가상화를 이용한 논리적, 물리적 망분리 구축

이용희* · 유승재**

요 약

정보 통신의 발전으로 공공기관과 기업에서는 인터넷 및 인트라넷을 이용하여 업무 연속성을 활용하고 있다. 이러한 환경에서 공공기관과 기업에서는 내부 정보의 유출에 대한 보호를 위해 많은 솔루션과 어플라이언스 장비들을 도입하고 있다. 그러나 이 역시 외부 네트워크와 연결이 되어 있어 완벽한 정보유출을 방지하기에는 역부족이다. 이를 극복하기 위해 내부 망과 외부 망으로 분리가 필요하다. 본 논문에서는 가상화를 이용하여 물리적인 망분리와 논리적인 망 분리를 적용하여 망 구성을 하고 그에 따른 기술적인 검토 및 망 분리에 대해 다양한 방안을 제시하였다.

The Construction of Logical, Physical Network Separation by Virtualization

YongHui Lee* · SeungJae Yoo**

ABSTRACT

With the development of information and communication, public institutions and enterprises utilize the business continuity using the Internet and Intranet. In this environment, public institutions and enterprises is to be introduced the number of solutions and appliances equipment to protect the risk of leakage of inside information. However, this is also the perfect external network connection is not enough to prevent leakage of information. To overcome these separate internal and external networks are needed. In this paper, we constructed the physical and logical network separation is applied to the network using the virtualization and thus the network configuration and network technical review of the various schemes were proposed for the separation.

Key words : 가상화, 논리적 망분리, 물리적 망분리, Virtualization, Logical network separation, Physical network separation

접수일(2014년 2월 6일), 수정일(1차: 2014년 3월 19일), 게재확정일(2014년 3월 24일)

* 신성대학교 정보지원센터 소장, 교양학부, 제철산업과
** 중부대학교 정보보호학과

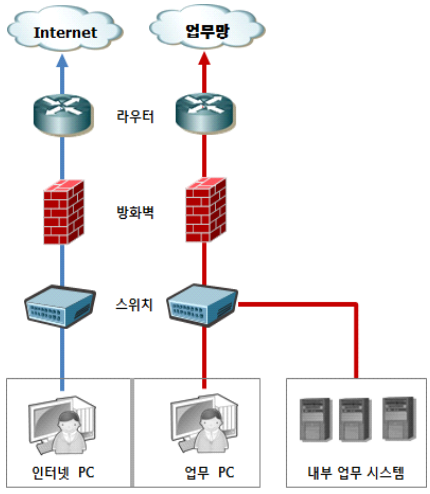
1. 서 론

정보통신의 발전으로 인하여 업무 지역이 서로 달라도 그에 대한 지리적 제약사항이 해소가 되고 있다. 특히 인터넷의 발전으로 더욱 편리한 업무환경으로 변화가 되고 있으며, 기업 및 관공서, 그 외 모든 곳에서 인터넷을 활용한 외부와의 업무 연속성을 확보하고 있다. 이러한 발전은 업무환경의 효율성 증대 효과를 가져 오게 되었다. 하지만 이러한 장점에 반해 외부와의 연결은 내부 정보의 유출이라는 역효과를 가져오기도 한다. 인터넷에 연결된 망은 외부의 유해한 요소로부터 많은 위험에 노출되게 된다. 악의적인 해커와 악성 바이러스, 스파이웨어 등이 대표적이며 외부적인 위험요소 외에도 내부적으로도 산업 스파이나 사용자의 실수로 인한 내부 정보의 인터넷 유출이 발생하기도 하며, 이러한 피해는 점차 늘어나는 추세이다. 즉 외부로부터의 침입 및 악의적인 공격으로부터 안전한 환경을 조성하는 것과 내부 사용자로부터 중요 자료를 보호해야하는 필요성은 계속해서 요구되고 있는 상황이다. 기업과 관공서의 주요 정보를 보호하기 위한 방안으로 정보보안 솔루션이 많이 도입되고 있다. 이메일 보안, DB암호화, 문서 보안, 내부정보 유출 방지, 출력물 보안등 다양한 방안의 솔루션이 제시되고 있으나 원척적인 내부 정보 보호를 위한 업무망과 외부망의 네트워크 분리의 필요성이 부각되었고 [1] 이에 따라 물리적인 망 분리가 요구되어 왔다. IT 기술의 발전으로 가상화 기술이 부각되고 있으며 이를 바탕으로 한 논리적인 망 분리가 제시되고 있다. 본 논문에서는 물리적인 망 분리와 논리적인 망 분리에 각각의 구조 및 구축 방안에 대해 방법을 제시하고 그에 따른 장단점을 비교 분석 하였다.

2. 망 분리

2.1 물리적인 망 분리

물리적인 망 분리는 모든 하드웨어 자원을 망에 따라 추가로 두어 사용을 하는 것을 말한다. (그림 1)에서 보는 바와 같이 망을 구성하는 라우터, 스위치 등 네트워크 장비와 방화벽, 정보보안 솔루션 및 통신 케이블(UTP 케이블, 광 케이블)등이 망의 종류에 따라 분리되어 사용이 되며 사용자의 PC도 망 종류에 따라 인터넷 PC 와 업무 PC를 따로 두어 사용하게 된다. (그림1)



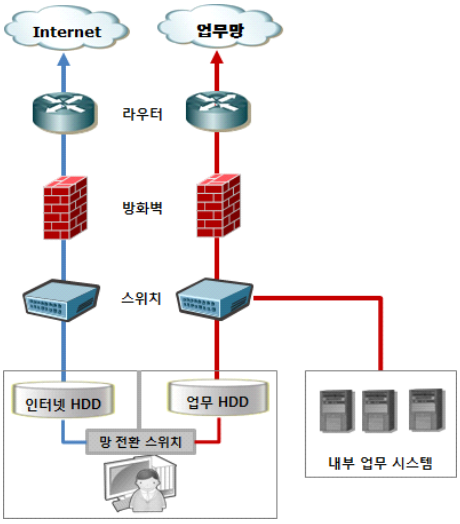
(그림1) 물리적인 망 분리 구성

위와 같이 PC를 각각 사용하는 망 분리는 네트워크상의 연결점이 없어 원천적으로 내부 정보의 인터넷 유출을 방지가 가능하다. 하지만 모든 IT 시스템의 자원이 이중으로 배치되어 사용되기 때문에 구축비용과 유지비용이 많이 소요가 되고 그로 인해 정보시스템을 관리하는 관리자의 업무량이 증가가 되기도 한다. 또한 인터넷을 통한 자료 활용의 불편함으로 업무 효율성 저하 및 선진 IT 시스템 적용이 어렵게 된다.

또 다른 물리적인 망 분리는 사용자 PC 환경만 망 전환 장치를 사용하여 구성 하는 방안이 있다. 하나의 PC에 두 개의 독립적인 저장장치(HDD) 및 그래픽카드 또는 별도의 망분리 PCI(Peripheral Component Interconnect) 카드를 설치하여 인터넷 망과 내부 망 사용시 전환 장치를 이용하거나 소프트웨어적인 망 전환을 통해 각각의 망을 사용하는 방식이다. 그림2는 물리적인 망 전환 스위치를 사용한 구성이며 (그림 3,4)는 별도 망 분리 PCI 카드를 설치하여 소프트웨어적로 망 전환을 사용한 구성이다.

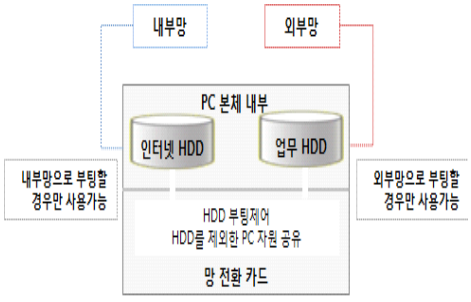
위의 두 가지 방식은 망을 전환시에 PC를 다시 부팅하거나 외부망과 내부망을 동시에 보면서 사용하기

가 어려워 인터넷에서 수집한 정보를 활용한 내부 업무 수행에 있어서는 많은 불편함을 가지게 되며 업무 연속성 및 효율성 저하가 발생하게 된다.

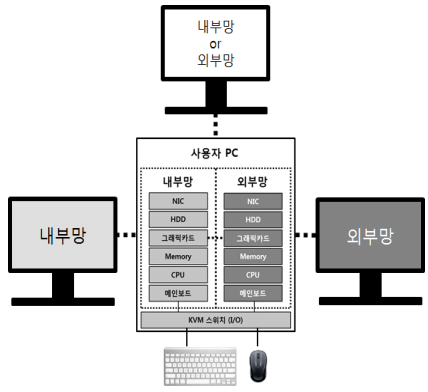


(그림2) 물리적인 망 분리 구성-망 전환 스위치

이러한 불편함을 최소화하기 위해 그림 3, 4와 같이 PC본체 한 대에 PC를 구성하는 메인보드, HDD, 그래픽카드 등 모든 자원을 이중으로 구성하여 동시에 외부망과 내부망 사용이 가능하며 내부에 KVM(Keyboard, Video monitor, Mouse) 스위치 역할의 장치를 구성하여 입출력 장치(모니터/키보드/마우스)만 공유하여 사용자의 편의성을 높이고, 모니터를 망 별로 설치하여 업무 효율성을 더 높일 수 있다.



(그림3) 물리적인 망 분리 구성-망 분리 장치



(그림4) 물리적인 망 분리 구성-듀얼 PC

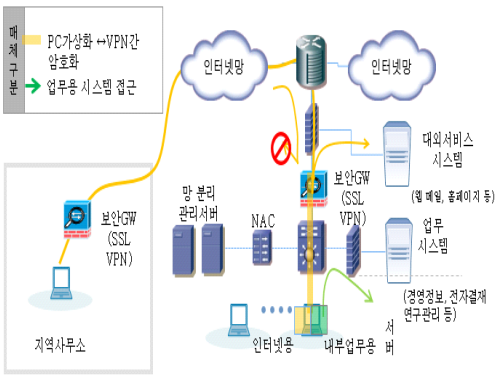
이렇듯 물리적인 망 분리는 가시적으로 완벽한 망 분리를 보여주고 있지만 물리적 망 분리 적용시에는 다음과 같은 위험을 고려해야 한다.

망 분리 후에 내부망과 외부망의 자료 이동 및 공유, 내부망 PC에 외부망 연결시 데이터 유출 가능성, 바이러스에 감염된 이동 저장 장치 사용, 내부망 자료의 인쇄 및 캡처에 따른 정보 유출 가능으로 물리적 망의 분리만을 통한 내부 정보 유출 및 악성코드 방지는 어려우며 추가적인 데이터 암호화, 저장 매체 제어, 출력물 보안 및 사용자 인증과 같은 솔루션을 도입 하거나 위의 사항에 맞는 보호 방안을 마련해야한다. 결론적으로 물리적인 망 분리는 물리적인 분리를 통해 가시성을 가지며 완벽한 망 분리로 높은 보안성과 안정성을 가져 오게 된다. 하지만 망간 데이터 교환이 불편하고 별도의 네트워크 망 구축 과 사용자 단말기의 추가 설치로 도입 및 유지비용의 증가를 가져오게 되며 높은 전력 소비로 그린 IT에 역행하게 되는 단점이 존재하게 된다.

2.2 논리적 망 분리

논리적인 망 분리는 (그림5)에서 나타낸 것과 같이 이미 구축되어 있는 네트워크를 이용하여 가상화 기술을 접목, 하나의 사용자 PC에서 인터넷의 이용과 내부 업무망 사용을 가능하게 하는 기술이다. 주로 가상화 기술을 기반으로 하여 가상화 구성 방식에 의해 인터넷 영역과 내부 영역으로 구분되며 가상화 영역의 망 분리를 통해 1대의 PC에서 업무 영역의 분리와 네트워크 가상화[2,3,4,5]를 이용하여 망 분리를 논리

적으로 구성한다.



(그림 5) 논리적 망 분리 개념도

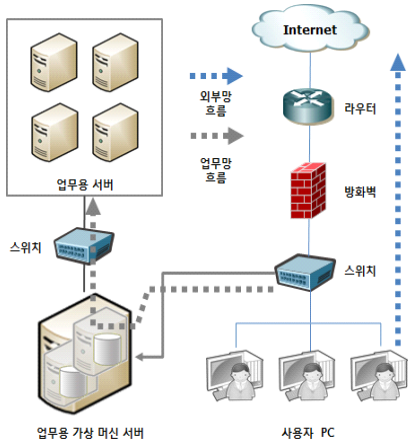
가상화 기반 기술은 사용자 인증을 통한 서버 접속 또는 보안영역 접속방법으로 문서가 생성, 조회되거나 다운로드 되는 일련의 과정이 중앙서버 또는 보안 영역을 벗어날 수 없어 정보 유출을 차단하고 사용자의 이벤트에 대한 이력 관리가 가능하며 기업의 보안 정책에 따라 데이터 및 사용자 관리가 가능하다.

2.2.1 서버기반(Server Based Computing) 망 분리

서버 기반의 논리적 망 분리는 SBC를 활용하여 가상 머신을 탑재한 서버에 접속하여 내부 업무망을 사용하고 인터넷을 사용할 시에는 기존 PC는 환경과 동일하게 이용을 하게 되는 방식이다. VMware 와 같은 가상머신[6,7,8]을 탑재한 서버를 중앙에 두고 각 사용자 PC가 중앙 서버에 접속하여 업무를 처리하는 방식이다. 사용자는 내부 업무처리를 위해 업무용 가상 머신 서버에 접속하여야만 하며 생성되거나 조회한 문서는 중앙 서버를 벗어날 수 없기 때문에 문서의 외부 유출을 막을 수 있다.

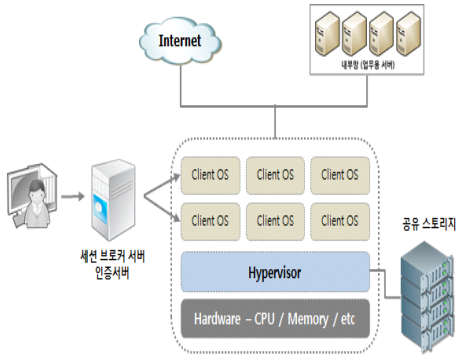
이 방식은 물리적으로 PC가 한 대만 있으면 되고, 각 업무환경을 중앙 서버에서 통제함으로써 유지보수 효율성이 높다. 이는 PC 의 저장장치가 손상되었을 경우 당장 업무 수행이 불가능 해지고, 심각한 경우 데이터 전체의 소실 위험까지 존재하게 된다. 또한 PC를 수리하고 OS를 재설치, 업무용 소프트웨어를 다시 설치하는 시간이 소요가 되고 이 시간 동안 업무는 마비되어 업무의 연속성을 해치게 된다.

하지만 SBC의 경우 PC가 물리적인 손상을 입는다 해도 다른 자리와 새로운 PC가 있으면 즉시 업무 수행이 가능하다. 모든 자료와 업무 환경이 서버에 보관되어 있기 때문이다, 또한 중앙 서버에 접속만 하면 사용이 가능하기 때문에 PC가 아닌 모바일 환경에서도 업무를 처리할수 있다. (그림6)은 이러한 SBC 기반의 논리적 망 분리에 대한 개념도를 나타낸 것이다.



(그림 6) SBC 기반 망 분리#1

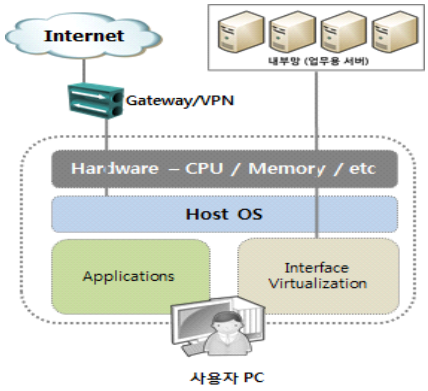
두 번째 서버 기반 가상화 망분리는 그림 7에서와 같이 가상화 서버를 중앙에 두어 각각의 사용자 별 클라이언트 OS를 가상화하여 연결된 사용자의 OS를 구동하여 서버에서 구동되는 가상화된 OS를 사용하는 방식이다.



(그림 7) SBC 기반 망 분리#2

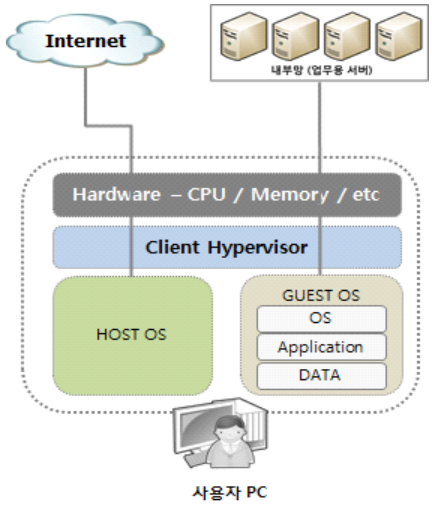
사용자는 세션 브로커 서버와 인증서버를 통해 중앙에 있는 서버에 접속을 하게 되고 서버의 네트웍 설정에 따라 인터넷 망 및 내부망을 사용 할 수 있다. 사용자의 OS 및 애플리케이션을 중앙에서 제어하기 때문에 데이터의 관리 및 통제가 원활하며 유지보수와 업그레이드가 수월한 장점이 있다. 하지만 사용자의 증가에 따른 서버의 성능 저하로 지속적인 성능 향상을 위한 투자비용이 필요하게 된다.

2.2.2 클라이언트 기반 가상화 망 분리



(그림 8) 데스크탑 가상화 기반 망 분리#1

클라이언트 기반 가상화 망 분리는 SBC 기반의 망분리와 마찬가지로 가상화 기반에서 동작을 하지만 서버가 아닌 개인별 데스크탑에서의 가상화 방법이다. NIC를 두 개 사용하여 호스트 운영체제와 가상머신에 각각 할당하고 분리된 망으로 연결하거나 VPN을 통하여 내부망으로 접속하도록 함으로써 망 분리를 실현하는 방식이다. SBC방법과 비교해 볼 때 데이터의 중앙화로 인한 이득과 중앙 통제에 따른 장점이 없는 반면 사용자 PC의 하드웨어 자원을 전부 사용할 수 있는 장점이 있다. 첫 번째 구성 방식은 그림 8과 같이 PC 데스크톱 OS를 가상화하여 Host OS와 Guest OS를 구성하여 각각의 영역에 대해 다른 네트워크를 설정하여 망을 분리한다. 두 번째 구성방식은 그림 9와 같이 클라이언트 하이퍼바이저를 이용하여 두 개 이상의 OS에 별도의 가상 네트워크를 사용하는 방식으로 구분된다. 첫 번째 방식은 두번째 방식과 달리 OS를 추가적으로 필요하지 않고 현재 사용되고 있는 OS 상에 가상의 공간을 생성하고, 가상공간에서 실행된 어플리케이션만 인터넷에 접속되도록 함으로써 망분리를 실현한다. 이 방법은 시스템 자원을 많이 소비하지 않기 때문에 기본의 PC에 얼마든지 적용 가능하여 최소한의 비용으로 망분리를 구축할 수 있다는 장점이 있다.



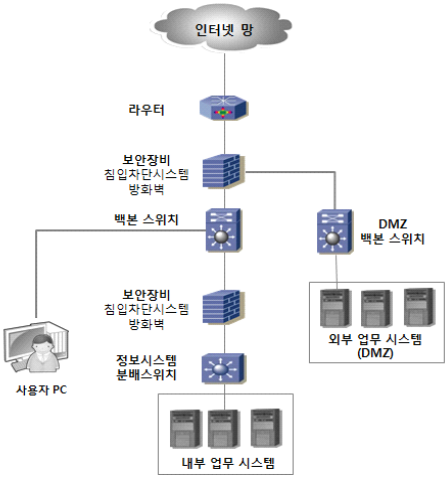
(그림 9) 데스크탑 가상화 기반 망 분리#2

2.3 물리적, 논리적 망분리 구축

2.3.1 물리적 망 분리 구축

기존의 운용 시스템은 (그림 10)과 같이 망의 구분 없이 내부 업무 시스템과 외부 업무 시스템을 사용하고 있으며, 지속되는 사이버 침해 및 해킹 피해사례가 증가하고 중요 데이터의 유출로 이에 물리적인 망 분리를 적용하여 이러한 피해 및 중요 자료에 대한 보호를 하고자 하였다.

사용자 단말기는 듀얼 PC를 사용하여 업무 효율성을 제고 하였고, 네트워크 장비 및 보안 장비는 기존 구성과 동일하게 인터넷용으로 추가 구축을 하였다.

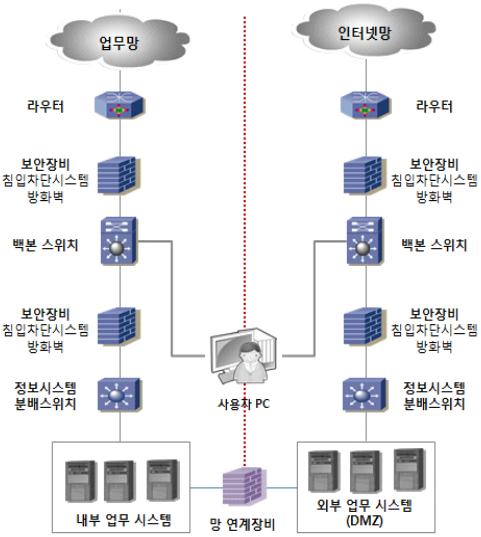


(그림 10) 물리적 망 분리 적용 전 구성

업무망은 인터넷 회선과의 연결을 제거 하고 지역 사무소와 전용회선으로 연결하고 VPN 장비를 통한 지역 사무소와 통신환경을 구성 하였다. 추가 적으로 내부 업무망과 외부 업무망 사이에 데이터를 전송해야 하는 필요성에 의해 망 연계장비를 두어 실질적으로 TCP/IP 통신을 배제한 데이터 전송을 가능하게 하였으며, USB 보안 및 출력물 보안등 외부 저장 매체로 인한 정보 유출을 막고자 정보보호 솔루션을 추가로 구축 하였다. (그림 11)은 최종적으로 물리적 망 분리를 적용한 구성도를 보여 주고 있다.

물리적 망 분리 적용 구성한 내역은 아래와 같다.

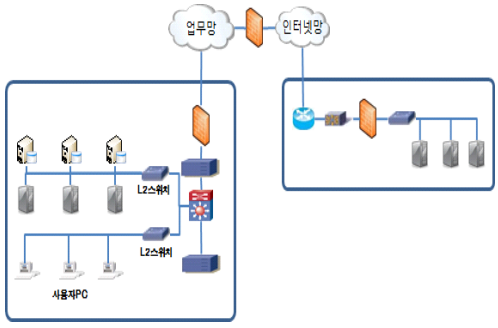
- 인터넷전용 네트워크장비 구축 : 스위치/라우터
- 인터넷 전용 보안 장비 구축 : 방화벽/IPS/망 연계장비
- 보안 솔루션 구축 : 매체제어(USB/외장 HDD) / 출력물보안/문서 암호화/데이터 암호화 솔루션
- 인프라 구축 : 사용자 UTP 케이블/건물간 광 케이블 구성
- 사용자 PC : 듀얼 PC 도입
- 프린터 서버 도입



(그림 11) 물리적 망 분리 적용 후 구성

2.3.2 클라이언트 기반 논리적 망 분리 구축

기존의 시스템 운용은 사용하고 있는 PC 환경을 그대로 사용하고자 하여 클라이언트 기반 가상화를 통한 논리적 망 분리를 적용하여 구성 하였다.

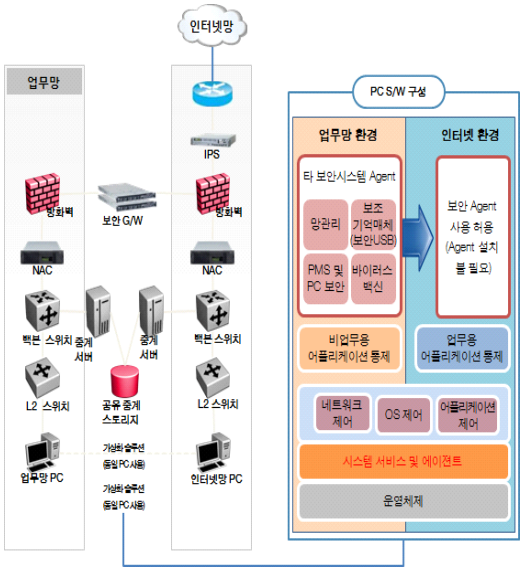


(그림 12) 논리적 망 분리 적용 전 구성

기존 구성은 (그림 12)와 같이 업무망과 인터넷 망의 주 회선을 별도로 구성이 되어 있으며 사용자 PC들은 업무망에 존재하고 인터넷 망을 이용할 시에는 업무망의 모든 네트워크 및 방화벽을 지나서 인터넷 망으로 전송이 되는 방식이며 보안적인 측면을 고려하여 업무망과 인터넷 망 사이에 방화벽을 두어 구성되어 있었다.

(그림 13)은 클라이언트 가상화 기반 논리적 망

분리를 적용한 구성과 사용자 PC의 환경 구성을 보여 주고 있다.



(그림 13) 논리적 망 분리 적용 후 구성

망 구성에서는 기존 네트워크 및 보안 장비를 최대한 활용을 하고, 추가된 장비 및 그 기능은 인터넷 망과 업무망 사이에 보안 G/W 및 중계서버를 두어 망간 데이터 전송이 가능하게 하였고 사용자 PC 환경은 기존에 사용하던 PC를 그대로 활용하여 기존 시스템 위에 서비스를 제어하는 에이전트를 설치하여 네트워크 및 OS, 망 별 어플리케이션을 제어하는 환경을 구축 하였다. 망 전환시에는 소프트웨어적인 망 전환 스위치를 사용하여 망 전환이 이루어지게 하였다.

논리적 망 분리 적용 구성한 내역은 아래와 같다.

- 클라이언트 가상화 솔루션 : 기존 PC에 설치
- 클라이언트 가상화 솔루션 관리 서버 : 업무망에 구성
- 중계서버 : 업무망과 인터넷 망에 설치 및 연계
- 보안 솔루션 구축 : 매체제어(USB/외장HDD)/출력물 보안/문서 암호화/데이터 암호화 솔루션

3. 물리적 망 분리와 논리적 망 분리 비교 결과

2절에서는 물리적 망 분리와 논리적 망 분리에 대해 다양한 구성 방식과 실제 구축 및 적용에 따른 필요 요소 및 구성 방안에 대해 언급하였다. 그에 따른 각 망 분리 결과에 대해 <표1>, <표2>에 나타내었다.

<표 1> 물리적 망 분리 결과

구분	물리적 망 분리		
	PC 2대	망 전환 장치	듀얼 PC
전환시 재부팅	없음	재부팅	없음
보안성	완전한 망 분리 구성으로 안정성 확보		
추가 장치	PC, 네트워크 및 회선	망 전환장치, HDD, 네트워크 및 회선	전용 PC 네트워크 및 회선
주요 장점	물리적 분리 보안	단일 PC상의 망 전환	물리적 분리 보안 단일 PC상의 전환 효과
주요 단점	구축 및 유지비용이 높다.	재 부팅으로 업무 연속성 저하	구축 및 유지비용이 높다.
사용자 현황관리	불가능	불가능	불가능

<표 2> 논리적 망 분리 결과

구분	논리적 망 분리	
	서버기반 가상화	PC 기반 가상화
전환시 재부팅	없음	없음
보안성	인터넷 영역에 대한 보안성 취약	커널과 분리되어 악성코드 감염이 안됨
추가장치	전환서버 및 SBC 솔루션	가상화 솔루션
주요장점	통제 및 관리가 편리함	기존 자원 활용으로 도입비용이 저렴
주요 단점	다양한 S/W 지원의 어려움	다양한 PC 환경 호환성 검증 필요
사용자 현황관리	가능	가능

4. 결 론

본 논문에서는 업무망과 외부망을 분리함으로써 외부의 악의적인 공격 및 해킹으로 인한 내부 주요 정보를 보호하기 위하여 물리적, 논리적 망분리를 구축하였다.

기존의 물리적 운용 시스템은 망의 구분 없이 내부 업무 시스템과 외부 업무 시스템을 사용하고 있어 지속되는 사이버 침해 및 해킹 피해사례가 증가하였다. 이를 해결하고자 업무망은 인터넷 회선과의 연결을 제거 하고 지역 사무소와 전용회선으로 연결하여 VPN 장비를 통한 지역 사무소와 통신환경을 구성 하였다. 내부 업무망과 외부 업무망 사이에 데이터를 전송을 위해 망 연계장비로 데이터 전송을 가능하게 하였다.

또한 논리적 망분리를 위해 클라이언트 기반 가상화를 통한 논리적 망 분리를 적용하여 구성 하였다. 망의 주 회선은 별도로 구성하여 사용자 PC 들은 업무망에 존재하고 인터넷 망을 이용할 시에는 업무망의 모든 네트워크 및 방화벽을 지나서 인터넷 망으로 전송이 되는 방식으로 구축하였다.

완전한 망 분리 작업을 통하여 안정성을 확보할 수 있었으며 커널과 분리되어 악성코드 위험 감염이 방지되는 효과를 얻을 수 있었다. 추후에는 이러한 연구 결과를 바탕으로 하여 인터넷 접속으로 인한 해킹, 파밍등에 대한 피해를 막을 수 있는 방법을 연구 개발할 예정이다.

참고문헌

[1] 이용희, 김현기. “국가기관 네트워크 망 분리 패러다임 변화에 관한 연구”, 정보처리학회논문지:기술교육 제 6권 제 3호, pp. 209-216. 2011.12.

[2] L. Peterson, S. Shenker, and J. Turner, “Overcoming the internet impasse through virtualization,” in Proc. of 3rd ACM Workshop on Hot Topics in Networks, pp.1-6, November 15-16, 2004.

[3] G. Schaffrath, C. Werle, P. Papadimitriou, A. Feldmann, R. Bless, A. Greenhalgh, and A.Wundsam, “Network virtualization architecture: proposal and initial prototype,” in Proc. of 1st ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures, pp. 63-72,August 17-21, 2009.

[4] N. M. K. Chowdhury and R. Boutaba, “A survey of network virtualization,” Computer Networks, vol. 54, no. 5, pp. 862-876, April, 2010. [5]Y. Che, Q. Yang, C. Wu and L. Ma,“BABAC: An access control framework for network virtualization using user behaviors and attributes,” in Proc. of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications, pp. 747-754, December 18-20, 2010.

[6] Derek Bem, “Virtual Machine for Computer Forensics - the Open Source Perspective,” Open Source Software for Digital Forensics, DOI 10.1007, pp. 25-42, Jan. 2010.

[7] Greg Dorn, Chris Marberry, Scott Conrad, and Philip Craiger, “Analyzing the impact of a virtual machine on a hostmachine,” International Federation for Information Processing, Advances in Digital Forensics V, IFIP AICT 306, DOI: 10.1007/978-3-642-04155-6_5, pp. 69-81, 2009.

[8] Richard Arthur Bares, “Hiding in a Virtual World Using Unconventionally Installed Operating Systems,” ISI 2009, pp. 276-284, Jun. 2009.

[저 자 소 개]

이 용 희 (Yong-Hui Lee)

1989년 2월 청주대학교 공학사
1991년 8월 청주대학교 공학석사
2001년 8월 청주대학교 공학박사
1995년 6월 ~ 2002년 2월 HYNIX SEMICON, ULSI LAB.
2002년 2월 ~ 현재 신성대학교 정보지원센터소장, 교양학부, 제철산업과 교수

email : lyhkpi@shinsung.ac.kr

유 승 재 (Seung-Jae Yoo)

1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교 정보보호학과 교수

email : sjyoo@joongbu.ac.kr