HCI 방식을 통한 논리적 망분리 사례 연구

최승표* · 신상욱**

*부경대학교 대학원 정보보호학협동과정

**부경대학교 IT융합응용공학과

A Case Study on Logical Network Separation through HCI method

Seoung Pyo Choi* · Sang Uk Shin**

*Interdisciplinary Program of Information Security, Graduate school, Pukyong National University

**Dept. of IT Convergence and Application Eng., Pukyong National University

E-mail : csp00@naver.com

요 약

악성코드 감염, 외부침입 등으로 인한 금융회사의 고객정보 유출, 기타 금융사고 발생에 대한 위험으로부터 금융거래를 보호하기 위해 금융위원회에서는 “금융전산 보안강화 종합대책”에서 업무망과 인터넷망 분리에 의한 안전한 금융거래와 고객정보 보호대책의 가이드라인을 제시하고 금융전산망 분리를 의무화시켰다. 이에 각 금융회사는 회사별 IT전산 환경에 맞는 물리적, 논리적 망분리 방법을 선택하여 망분리 시스템을 구축하고 있다. 본 논문은 전통적 범용장비의 구성과 최근 발전중인 가상화 기술 중 하나인 Hyper Converged를 통한 통합형 HCI(Hyper Converged Infrastructure) 방식에 대한 비교 및 사례 연구로 논리적 망분리 구축을 위한 효율적인 인프라 구성 방안을 제시한다.

ABSTRACT

To protect financial services against danger of financial accidents and customer information leakage caused by malware, injection attack and so on, Financial Services Commission announced “Financial Networks Security Enhancement Comprehensive Plan“, which suggests the guideline of protecting customer information and providing secure financial services by separating network topology and then makes the financial company use network partitioning system. In consequence of this policy, financial companies respectively chose between the physical partitioning mechanism or the logical partitioning mechanism according to their IT environment. This paper suggests an efficient infrastructure configuration plan for making the logical network partition, by comparison of a construction of traditional general equipment and an integrated HCI(Hyper Converged Infrastructure) through ’Hyper Converged’ which is one of virualization techniques for developing currently, and the case study of the integrated HCI method.

키워드

HCI(Hyper Converged Infrastructure), Hyper Converged, 망분리, 가상화, VDI(Virtual Desktop Infrastructure)

Ⅰ. 서 론

정보기술의 지속적인 발전에 따른 서버, 스토리지, 네트워크 등을 구성하는 독립적인 시스템 기반 IT 인프라에서 통합형 HCI(Hyper Converged Infrastructure) 방식을 통한 IT 인프라로 변화하고 있다. 이것은 하드웨어 성능의 비약적 발전과 하드웨어 제조사들의 기술 상향평준화 및 비용 하락이 VDI(Virtual Desktop Infrastructure) 기술의 보편화를 촉진시키고 있으며[1], H/W 및 S/W 모두 통합하여 제공하는 HCI 기반 방식이 주목받고 있다.

안전한 금융거래와 고객정보 보호가 중요한 금융회사에서는 업무망과 인터넷망을 분리하여 금융 사고에 대한 안정성을 확보하도록 가이드 되고 있다[2,3,4]. 따라서 금융회사에 적용되는 망분리 및 서버 가상화 기술 또한 HCI 기반으로 구축되는 사례가 증가하고 있으며, 이는 HCI가 망분리 구성에서 효율적인 방안이 되고 있다는 것을 의미한다.

본 논문은 논리적 망분리 구축 시 전통적 범용 장비의 구성과 통합형 HCI 방식에 대한 비교 연구로 효율적인 인프라 구성 방안을 제시하고자 한다.

II. 관련 연구

2.1 가상화 데스크톱 인프라(VDI)

VDI로 알려진 DaaS(Desktop as a Service)[5]는 이전부터 꾸준히 발전되어진 클라우드 데스크톱 가상화 기술이다. VDI는 보통 사용자를 위한 클라이언트, 연결 관리를 위한 브로커, 하이퍼바이저 기반의 서버, 사용자 데이터와 가상 이미지를 가지고 있는 스토리지 등 크게 4개의 구성요소로 이루어져 있다. 하이퍼바이저는 가상머신이 실행되기 위한 중요한 요소로 대표적으로 MS Hyper-V, VMWare ESX, Citrix XenServer 등이 있다.

2.2 논리적 망분리

논리적 망 분리는 이미 구축되어 있는 네트워크를 이용하여 VDI 기술을 접목, 하나의 사용자 PC에서 내부 업무 망과 인터넷 망을 분리하여 사용을 가능하게 하는 기술이다[6,7].

가상화 기반 기술은 사용자 인증을 통한 서버 접속 또는 보안영역 접속 방법으로 데이터를 생성, 조회, 수정, 다운로드 되는 과정이 보안영역 또는 업무망을 벗어날 수 없다. 따라서 중앙서버에 의해 정보 유출을 차단하고 사용자 이벤트에 대한 이력 관리가 가능하며 기업의 보안 정책에 따라 관리가 가능하다[8,9].

III. HCI 방식을 통한 논리적 망분리

3.1 Infrastructure 유형별 비교

일반적으로 전통적인 IT 인프라를 구축하기 위해 서버, 스토리지, 네트워크 등의 장비를 각 벤더들로부터 따로 제공받아 이를 통합하여 구축한다. 구축한 인프라에 맞는 S/W 테스트 및 검증 또한 필요하다. 이러한 구조는 인프라 구축에 드는 시간 및 시스템 관리 측면에서 많은 자원을 필요로 한다. 이러한 문제의 해결책으로 인프라를 구축하기 위해 필요한 서버, 스토리지, 네트워크 및 S/W가 사전에 통합되어 검증된 하나의 시스템으로 제공되는 개념인 CI(Converged Infrastructure)가 있지만 이것은 빠른 서비스 구축이 가능하다는 점에도 불구하고 비용 문제 및 시스템 확장의 어려움을 가지고 있다. 특히 고성능 외장형 스토리지의 비용적인 부담이 가장 크게 작용했다고 볼 수 있다.

HCI(Hyper Converged Infrastructure)는 이러한 CI의 문제점을 개선한 개념으로 외장 스토리지를 없애고 서버와 전체 스토리지 자원을 하나로 묶어 내장 스토리지 풀로 제공한다는 것이 가장 큰 특징이라고 볼 수 있다. 따라서 HCI는 이전 구조의 복잡성을 제거함과 동시에 확장성을 만족시키고 비용 절감을 제공한다. 그림 1은 HCI의 전형적인 구조를 나타내고 있다.

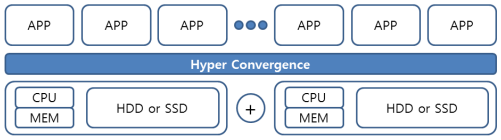

그림 1. Hyper Converged Infrastructure

3.2 논리적 망분리의 HCI 구성 시 고려사항

HCI 개념이 확장성 및 비용절감에 대한 장점을 말하고 있지만, 실질적으로 이를 이용하여 논리적 망분리 구축을 하게 될 경우 몇 가지 고려해야 할 사항이 있다.

3.2.1 확장성에 대한 고려사항

HCI 개념은 앞서 설명한 대로 구조상 서버, 네트워크, 스토리지, 소프트웨어를 통합하여 제공하는 접근법을 가지고 동시에 확장성을 만족시킨다. 하지만 이는 이전 CI개념에 의한 차선책일 뿐이며, 따라서 구축된 논리적 망분리 구조에서 필요에 의해 스케일 업 또는 스케일 아웃이 능동적으로 가능한지 판단해야 할 것이다. 한번 구축된 인프라가 변경되는 경우는 잘 없지만, 논리적 망분리는 VDI가 점유하는 리소스 및 네트워크 사용률, 스토리지에 대한 의존도가 높기 때문에 만약 사용자 증가로 인한 특정 부분의 스케일 업이 전통적인 IT 인프라 보다 확실히 경제적인지 또는 안정성 및 시간적인 비용을 고려하여야 한다.

3.2.2 유지보수 측면에 대한 고려사항

물리적 및 논리적 장애 포인트 발생 대비는 인프라 구성 시 또는 운영 시 필수적인 고려사항이다. HCI가 효율적으로 관리하기 위한 솔루션 및 운영 오케스트레이션이 제공되어 유지된다고 할지라도 논리적 망분리에서 VDI의 가상머신, 네트워크, 스토리지는 여전히 장애 포인트 대상이다. 따라서, 논리적 망분리 구축에서 HCI 방식과 전통적인 인프라 방식 중 어떠한 구조 선정이 유지보수 측면에서 효율적인지 또는 타당한지 고려하여야 한다.

3.2.3 보안 정책에 대한 고려사항

망분리 구성의 가장 큰 목적은 외부로부터의 침입 및 악의적인 공격으로부터 안전한 환경을 조성하는 것과 내부 사용자의 중요 정보들을 보호이다[5]. 따라서 다양하게 발전하는 외부 침입 요소 및 정보 유출에 대비하여 보안 정책의 변경 요구사항이 있을 때 온디멘드 방식으로 적용이 가능한가에 대한 고려사항이다. 추가적인 보안은 심플한 정책일 수도 물리적 보안장비의 추가 또는 보안 솔루션의 적용 사례가 있을 수 있으며, 구축된 HCI 논리적 망분리가 이를 적절하게 수용할 수 있는가에 대해 생각해 보아야 할 것이다.

3.3 HCI 구축 사례

금융위원회 "금융전산 보안강화 종합대책" 가이드라인에 근거하여 2016년 말 논리적 망분리를 통합형 HCI로 구축한 A 금융사의 사례가 있다.

A사는 최근 망분리 사례 및 시장 조사를 거치고, HCI 방식에 대하여 PoC(기술검증, Proof of Concept)를 진행한 결과 H/W의 안정성 및 솔루션 호환성을 검토하여 통합형 HCI로 논리적 망분리 시스템을 구축하였다.

A사의 망분리 구축 시 중점 고려사항은 H/W 증가로 전산실 상면 확장, 항온항습 설비 증설, 향후 전산센터 이전에 따른 비용 발생 등 이다.

또한, 모든 직원이 동시 인터넷 사용을 하지 않는다는 점, 망분리 대상을 인터넷망에 한정한 점, HCI 구성을 통한 전산실 확장 없이 설치 가능하고, 이후 전산센터이전 효율성 등을 고려하여 HCI 구성을 통한 성공적인 사례라 하겠다.

Ⅳ. 결 론

정보기술의 비약적인 발전에 따라 하드웨어 성능 및 가상화 기술을 바탕으로 전통적 방식의 IT 인프라 구성에서 통합형 HCI 방식으로 발전하고 있으며 이는 기존 인프라 구조에서 발생되었던 복잡성을 제거하고 동시에 확장성을 만족 시키며 시스템 관리의 문제점에 대한 해결책으로 볼 수 있다. 하지만, HCI 방식이 모든 IT 인프라 구성에 적용된다고 볼 수는 없다. HCI 방식 특성인 기술적 한계 즉, 하이퍼바이저에 대한 Application 호환성 문제 등으로 인프라 구축이 성공하지 못할 수 있기 때문이다.

A사는 전체 사용자 및 향후 사용자 증가에 대한 스토리지 용량이 전체 스토리지 자원을 하나로 묶는 내장 스토리지 풀 구성(SSD: Solid State Drive, 1.9TByte * 36개)으로 필요 용량을 확보하였고, 망분리 대상을 인터넷망에 한정하여 향후 발생할지 모를 Application에 대한 호환성을 최소하였으며, 외부 침입 및 악의적인 공격, 정보 유출 등 보안 요구사항에 대하여 메일 시스템은 전통적 방식의 인프라 구성으로 독립적인 보안 정책 운영 가능토록 구축하였다.

HCI 방식을 통한 IT 인프라 구성 시 확장성, 유지보수, 보안정책에 대한 고려 사항을 통해 구축한다면 H/W 및 S/W의 유휴 자원 사용에 대한 가용성 확대를 통해 효율적인 IT인프라 구축이라 할 수 있다.

참고문헌

[1] 김두연, 송기웅, "클라우드 기반의 가상화 데스크톱 도입 사례 연구: 제로 클라이언트를 중심으로", 한국IT서비스학회 학술대회 논문집, pp 428~432, 2012.

[2] 금융위원회, "금융 전산 망분리 가이드라인", 2013.

[3] 금융위원회, "전자금융감독규정", 2016.

[4] 박지윤, 정윤선, 이재우, "금융권 망분리 현황과 망분리 정책 개선에 대한 고찰",

[5]오명훈, 김성운, "DaaS 기술 현황과 표준 이슈", TTA Journal, Vol. 139, pp. 48-58, 2012 2.

[6] N. M. K. Chowdhury and R. Boutaba, "A survey of network virtualization," Computer Networks, vol. 54, no. 5, pp. 862-876, April, 2010.

[7] Y. Che, Q. Yang, C. Wu and L. Ma, "BABAC: An access control framework for network virtualization using user behaviors and attributes," in Pro. of the 2010 IEEE/ACM int'l Conference on Green Computing and Communications, pp. 747-754, December 18-20, 2010.

[8] 이용희, 유승재, "가상화를 이용한 논리적, 물리적 망분리 구축", 융합보안논문지, 제 14권 제 2호, pp. 25-33, 2014 3.

[9] 조병주, 윤장호, 이경호, "금융회사 망분리 정책의 효과성 연구", 정보보호학회논문지, 25(1), February 2015.