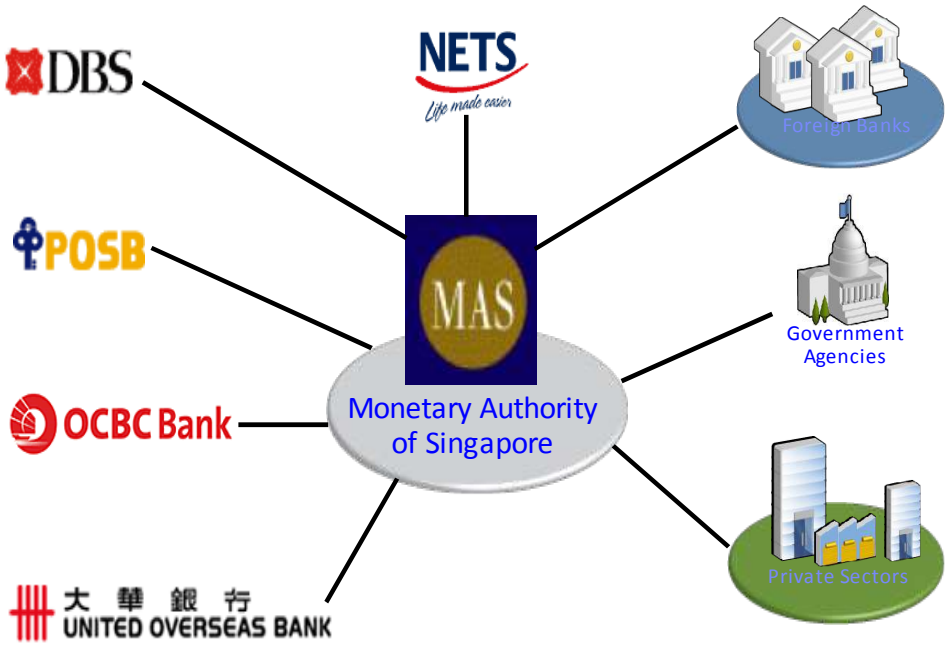
자금세탁방지프로젝트(Anti-Money-Laundering Project)



© 2011 IBM Corporation

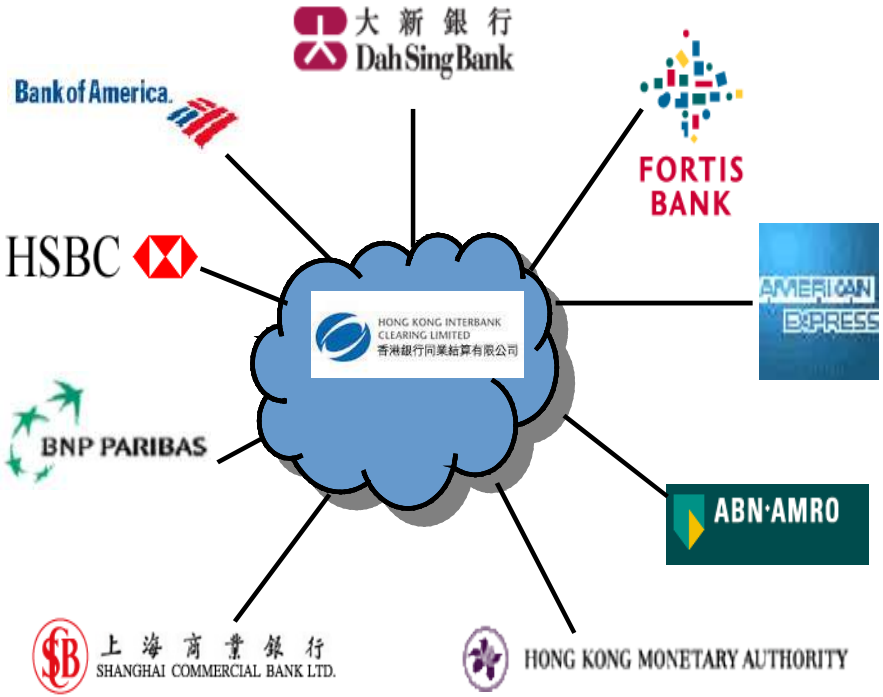
Connect:Direct Case Study – 해외(Secure HUB for Inter-Bank)

은행, 금융기관등을 연계하는 허브역할을 담당하는 기관의 안정적 데이터전송 표준



Monetary Authority of Singapore

Hong Kong Inter-Bank Clearing Limited



© 2011 IBM Corporation

도입 후 기대효과

구분	도입 전	도입 후
안정적인 데이터 전송	Mission Critical한 데이터 전송에 있어서 목적지까지 요구되는 시간 내에 전송이 확실하게 보장되어야 함.	자동 세션 재접속, CheckPoint Restart 보장되는 데이터 전송으로 인하여 데이터 전송의 안전성과 신뢰성을 확보할 수 있으므로 시장에서의 믿음이 증대될 것입니다.
운영효율 극대화	스크립트 지원에 의한 후속작업 자동화와 잡 스케줄러와의 연계를 통한 대량 Batch 전송 자동화가 요구됨.	대량 배치 전송 시, 잡 스케줄러와의 연계 및 강력한 스크립트 기능으로 즉각적인 후속작업 처리가 가능해짐으로 인해 다양한 업무 시스템간 협업의 자동화를 구현할 수 있습니다.
업무개발 용이	업무개발 의한 잦은 프로그램 개발 요구 제거 및 전송 스크립트만 Call해주는 방식으로 간편한 전송업무 개발이 요구됨.	추가업무 구성 및 적용 시 재 프로그래밍이 필요 없이 간단하고 빠르게 처리 가능해지며, 업무 개발 개발 시 C:D의 전송 스크립트만 Call해주면 되므로 전송업무 개발이 매우 쉬어짐.
보안 강화	FTP 사용으로 인한 ID/PW 노출 위험 제거 및 보안 강화 요건 충족이 요구됨	강력한 보안 기능으로 FTP 사용에 따른 위험성을 없앨 수 있으며, 데이터 전송에 대한 금융감독원 권장사항을 준수할 수 있습니다.
전송 모니터링 관리	전송 현황 파악 및 전송 실패 시 즉각적인 Alert 및 로그를 통한 정확한 원인 규명 및 신속한 후속 조치가 요구됨.	데이터 전송 작업에 대해 진행 현황의 전구간 상세 모니터링과 리포팅 및 관리가 가능해짐으로 인해 신속하게 오류를 탐지할 수 있으므로 즉각적인 복구기능을 구축할 수 있습니다.

© 2011 IBM Corporation

감사합니다

© 2011 IBM Corporation