물리적으로 분리된 네트워크간 데이터 전송을 위한 자료교환시스템 구현

한영섭, 김정수
국방기술품질원 정보체계실
e-mail : {yshan, jskim}@dtaq.re.kr

Data Exchange System Implementation for Data Transmission between Physically Disconnected Networks

Youngsub Han, Jungsoo Kim
Computer & Information Management Department,
Defense Agency for Technology and Quality

요 약

중요한 정보를 보유하고 있는 인트라넷 서버의 보안을 강화하기 위해 공공기간에서는 최근에 인터넷과 인트라넷을 물리적으로 분리하여 운영하고 있다. 그러나 물리적으로 분리된 네트워크로 인해 서버간의 데이터 전송에 어려움이 발생하였다. 사용자들이 인터넷 자료를 인트라넷에서 사용하고 싶을 때 또는 그 반대의 경우에 자료교환이 불편하고 처리시간도 많이 소요되었다. 이 문제를 해결하기 위해 분리된 인터넷과 인트라넷간에 사용자들이 손쉽게 자료를 교환할 수 있는 시스템 개발이 필요하였다. 본 논문에서는 분리된 네트워크간에 대용량 파일의 효과적인 송수신 및 e-mail 을 발송할 수 있는 자료교환 아키텍처를 제안하고, 구현한 내용을 다루었다. 자료교환시스템을 구현함으로써 사용자에게 사용 편의를 제공하였고, 자료교환을 위한 행정처리 시간도 감소되었다.

1. 서론

최근에 정보보호는 기업 및 공공기관에서 중대한 관심사가 되었다. 선점기술에 관한 정보유출은 기업의 흥망을 좌우할 수 있고, 개인정보의 유출은 개인에게 피해를 줄 뿐만 아니라 기업 및 기관의 신뢰에도 큰 영향을 미친다. 이에 기업 및 공공기관에서는 정보보호를 위해 방화벽, 웹 방화벽, IPS(Intrusion Protection System), IDS(Intrusion Detection System) 등 정보보호 제품에 많은 비용을 투자하여 해킹 및 불법 정보유출을 방지하고 있다.

중요한 자료를 보유한 인트라넷 서버를 해킹으로부터 보호할 수 있는 강력한 방법은 인터넷과 인트라넷을 물리적으로 분리하는 것이다. 중요 정보는 분리된 인트라넷에서만 유통하게 하여 인터넷에 연결되어 발생될 수 있는 해킹요소를 완전히 차단할 수 있다. 해킹으로부터 개인정보 등 중요 데이터를 보호하기 위해 우리나라에서는 2008 년 이후부터 공공기관에서 인터넷과 인트라넷을 물리적으로 분리하는 사업을 추진하고 있다. 군 관련기관은 네트워크 구축 초기부터 인터넷과 인트라넷을 물리적으로 분리 운영하고 있다.

물리적으로 분리된 네트워크로 인해 보안은 강화되었지만 인터넷에서 인트라넷으로 또는 그 반대의 경우로 자료를 교환하는데 있어서는 불편을 초래하였다. 사용자가 인터넷에서 확보한 자료를 분리된 인트라넷으로 가져오기 위해서는 사용 허가된 USB 저장장치 등의 보조기억매체를 이용해 수동으로 자료를 복사해 이동해야 한다. 또한 인트라넷 자료를 인터넷 메일로 발송하기 위해서는 자료의 불법유출 방지를 위해 자료를 보조기억매체에 복사하여 자료반출에 대한 보안담당부서의 허가 및 자료 복호화 등의 절차를 거쳐야 한다. 인터넷 서버에서 수집된 자료를 인트라넷 서버로 가져오거나 그 반대의 경우에도 데이터 전송이 불편하고, 처리시간도 많이 소요되었다. 이에 따라 사용자들에게 자료 송수신의 편리함을 제공하고, 불법 자료유출을 방지하며, 전송시간을 단축할 수 있는 효과적인 데이터 전송방법이 필요하였다.

본 논문은 물리적으로 분리된 네트워크간에 대용량 데이터를 송수신할 때 보안성 및 데이터 신뢰성을 확보하고, 사용자에게 사용 편리를 제공하며, 데이터 전송속도를 향상시킬 수 있는 자료교환시스템 구현에 대해 다루었다. 논문의 구성은 다음과 같다. 2 장에서 분리된 네트워크간의 데이터 전송방식과 데이터 전송을 위한 하드웨어 발전사 및 아키텍처를 고찰하였다. 3 장에서는 대용량 파일 전송 및 e-mail 발송을 위한 아키텍처의 설계, 구현을 기술하였고, 4 장에서는 결론을 도출하였다.

2. 관련 연구

2.1 분리 네트워크간 자료교환장치 발전 동향

물리적으로 분리된 네트워크 간에 자료를 교환하기

위해서는 파일 및 데이터를 전송하는 장치가 필요하였다. 분리된 네트워크간에 자료를 전송하는 장치는 초기에 보조기억매체를 사용하는 단계를 시작으로 하여 다음과 같은 단계를 거쳐 발전되어 왔다[1].

- 1 세대: 보조기억매체를 이용한 Off-Line 방식
- 2 세대: 타이머를 이용한 네트워크 자동절체 스위칭 방식
- 3 세대: 프로그램에 의한 네트워크 자동절체 스위칭 방식
- 4 세대: SAN(Storage Area Network)을 이용한 자료전송 방식

1 세대는 원시적인 자료전송 방식으로, 외부자료를 내부에 전송할 방법이 시스템적으로 구축되지 않은 상황에서 자료를 송수신하기 위해 수작업으로 보조기억매체를 이용하여 데이터를 전달하는 Off-Line 자료 전송방식이다. 수작업에 의존하므로 DB 및 파일을 전송하는 작업이 불편하고, 업무처리 절차가 여러 단계를 거쳐 복잡하였다.

2 세대는 타이머를 이용한 네트워크 자동절체 스위치 방식이다. 폐쇄 네트워크 중간에 연동서버를 두고 타이머 스위치를 통해 연동서버와 인트라넷 서버가 연결되어 데이터가 전송되고, 정해진 시간이 지나면 연동서버와 인터넷 서버가 연결되어 데이터가 전송되는 방식이다. 자동절체 스위치 장치는 인터넷과 인트라넷간의 연결을 물리적으로 분리하기 위해 필요하였다. 그러나 타이머를 이용해 정해진 시간에 네트워크가 전환됨에 따라 자료 전송량이 많을 경우 자료전송 중에 데이터 손실이 발생할 수 있었고, 자료 전송량이 적을 경우 전송작업이 끝나도 정해진 시간간격 동안은 네트워크 전환이 이루어지지 않아 대기시간이 발생하였다.

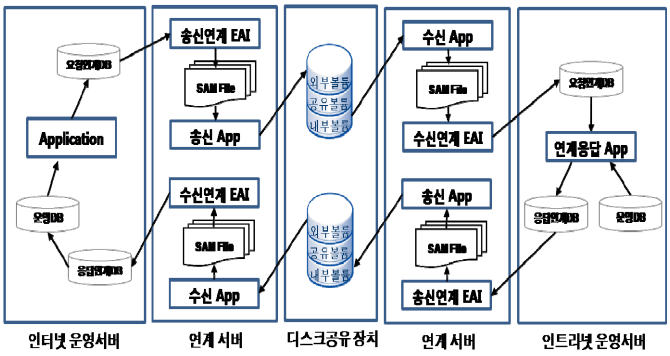
3 세대에는 2 세대의 문제점을 해결하기 위해 타이머 스위치 대신에 프로그램을 이용하여 자동절체를 수행하였다. 프로그램을 이용한 자동절체 스위칭 방식은 인터넷서버-연동서버-인트라넷서버 간의 네트워크 전환을 2 세대의 물리적인 타이머가 아닌 프로그램을 이용하여 자동절체 스위치를 조작할 수 있도록 개선한 것이다. 3 세대에는 작업이 완료되는 시점에 네트워크를 자동으로 전환하여 2 세대의 발생 가능한 데이터 손실을 방지하였고, 데이터 전송 대기시간을 줄여 데이터 전송의 효율성을 향상시켰다.

4 세대는 스위치를 이용하는 방식 대신에 최근 등장한 SAN 스토리지 장치를 이용한 데이터 교환 방식이다. 서버와 스토리지 장치를 Fiber Channel 로 연결하는 방식으로 인터넷과 인트라넷간의 네트워크를 분리하여 보안을 강화하였고, SAN 을 이용함으로써 데이터의 전송속도도 향상시켰다. SAN 을 이용하여 데이터를 저장하는 방식은 데이터 보안을 위해 CKD (Counter Key Data)방식을 사용하였다. 스토리지에 저장하는 방식은 Unix 에서 사용하는 FBA(Fixed Block Address) 방식의 저장방식이 아니라 CKD 방식을 사용하기 때문에 일반적인 Unix 또는 Windows 시스템에서는 저장소의 데이터에 접근할 수 없다.

본 논문은 4 세대 장비를 기반으로 데이터 전송 아키텍처를 설계하였다. SAN 스토리지 장비는 거의 실시간으로 자료를 송수신할 수 있는 장점이 있어 최근에 많이 사용되고 있다.

2.2 분리된 네트워크간 데이터 전송 아키텍처

SAN 스토리지 장비와 EAI(Enterprise Application Integration)를 기반으로 분리된 네트워크 간에 DB 데이터의 보안성과 신뢰성을 확보하기 위해 논문[1]에서 그림 1 과 같은 데이터 전송 아키텍처를 제안하였다. 이 아키텍처는 인터넷에서 인트라넷의 DBMS 에 있는 데이터를 활용하고자 했을 때 인터넷에서 요청한 자료를 인트라넷에서 검색하여 그 결과를 인터넷으로 전송해 주는 아키텍처이다. 이 아키텍처에서 데이터 전송의 한 방향을 활용하면 인터넷에서 획득한 정보를 인트라넷의 서버로 전송하여 사용자들에게 획득한 정보를 제공할 수 있다.



(그림 1) 분리 네트워크간 데이터 전송 아키텍처[1]

다양한 DBMS(Data Base Management System), 전송 프로토콜 등으로 개발된 애플리케이션의 통합을 용이하게 하고자 EAI 가 출현하게 되었다[3]. EAI 는 새로운 미들웨어를 이용해 비즈니스 프로세스를 중심으로 기업 내 각종 애플리케이션의 상호연동이 가능하도록 통합하는 솔루션이나 방법을 말하는데, 이는 시스템 간의 직접적인 의존도를 줄이고 시스템의 이식성 및 적응성을 향상시키며, 시스템 통합을 위한 복잡도를 줄일 수 있는 장점이 있다.

그러나 [1]에서 제안한 아키텍처를 구현하는 과정에서 WAS(Web Application Server)에서 실행되는 EAI 서버의 부하가 높을 경우, EAI 솔루션의 소켓방식으로 데이터를 전송하면 가끔 대용량의 파일 전송이 실패하는 문제점이 발생되었다. [2]에서 주장했듯이 시스템 품질의 경우 EAI 도입 패키지 특성 요인이 서비스 품질에 큰 영향을 미쳤다.

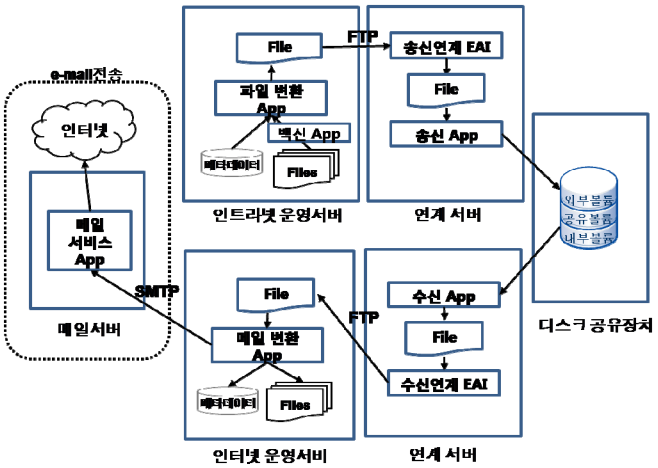
3. 자료교환시스템 설계 및 구현

3.1 대용량 파일 전송 아키텍처 설계

분리된 네트워크간에 대용량 파일을 효과적으로 전송하기 위해 그림 2 와 같이 아키텍처를 제안하였다. 대용량 파일을 전송할 때 서버의 메모리 사용량이 많

을 경우 소켓방식은 서버의 메모리를 많이 차지하여 데이터 전송이 실패하는 경우가 발생하였다. 이를 해결하기 위해 본 논문에서는 소켓방식을 이용하는 대신 FTP 방식을 이용하여 데이터를 전송하는 아키텍처를 제안하였다.

그림 2 의 점선으로 표시한 e-mail 전송부분을 제외한 아키텍처가 대용량 파일 전송 아키텍처 설계 부분이다. 이 아키텍처는 파일과 DB 의 메타 데이터를 파일 변환 프로그램을 통해 한 개의 파일로 묶어서 EAI 의 FTP 방식을 통해 데이터를 전송하도록 설계하였다. 전송 파일을 한 파일로 묶어 처리함에 따라 EAI 작업의 복잡도를 줄일 수 있었다. 그리고 파일 변환시 서버에서 바이러스를 점검하는 백신 프로그램을 수행한 후에 파일이 통합되도록 설계하였다. 이는 바이러스에 감염된 파일이 분리 네트워크간에 전송되지 못하도록 하여 바이러스 침해방지 및 보안을 강화하였다



(그림 2) 자료교환시스템 아키텍처

3.2 e-mail 전송 아키텍처 설계

분리된 네트워크에서 메일을 보내는 메일전송 아키텍처는 대량파일 전송 아키텍처와 기본 구조는 같으나 차이점은 그림 2 의 점선으로 표시한 부분과 같다. 인트라넷에서 송신된 자료가 인터넷 애플리케이션 서버에 도착하면 이 자료를 메일발송 형태로 전환한 후 메일서버에 데이터를 전달하여 메일서버에서 메일이 발송되도록 설계하였다. 인터넷 애플리케이션 서버에서 자신의 SMTP 서비스를 통해 메일을 발송할 수도 있으나, 수신측 메일서비스 정책에 따라 스팸 메일로 분류될 가능성이 있어 송신자 메일주소와 같은 도메인의 메일서버를 통해 메일을 보내도록 설계하였다.

3.3 구현 및 고찰

물리적으로 분리된 네트워크간 자료교환을 위해 그림 2 에서 제안한 대용량 파일 전송 아키텍처와 e-mail 아키텍처 설계를 이용하여 자료교환시스템을 개발하였다. 자료교환시스템은 인터넷용 시스템과 인트라넷용 시스템으로 구분되어 2 대의 서버에서 운영된다. 인터넷용 시스템은 사용자들이 획득한 파일을 인트라넷으로 송신할 수 있는 기능이 있고, 인트라넷 시스템에는 인터넷 자료 수신 및 인트라넷 자료를 e-mail 로 발송하는 기능이 있다. 구현된 주요 기능은 표 1 과 같다.

<표 1> 자료교환시스템 구현 기능

구 분	주요 기능
인트라넷 시스템	○로그인: 포탈시스템에서 Single Sign On ○인터넷 자료 수신: 목록보기, 파일 다운로드 ○인트라넷 자료 송신: 인터넷 e-mail 발송내용 작성, 결재요청, 부서장 결재 ○자료교환 내역 모니터링 ○시스템 관리: 최대 전송량 설정 등
인터넷 시스템	○로그인: 포탈시스템 계정으로 로그인 ○인터넷 자료 송신: 파일 업로드 ○인터넷 메일 발송 ○시스템 관리: 최대 전송량 설정 등

기능을 구현할 때 EAI 솔루션을 이용하여 데이터 송수신 모듈을 개발함으로써 개발기간 및 공수를 줄일 수 있었고, 데이터 송수신의 안정성을 확보할 수 있었다. 또한 파일 다운로드, 업로드는 상용 컴포넌트를 이용하여 개발함으로써 시스템의 신뢰성을 높였다.

시스템을 구현한 후 인터넷에서 인트라넷으로 파일 전송시간을 측정해 본 결과, 50M 는 평균 7 초, 100M 는 15 초, 500M 는 58 초의 전송시간이 소요되었다.

4. 결 론

본 논문에서는 물리적으로 분리된 인터넷과 인트라넷 네트워크간의 대용량 파일을 안정적으로 전송하기 위한 아키텍처를 설계하였고, 자료교환시스템을 구현하였다. 자료교환시스템 구현을 통해 보조기억매체를 이용해 수작업으로 이루어지던 자료교환이 정보시스템을 이용해 자동화됨에 따라 사용자에게 자료교환의 편의를 제공하였고, 행정처리 시간도 절약되었다.

향후 발전방향으로는 사용자가 분리 네트워크 상황을 느끼지 못하도록 데이터를 실시간으로 전송할 수 있는 아키텍처 및 하드웨어의 연구가 필요하다.

참 고 문 헌

[1] 김재우 등 4 명, “분리된 네트워크간 데이터전송의 보안성 향상을 위한 아키텍처 설계”, 한국정보보호학회 동계학술대회 논문집, Vol. 19, No. 2, 2009.

[2] 임정현, “EAI 시스템의 성과에 영향을 미치는 요인에 관한 연구”, 한국외국어대학교 경영정보대학원 석사학위 논문, Feb. 2003.

[3] Du, Wuliang Peng and Li Zhou, “Enterprise Application Integration: an Overview”, IITA Workshop, 2008.

[4] Khubaib Ahmed Qureshi, “Enterprises Application Integration”, 2005 International Conference on Emerging Technologies, September, 2005.