https://doi.org/10.33778/kcsa.2023.23.5.021

네트워크 가상화 기반 클라우드 보안 구성에 관한 연구

홍 상 범*, 김 성 철**, 이 미 화**

요 약

클라우드 컴퓨팅 환경에서 서버나 애플리케이션들이 수 분 사이에 구축되고 장애 발생 시 복구 또한 쉬워졌다. 특히, 잠시 서비스하기 위해서 물리적인 서버를 구축하는 것 보다 클라우드에서 가상 서버를 이용하면 편리함과 동시에 비용도 저렴하다. 하지만 그러한 서버나 애플리케이션들의 기반이 되는 네트워크나 보안시스템은 대부분 하드웨어 기반으로 구성되어 있어 클라우드 가상화 적용에 어려움이 많다. 클라우드 내에서도 네트워크나 보안설비 등에 대한 가상화를 통한 보호가 필요하게 되었다. 본 논문은 네트워크 가상화 기술을 활용하여 클라우드 네트워크의 보안을 강화하는 방법에 대한 연구를 다루고 있다. 가상 서버 및 가상 네트워크를 생성해 다양한 보안 이점을 제공하는 가상화 기술을 활용해 링크 가상화와 라우터 가상화를 적용하여 보안이 강화된 네트워크를 구성하였다. 구성된 네트워크에 가상 방화벽 기능을 적용해 네트워크를 격리할 수 있었으며, 이 결과를 토대로 가상화 환경에서 보안 취약점을 극복하고 안전한 네트워크 구성을 위한 관리 전략을 제안하는데 기여할 것으로 기대된다.

A study on Cloud Security based on Network Virtualization

Sang-Beom Hong*, Sung-Cheol Kim**, Mi-Hwa Lee**

ABSTRACT

In the cloud computing environment, servers and applications can be set up within minutes, and recovery in case of failures has also become easier. Particularly, using virtual servers in the cloud is not only convenient but also cost-effective compared to the traditional approach of setting up physical servers just for temporary services. However, most of the underlying networks and security systems that serve as the foundation for such servers and applications are primarily hardware-based, posing challenges when it comes to implementing cloud virtualization. Even within the cloud, there is a growing need for virtualization-based security and protection measures for elements like networks and security infrastructure. This paper discusses research on enhancing the security of cloud networks using network virtualization technology. I configured a secure network by leveraging virtualization technology, creating virtual servers and networks to provide various security benefits. Link virtualization and router virtualization were implemented to enhance security, utilizing the capabilities of virtualization technology. The application of virtual firewall functionality to the configured network allowed for the isolation of the network. It is expected that based on these results, there will be a contribution towards overcoming security vulnerabilities in the virtualized environment and proposing a management strategy for establishing a secure network.

Key words : Network Virtualization, Router Virtualization, Link Virtualization, Cloud Security, Security Control, Virtual Server, Container, Host Virtualization

접수일(2023년 09월 15일), 수정일(2023년 12월 11일), 게재확정일(2023년 12월 12일)

* 한전KDN 정보보호실(주저자, 교신저자)
** 한전KDN 정보보호실(공동저자)

1. 서 론

클라우드 컴퓨팅은 자원의 효율적인 사용과 유연한 확장성을 통해 기업과 개인 모두에게 다양한 이점을 제공하고 있다. 이러한 이점 중에서도 가상화 기술은 클라우드 컴퓨팅의 핵심 기반 기술로서, 이를 통해 물리적 자원의 추상화와 분리가 이루어져 다양한 서비스 및 애플리케이션을 효과적으로 실행할 수 있다. 네트워크 가상화는 네트워크 자원을 가상화함으로써 네트워크 관리와 구성을 단순화하고 유연성을 높일 수 있는 기술이다. 즉, 네트워크 가상화는 소프트웨어 형태로 만들어진 라우터, 스위치, 방화벽 등을 활용하여 구축한다. 초창기 라우터는 소프트웨어로 구축하였다가 성능 이슈로 다시 하드웨어로 구성되었다. 현재 클라우드 내에서 가상화를 위해 소프트웨어로 된 라우터, 스위치, 방화벽 등이 요구되고 있다.

본 논문은 네트워크 가상화 기술을 활용하여 클라우드 내에서도 보안을 강화할 수 있는 방안 제시를 목표로 한다. 클라우드 환경에서 가상화 기반 보안 네트워크의 구현과 관리 방법, 그리고 이로 인해 얻을 수 있는 장점들에 대한 이해를 높이고자 한다. 네트워크 가상화는 어플리케이션과 네트워크 사이에 가상화 개념을 도입하여 어플리케이션과 네트워크를 구성하는 특정 자원 사이의 밀접한 물리적 연관성을 논리적 연관성으로 전환하여 네트워크의 구성 및 작동을 단순화 해주는 기술이다[1][2]. 네트워크 가상화 기술은 크게 링크 가상화와 라우터 가상화가 있으며 링크 가상화는 가상화 소프트웨어를 이용해 하나의 물리적인 네트워크 인터페이스(NIC: Network Interface Card)로부터 다수의 가상 네트워크 인터페이스를 제공하는 기술을 의미한다[3][4]. 라우터 가상화는 가상화 소프트웨어를 이용해 네트워크에서 링크들을 연결하는 노드이며 수신된 패킷을 목적지 네트워크에 근접한 네트워크로 적절히 포워딩한다. 또한 각 라우터는 이웃한 라우터들과 서로 경로 정보를 교환함으로써 각 라우터가 최적의 경로를 선택할 수 있도록 한다[3]4]. 현재 대부분의 클라우드 네트워크는 클라우드로 들어가는 관문(라우터 등)에 대해서는 방화벽이나 침입방지시스템 등 다양한 보안시스템을 구축하여 보안을 강화하고 있다. 하지만 클라우드 관문을 통과한 이후에는 대부분 하드웨어로 구성된 보안장비로 인해 더 이상 보안을 강화할 수 없다. 많은 가상화 기업들이 만들어 놓은 네트워크 기능 가상화(Network Function Virtualization, NFV)를 활용할 수 있고 라우터 소프트웨어 등을 통해 자체적으로 구축할 수도 있다. 본 논문의 4장 가상화 기반 네트워크 구성 방안 부분에서 네트워크 및 방화벽 가상화 소프트웨어인 VyOS를 통해 클라우드 네트워크를 구성하고 클라우드 내부 보안 강화 방안을 제시한다. VyOS 또한 NFV를 구축하는데 활용되는 가상화 도구로써, 미국의 Broadcom사가 Vyatte 제품 개발을 포기하자 다른 사람들이 소스 코드를 가져와서 VyOS라는 오픈 소스 NOS(Network Operating System)로 데비안 리눅스 기반으로 개발하였다. VyOS는 소프트웨어 라우터 기능뿐만 아니라 소프트웨어 방화벽 기능을 하고 있어 클라우드에서 꼭 필요한 도구 중 하나다. VyOS는 GUI 환경이 없이 리눅스 명령창을 통해 실행되는 것이 특징이다.

2. 네트워크 가상화 기술 개요

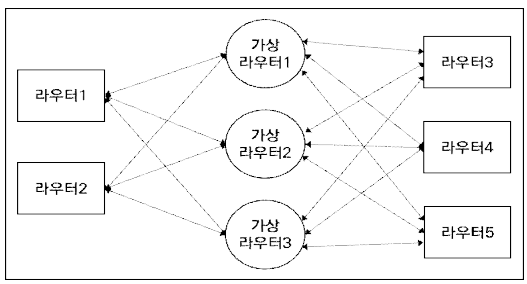
네트워크 가상화는 가상화 소프트웨어를 사용하여 하나의 물리적인 네트워크 인프라를 여러 개의 가상 네트워크로 분할하고, 각 가상 네트워크를 독립적으로 관리하고 구성할 수 있는 기술이다. 가상화의 한 형태로, 가상머신, 스토리지, 서버 등과 함께 클라우드 컴퓨팅 환경에서 널리 사용된다. 네트워크 가상화 기술로는 하나의 물리적 네트워크 장비에서 다수의 가상 네트워크 인터페이스 기능을 지원해 주는 링크 가상화, 하나의 물리적인 라우터에서 자원을 분리하여 다수의 가상라우터를 구성하는 라우터 가상화가 있다. 최근 모바일, 태블릿 등 사용량 및 클라우드 서비스의 증가, 데이터 전송량 증가에 따라 소프트웨어 정의 네트워크(Software Defined Network, SDN)와 NFV가 네트워크 가상화의 핵심기술로 떠오르고 있다. NFV는 서버 가상화 기술을 네트워크 가상화에 접목한 기술로 미래의 클라우드 환경은 서버 뿐만 아니라 네크워크까지 가상화하여 오케스트레이션하는 환경으로 바뀔 것으로 보안다[5].

2.1 링크 가상화

링크 가상화(Link Virtualization)는 네트워크 가상화의 한 형태로, 네트워크 링크를 논리적으로 분리하고 가상 네트워크로 나누는 기술을 나타낸다. 이를 통해 여러 개의 가상 네트워크가 하나의 물리적 네트워크 인프라를 공유할 수 있으며, 이러한 가상 네트워크는 독립적으로 관리하고 구성될 수 있다. 링크 가상화는 데이터 센터 환경에서 가상머신 또는 컨테이너 간의 가상 링크를 구현하며 서로 다른 가상 서버 또는 컨테이너 간에 효율적인 통신 및 자원 공유가 가능하다. 또한 링크 가상화는 SDN 및 NFV의 구현에서도 사용될 수 있다. 이러한 기술을 사용하면 네트워크 자원을 동적으로 할당하고 관리하여 효율성을 향상시키고 유연성을 제공할 수 있다.

2.2 라우터 가상화

라우터 가상화는 가상화 기술을 사용하여 네트워크 라우터 기능을 가상으로 구현하는 것을 의미한다. 이것은 물리적인 라우터 하드웨어를 사용하는 대신 소프트웨어 기반의 가상라우터를 생성하고 실행하여 네트워크 트래픽을 관리하고 라우팅하는데 사용된다. 가상라우터는 물리적 하드웨어와 비교해 더 적은 자원을 사용할 수 있으므로 하드웨어를 더 효율적으로 활용할 수 있고 쉽게 스케일링하고 구성할 수 있으며, 가상 환경 내에서 여러 개의 라우터를 실행할 수 있다.

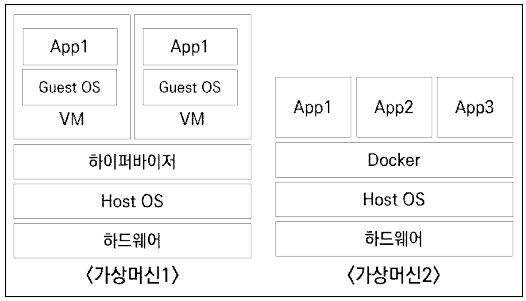


(그림 1) 가상 네트워크 개념도

(그림 1)은 물리 라우터 5대와 가상라우터 3대를 활용하여 구성된 클라우드 네트워크이다. 물리 라우터와 가상라우터들이 섞여 라우팅 테이블이 복잡해질 수 있고 하나의 물리 라우터로 가상 네트워크를 구성한 것에 비해 더 많은 네트워크를 구성할 수 있다. 또한, 네트워크 접점이 많아져 보안에 취약할 수 있다. 가상라우터의 방화벽 기능 등을 통해 보안이 향상된 네트워크를 구성할 수 있다. 즉, 클라우드 환경에서 별도의 설비 없이 가상라우터들로 보안을 강화할 수 있다.

2.3 호스트 가상화

호스트 가상화는 호스트가 가지고 있는 컴퓨팅 자원을 추상화하여 사용자에게 추상화된 논리적 자원 형태로 할당하는 기술로 정의한다[3]. (그림 2)는 호스트 가상화를 보여주고 있다. 왼쪽 <가상머신1>은 하드웨어에 OS를 설치하고 하이퍼바이저 위에 가상머신을 구성한 형태이고 오른쪽 <가상머신2>는 하드웨어에 OS를 설치하고 그 위에 Docker 엔진을 설치하고 컨테이너 기반으로 가상머신을 구성한 형태이다. <가상머신1>은 유연성은 떨어지지만 모든 OS로 가상화를 구성할 수 있고 GUI를 지원한다는 장점이 있다. <가상머신2>는 Docker를 통해 쉽게 서버 구축이 가능하지만 리눅스 OS만을 지원하고 GUI를 지원하지 않는 단점이 있다. 실제 클라우드는 두 방식을 모두 적용하는 쿠버네티스를 통해 구성한다. 쿠버네티스는 명령창을 통해 전체 가상 서버들을 오케스트레이션 할 수 있다.



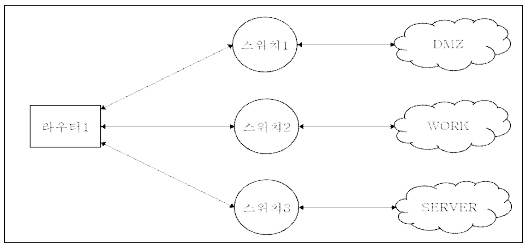
(그림 2) 호스트 가상화

3. 가상화 보안 네트워크 구성

3.1 물리 네트워크 구성

물리 네트워크는 가상화라는 개념 이전에 구성

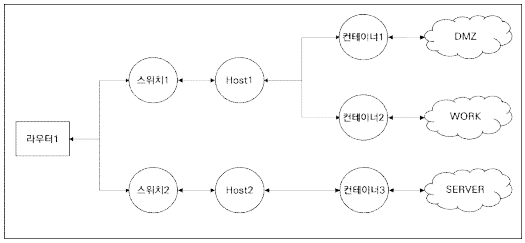
하였던 네트워크를 의미한다. (그림 3)과 같이 하나의 라우터에서 라우팅 테이블을 만들고 스위치를 통해 DMZ망, WORK망, SERVER망 등을 구성한다. 서로 다른 네트워크 간 접근제어는 라우터 또는 방화벽 등을 추가하여 수행한다. 라우터1의 포트 수가 부족할 경우 추가적으로 라우터 및 스위치를 구성해야 한다. 라우터나 스위치 등을 하드웨어 설비로 구축해야 해서 유연성이 떨어지고 비용이 많이 드는 단점이 있다.



(그림 3) 물리 네트워크 개념도

3.2 컨테이너 기반 가상화 네트워크 구성

컨테이너 기반 가상화 네트워크는 Docker 환경과 유사하다. (그림 4)는 하나의 물리 라우터와 2대의 스위치로 네트워크를 구성하고 Host1, Host2에 Docker와 같은 가상화 인프라를 설치하고 컨테이너별로 서비스를 구성한다.

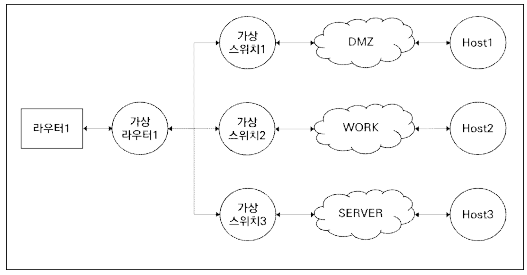


(그림 4) 컨테이너 기반 가상 네트워크 개념도

Docker 엔진이 설치된 Host1에서는 Host1에서 생성한 컨테이너1과 컨테이너2만을 관리할 수 있다. Host1에서 구축된 컨테이너(서비스 등)들은 Port를 다르게 하여 Host1의 IP로 외부와 통신한다. 컨테이너1과 컨테이너3이 통신을 하기 위해서는 Host1과 Host2의 IP로 해당 Port를 통해 통신을 해야 한다. 클라우드 벤더에서는 이러한 부분에 대해 쿠버네티스를 통해 Host1과 Host2, 그 이상의 Host들을 오케스트레이션하여 효율성과 안정성을 높인다. 물리적인 라우터1에는 보안 설정을 구성할 수 있지만 스위치1, 스위치2 뒤단에는 보안 설정이 없어 내부자의 의한 보안 침해 방지 등의 설정이 미흡하다.

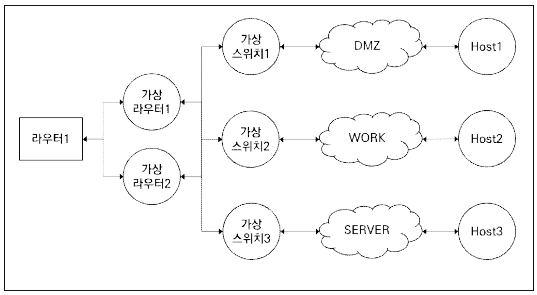
3.4 라우터 가상화 기반 네트워크 구성

라우터 가상화 기반 네트워크는 가상라우터(가상스위치 기능 포함)를 활용하여 네트워크 구성을 의미한다. (그림 5)에서 물리 라우터1에서 경로를 배정받은 가상라우터1은 자체 성능이 감내하는 한도까지 라우팅 설정할 수 있다. 가상스위치1, 가상스위치2, 가상스위치3 총 3개의 대역을 할당받아 대역을 구성하였으며 가상라우터1은 가상화 네트워크 전체에 대해 접근제어를 수행할 수 있다. 즉, 가상라우터1의 라우터 기능과 방화벽 기능을 활용하여 Work망에서 Server망의 접근 허용, Server망에서 DMZ망의 접근 차단 등의 설정을 용이하게 할 수 있다.



(그림 5) 라우터 가상화 기반 네트워크 개념도

소프트웨어 라우터 및 방화벽을 통해 유연한 보안설정이 가능하지만 가상라우터1에 장애 발생 시 네트워크 전체가 마비가 될 수 있는 문제점이 존재한다. (그림 6)은 (그림 5)에서 가상라우터1에 장애가 발생할 경우에 대한 문제점을 보완한 가상라우터 이중화한 구성도이다. 가상라우터1의 모든 설정을 가상라우터2에도 동일하게 설정하여 둘 중 하나가 장애가 발생하더라도 DMZ망, WORK망, SERVER망의 라우팅 테이블이 그대로 유지된다. (그림 6)의 경우 가상라우터 2대만으로 구성되었지만 더 많은 구성도 가능하다.



(그림 6) 라우터 가상화 기반 네트워크 이중화

가상라우터1, 가상라우터2 뿐만아니라 더 많은 가상라우터들을 효과적으로 관리할 수 있는 쿠버네티스 및 MPI(Message Passing Interface) 등에서 사용하는 클러스터링 기술이 요구된다. MPI는 분산 및 병렬처리 환경에서 메시지 교환에 의해 멀티 프로세싱이 가능한 기술 표준이다. “Message Passing”이란 멀티 프로세서 환경에서 여러 프로세스 간 데이터를 주고받기 위해 메시지를 사용하여 통신하는 방식을 의미한다. MPI는 필요 및 기능에 따라 여러 코어들의 서브그룹을 만들어 프로세스를 실행할 수 있다[6]. VyOS에 MPI를 적용하여 자원관리를 수행한다면 효율적인 가용성 확보가 가능할 것으로 보인다.

4. 가상화 기반 네트워크 구성 방안

본 장은 실제 개인이나 기업이 네트워크 가상화 소프트웨어인 VyOS를 통해 보안이 강화된 클라우드를 구성할 수 있는 방안을 제시한다. 또한, 실제 VyOS 환경을 구축하고 외부 인터넷이나 다른 가상화 Docker 환경과 연계 및 보안 구성을 시뮬레이션 하였다. 가상라우터 VyOS를 이중화 구성하여 하나의 가상라우터에 장애 발생 시에도 정상적인 네트워킹이 가능하였다. 23년 국정원에서 제정한 “국가 클라우드 컴퓨팅 보안 가이드라인(2023.01)”을 본 연구를 통해 만족할 수 있을 것으로 판단된다.

4.1 시뮬레이션 환경

시뮬레이션은 Host(Windows 10)의 Hyper-V, Docker 환경을 구성하고 VyOS를 통해 DMZ, WORK, SERVER 네트워크, 다른 가상화 네트워크의 라우팅을 설정한다. VyOS의 방화벽 기능을 통해 보안정책을 설정하여 내부 가상화 부분의 보안을 강화하였다. 세부 네트워크 구성 내용은 <표 1>과 같다. 가상화 환경도 Hyper-V, Docker 환경으로 구성하였다.

<표 1> 환경구성

구분	OS	가상 환경
Host	Windows 10 Pro	-
가상라우터1,2	VyOS(Linux Ubuntu)	Hyper-V
Guest1 OS	Windows 10 Pro	Hyper-V
Guest2 OS	Ubuntu 20.04	Hyper-V
Guest3 OS	Linux Redhat Hat 8.4	Hyper-V
Guest4 OS	Ubuntu 20.04	Docker

4.2. 비교분석

네트워크 가상화는 유연성이 뛰어나 <표 2>와 같이 추가적인 구성이 가능하다. NW 가상화를 하지 않았을 경우 쿠버네티스를 통해 클러스터링으로 가용성 확보가 가능하지만 운영 중에는 할 수 없다. 네트워크 가상화를 적용한 경우 운영 중에도 병렬화를 통해 가용성 확보가 가능한다. 그 외 서브 네트워크 구성이나 가상 방화벽 추가 구성, 클라우드 내부 보안 설정 등을 용이하게 할 수 있다.

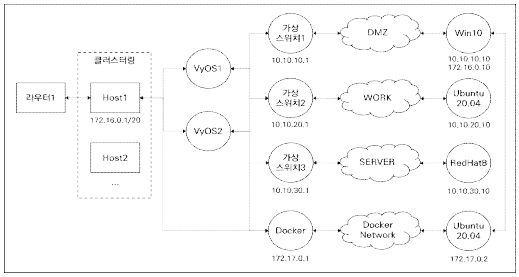
<표 2> 네트워크 가상화 전후 비교

구분	NW 가상화 전	NW 가상화 후
호스트 병렬화 적용	X	O
서브 네트워크 구성	X	O
보안설비 추가 구성	X	O
클라우드 내부 보안	X	O

4.3 가상화 기반 보안 네트워크 구성 사례

본 절에서는 네트워크 가상화 기반으로 실제 보안 네트워크 구성을 시뮬레이션 한 사례이다. (그림 7)에서 Host1은 외부 라우터1으로부터 IP를 부여 받은 서버이다. Host1의 Hyper-V에 VyOS1, VyOS2로 가상라우터를 이중화 구성하고 3개의 네트워크 대역 DMZ망 (10.10.10.1/24), WORK망 (10.10.20.1/24), SERVER망 (10.10.30.1/24)을 구성하였다. 또한, 다른

가상화 Docker 네트워크와의 연결을 설정하였다. DMZ망에 구성된 Win10은 VyOS를 통해 Docker 네트워크와 라우팅을 설정하여 통신이 가능하다. 또한, VyOS의 방화벽 기능을 통해 WORK망의 Ubuntu에서 DMZ망의 Win10으로 접근을 허용하였고 SERVER망의 RedHat8에서 WORK망으로 접근 차단을 설정하였다. 또한, WORK망에서 SERVER망으로 특정 IP를 추가하여 접근허용 등의 정책을 설정하였다.



(그림 7) 가상 네트워크 구성도

VyOS1, VyOS2는 모든 설정을 동일하게 설정한 Active-Active 구성 형태다. VyOS1, VyOS2 중 하나의 시스템에 장애 발생 시 다른 VyOS를 통해 라우팅이 가능하도록 가용성을 향상시켰다. 하지만 VyOS1, VyOS2가 하나의 시스템에서 구성되어 있으므로 VyOS1, VyOS2 시스템에 모두 장애 발생 시 네트워크 전체가 마비될 수 있다. 더 많은 VyOS에 대해 쿠버네티스 및 MPI의 클러스터링을 통한 시스템 간 가용성 확보가 추가적으로 요구된다.

5. 결 론

본 연구에서 네트워크 가상화를 통한 클라우드 보안 강화 방안에 대해 논의하였다. 네트워크 가상화를 통해 좀 더 유연하고 다양한 클라우드 네트워크 구성이 가능해졌다. 또한, 가상화의 방화벽 기능을 통해 클라우드 네트워크 내에서도 접근제어 등을 적용할 수 있어 보안성을 향상시킬 수 있었다. 가상화를 통해 추가적인 설비 추가 없이 클라우드 환경을 구성할 수 있지만 성능 이슈 또한 고려되어야 한다. 대부분의 클라우드 네트워크 구성 시 클라우드 관문에 대해서는 라우터 및 방화벽과 같은 설비 등으로 보안을 강화하는 반면, 클라우드 내부는 라우터 및 보안설비가 대부분 하드웨어로 되어 있어 추가적인 보안 구성이 어려웠다. 클라우드의 규모가 점검 커지고 있어 보안의 분산화가 필요하게 되었다. 다양한 서비스 제공을 위해 보안은 클라우드에서 핵심 이슈가 되었다. 현재 하드웨어로 구성된 네트워크 및 방화벽과 같은 설비들이 가상화를 위해 소프트웨어로 구현되고 있는 추세다. 향후 보안 관제 분야의 핵심이되는 설비로써 IPS(침임방지시스템)와 같은 보안설비들도 가상화하여 클라우드 전반에 대해 보안 강화가 요구된다. 보안은 외부 보안 뿐만아니라 내부 보안도 중요하므로 클라우드 내부에서도 권한별, 네트워크별 등 접근제어 등을 통해 보안을 강화한다면 더욱 안전한 클라우드 환경을 구성할 수 있을 것이다. 또한, 클라우드 내에서의 다양한 서비스에 대해 MPI 등을 활용한 고가용성(HPC) 분야에 대한 연구가 필요하다. 향후 클라우드 내에서 서비스들의 자원을 최대 활용한 성능을 향상이 요구된다.

참고문헌

[1] 김대영, 문수복, 박성용, 변성혁, 이순석, 신명기, 정일영, “네트워크 가상화에 대한 고찰”, 한국정보과학회, 2008.

[2] 이승호, 정문영, 서승우, “네트워크 가상화 모델링을 통한 대역폭 할당 최적화”, 대한전자공학회, 2009.

[3] 강승석, 손예진, 문은지, “클라우드 컴퓨팅 서비스 구현을 위한 네트워크 가상화 연구”, 한국지역정보화학회지, 2010.9.

[4] 이신형, 유시환, 이치영, 이종원, 유혁, “미래 인터넷을 위한 네트워크 가상화 기술의 연구 동향”, Telecommunications Review, 2011.

[5] Rajendra Chayapathi, Syed Farrukh Hassan, Paresh Shah, “NETWORK FUNCTIONS VIRTUALIZATION(NFV) with A TOUCHOF SDN”, Addison-Wesley, ,pp. 37-79, 2016.10.

[6] MPI Forum, "MPI: A Message-Passing Interface Standard", pp. 1-6, 23-140, MPI Forum, 2012.

〔저자소개〕

홍 상 범 (Sang-Beom Hong)
2007년 12월 ~ 현재 한전KDN 재직
2002년 02월 충남대학교 석사
2020년 02월 전남대학교 박사

email : sb.hong07@kdn.com

김 성 철 (Sung-Cheol Kim)
1995년 10월~ 현재 한전KDN CISO 재직
2012년 09월 헬싱키대 석사
2020년 02월 전남대학교 박사

email : kim.sungcheol17@kdn.com

이 미 화 (Mi-hwa Lee)
2007년 12월~ 현재 한전KDN 재직
2002년 02월 공주대학교 학사
2018년 02월 고려대학교 석사

email : mihwalee_98@kdn.com