https://doi.org/10.33778/kcsa.2021.21.2.003

ScienceDMZ 기반의 네트워크 구성에서 접근제어정책 적용★

권우창*, 이재광**, 김기현***

요 약

데이터 기반의 과학연구가 추세인 요즘 대용량의 데이터 전송은 연구 생산성에 많은 영향을 미친다. 이러한 문제를 해결하기 위해서 대용량 과학 빅데이터를 전송하기 위한 별도의 네트워크 구조가 필요하다. ScienceDMZ는 이러한 과학 빅데이터를 전송하기 위해서 고안된 네트워크 구조이다. 이러한 네트워크 구성에서는 사용자 및 자원에 대한 접근제어정책(ACL, access control list) 수립이 필수적이다. 본 논문에서는 실제 ScienceDMZ 네트워크 구조로 구현된 R&E Together 프로젝트와 네트워크 구조를 설명하고, 안전한 데이터 전송 및 서비스 제공을 위해 접근제어정책을 적용할 사용자 및 서비스를 정의한다. 또한 네트워크 관리자가 전체 네트워크 자원 및 사용자에 대해 일괄적으로 접근제어정책을 적용할 수 있는 방법을 제시하며, 이를 통해 접근제어정책 적용에 대한 자동화를 이룰 수 있었다.

Application of access control policy in ScienceDMZ-based network configuration

Woo Chang Kwon*, Jae Kwang Lee**, Ki Hyeon Kim***

ABSTRACT

Nowadays, data-based scientific research is a trend, and the transmission of large amounts of data has a great influence on research productivity. To solve this problem, a separate network structure for transmitting large-scale scientific big data is required. ScienceDMZ is a network structure designed to transmit such scientific big data. In such a network configuration, it is essential to establish an access control list(ACL) for users and resources. In this paper, we describe the R&E Together project and the network structure implemented in the actual ScienceDMZ network structure, and define users and services to which access control policies are applied for safe data transmission and service provision. In addition, it presents a method for the network administrator to apply the access control policy to all network resources and users collectively, and through this, it was possible to achieve automation of the application of the access control policy.

Key words : High speed network, ScienceDMZ, ACL, KREONET

접수일(2021년 02월 28일), 수정일(2021년 03월 18일), 게재확정일(2021년 04월 05일)

★ 본 연구는 2020년도 한국과학기술정보연구원(KISTI) 주요사업 과제로 연구되었음.

* 한국과학기술정보연구원/과학기술연구망센터(주저자)

** 한남대학교/컴퓨터공학과(공동저자)

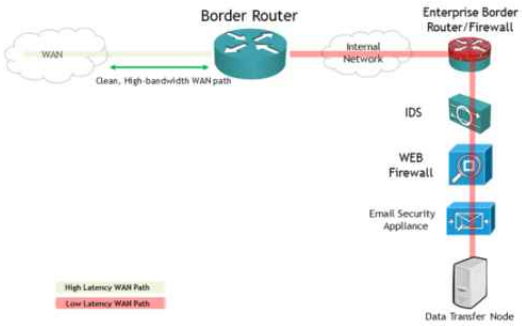
*** 한국과학기술정보연구원/과학기술연구망센터(교신저자)

1. 서 론

최근 과학연구에 대한 추세는 초대형 실험장비의 방대한 데이터 분석을 통한 자연 현상을 기술하는 데이터 기반의 과학연구가 추세이다[1]. 점차 많은 분야에서 시뮬레이션 중심의 연구에서 실험장비의 대용량 과학데이터에 대한 계산 분석 환경으로 변하고 있고 거대 실험장비 중심으로 천문우주[2], 위성정보[3], 유전체분석[4], 핵융합연구[5] 등 다양한 과학분야에서 이러한 베이스로 연구를 진행중이다.

이렇게 대규모 과학시설에서 발생하는 과학 빅데이터를 효율적으로 이동시켜 분석하는게 과학연구에 있어 중요한 요구사항이 되고 있다. 이런 상황에서 필연적으로 데이터를 고속으로 이동시키는 네트워킹 인프라와 그 데이터를 분석하는 컴퓨팅 리소스일 것이다.

국내 연구기관 들의 경우 빅데이터 전송을 위한 전용의 고속의 네트워크가 구축된 사례가 흔치 않은 실정이다.



(그림 1) 일반적인 연구기관 네트워크 구조

그림 1처럼 대부분의 연구기관의 네트워크는 비즈니스 트래픽과 연구전용 트래픽이 혼재된 상태이며, 그마저도 여러 단계를 거치거나 보안장비(DDOS 방화벽, 침입탐지시스템(IDS), 웹방화벽(L7대응), 이메일 보안장비)를 거치다보니 성능하락은 더욱더 심해지고 있다. 또한 이러한 보안장비를 거치는 것은 할당된 네트워크 대역폭에 비해 데이터 전송 시 전송효율을 극대화하기 어려운 구조이다. 특히, 비즈니스 트래픽과의 전송경로 공유는 연구데이터에 대한 전송성능의 보장을 어렵게 하고 있다. 이러한 문제를 해결하기 위해 과학 빅데이터 전송을 위한 전용의 네트워크 구성 및 시스템이 필요하다.

이러한 문제를 해결하고자 미국 ESnet[6] 엔지니어에 의해 제안되고 발전되어온 ScienceDMZ[7] 모델은 대용량 벌크 데이터 전송, 실험 원격 제어 및 데이터 시각화를 포함한 고성능 과학 어플리케이션의 요구에 맞게 설계된 환경을 구성함으로써, 연구 기관에서 발생할 수 있는일반적인 네트워크 성능 문제를 해결한다.

ScienceDMZ는 종단간 전송효율성을 극대화하기 위해 네트워크, 데이터 전송 노드 그리고 기관 내 네트워크 보안 정책 등 복합적인 구성요소들을 최적화하는 혁신적인 기술을 말하며, 다음과 같은 핵심개념을 구현하고 있다.

- 과학 네트워크와 범용 네트워크가 구분되고 고성능 어플리케이션을 위해 명확히 설계된 네트워크 아키텍처
- 데이터 전송을 위한 전용 시스템의 사용
- 네트워크 성능 보장과 모니터링 및 문제 해결을 위한 성능 측정 및 네트워크 테스트 시스템
- 고성능 과학 환경에 맞춘 보안 정책과 강화 메커니즘

(그림 2) ScienceDMZ 구성요소

본 논문은 이러한 ScienceDMZ 네트워크 구조에서 고성능 과학 환경에 맞춘 보안 정책과 강화 메커니즘의 적용 사례 및 방법에 대해 기술하고자 한다.

2. 연구 동향

2.1 국외 ScienceDMZ 연구 동향

2010년 초반 미국의 ESnet에서 시작된 ScienceDMZ 개념의 정립과 실제 슈퍼컴퓨팅센터, 데이터센터 등에 적용을 통해 연구 전용 데이터의 전송 성능을 획기적으로 개선하였으며, 이를 토대로 2015년부터 미국의 과학재단인 NSF의 지원을 통해 PRP(Pacific Research Platform)[8] 프로젝트는 ScienceDMZ 기술을 고도화하고 확대 적용하여 미국내 빅데이터 기반 주요 6개 연구분야를

중점 지원하는 리서치 플랫폼으로 고도화를 진행하고 있다. PRP는 미국의 서부 지역의 저명한 연구소와 대학교를 중심으로 기존의 백본 업그레이드 사업을 통해 구축된 100G 백본을 이용하여 주요 거점 지역의 ScienceDMZ를 고속으로 연동함으로써 빅데이터 전달 체계와 컴퓨팅 체계를 연계하는 하나의 거대한 리서치 플랫폼으로 구축하여 현재는 NRP 프로젝트로 확대 되었다. NRP(National Research Platform)[9] 프로젝트는 미국 서부 지역으로 한정 지었던 한계를 벗어나 미국 전역으로 확대되어 ScienceDMZ을 구축하고 있으며, ScienceDMZ 기반의 빅데이터 고속도로 체계를 구축하고 CPU, GPU 기반의 DTN(Data Transfer Node)[10]을 이용하여 AI 플랫폼을 연계하여 연구 기관 및 교육기관에 대한 빅데이터 기반의 AI 연구와 교육을 지원하고 있다.

이러한 국제 동향을 통해 최근 아시아 국가들도 ScienceDMZ 구축을 진행하고 있으며, 이를 토대로 APRP(Asia Pacific Research Platform)[11] 프로젝트를 진행하고 있다. APRP에 속한 국가들 중 ScienceDMZ을 구축하여 운영하고 있는 나라들은 한국, 호주, 싱가폴, 뉴질랜드, 일본, 파키스탄, 말레이시아, 필리핀 등이 있으며, 점차적으로 아시아 지역에서 늘어나고 있는 추세이다. 위의 나라들 중 ScienceDMZ을 구축하고 CPU, GPU 기반의 DTN을 이용하여 AI 플랫폼을 연계하는 작업을 진행하고 있는 나라는 한국이 유일하며, 미국, 유럽, 아시아 지역을 빅데이터 고속도로 체계를 구축하는 프로젝트인 GRP(Global Research Platform)[12] 프로젝트가 현재 진행 중이다. GRP 프로젝트를 통해 한국은 선진국의 빅데이터 거점으로서 아시아 지역 허브 역할을 하고 있으며, 이러한 빅데이터를 아시아 지역에 공유하고, 유관 기술을 선도하고 있다.

2.2 국내 ScienceDMZ 연구 동향

국내의 경우 한국과학기술정보연구원(KISTI)의 국가과학기술연구망(KREONET)[13]에서 이러한 출연연구소들의 과학 연구 수행을 돕기 위해 8개의 출연연구소들(한국과학기술정보연구원, 한국항공우주연구원, 한국화학연구원, 한국한의학연구원, 국가핵융합연구소, 한국과학기술원, 한국에너지기술연구원, 한국생명공학연구원)과 함께 ScienceDMZ 네트워크 구축 및 빅데이터 전송 기술을 제공하는 프로젝트 R&E Together를 진행하고 있으며, 이 프로젝트를 통해 AI 연구자가 다른 AI 연구자로 부터 빅데이터를 전송 받아 즉시 시스템에 적용하여 연구 결과를 도출하는 미래형 과학 협업 인프라 서비스를 제공하는 것을 목표로 하고 있다.

2.3 효율적인 접근제어정책(ACL) 수립 필요성

이런 ScienceDMZ 환경에서 구축된 네트워크에서는 기존의 보안장비(DDOS 방화벽, 침입탐지시스템(IDS), 침입방지시스템(IPS), 웹방화벽(L7 방화벽)를 이용하지 않기 때문에 필히 보안정책을 마련해야 하며, 적절한 접근제어정책(ACL) 수립하여야 한다.

하지만 기본적으로 폐쇄망으로 운영되며 종단간 네트워크 최적화 기술인 ScienceDMZ 네트워크 구조는 1:1 관계의 종단간 전송 시에는 접근제어정책에 대한 목록의 복잡도가 크지 않다. 양끝단의 접근제어할 사용자의 IP와 전송 및 서비스에서 사용할 port 정보 수준만 있어도 적절한 접근제어정책을 수립할 수 있다.

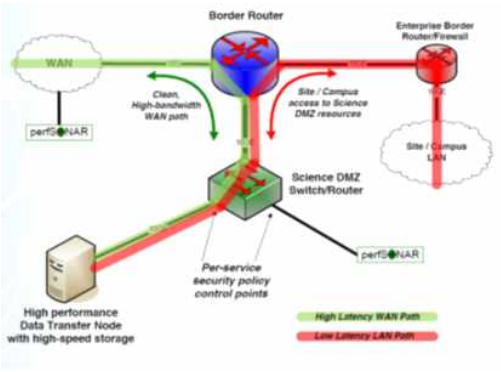
하지만 이렇게 ScienceDMZ 환경으로 구축된 네트워크 위에 데이터 전송 및 응용서비스가 올라갈 경우 네트워크 구조가 N:N으로 확장되고 그 복잡도가 커지면 해당 네트워크에 연결된 모든 엔드포인트에서는 네트워크에 연결된 모든 엔트포인트 및 서비스에 대한 접근제어정책 목록을 갖고 있어야 하며 관리에 대한 공수 또한 커지게 된다. 본 논문에서는 ScienceDMZ 환경에서 구축된 네트워크에서의 효율적인 접근제어정책에 대해서 기술하며, 실제 네트워크에서의 운용결과를 보이고자 한다.

3. ScienceDMZ 기반의 네트워크 구축 현황 및 ACL 적용 방안

빅데이터 전송 시스템은 ScienceDMZ 인프라 구축과 최적의 데이터 전송 노드인 DTN을 이용하여 빅데이터의 손실이 없는 고속의 데이터 전송을 위한 네트워크를 구축하는 것을 말하며, 실제로 데이터 전송 시스템을 구축하기 위해 각 출연연구소(한국과학기술정보연구원, 한국항공우주연구원, 한국화학연구원, 한국한의학연구원, 국가핵융합연구소, 한국과학기술원, 한국에너지기술연구원, 한국생명공학연구원)의 전산 담당자들과 협력하여 각 기관의 DTN 서버를 구축하고 ScienceDMZ을 위한 네트워크 구축을 수행하였다. 본 절에서는 R&E Together 인프라를 구성하는 구성요소들과 빅데이터 전송 환경의 개발 과정에 대해 설명한다.

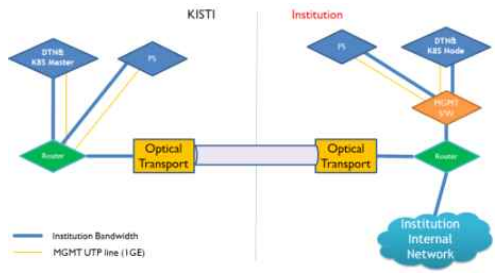
3.1 빅데이터 전송 환경 구축

빅데이터 전송 시스템을 구축하기 위해서는 ScienceDMZ을 이용한 네트워크의 구조와 DTN 서버의 설치가 필수적이다. 그림 1은 기존 네트워크를 구성하고 있는 대부분의 연구소들의 네트워크 구성을 보여주고 있다. 기존의 네트워크 구성을 보면 일반망인 인터넷 망과 연구망을 같이 사용하며, 다양한 보안 장비들을 하나의 네트워크에 연결하여 복잡한 네트워크 구조로 구성된 것을 볼 수 있다. 데이터 전송 서버의 경우 보안장비를 거쳐서 위치할 경우 전송 성능의 저하를 가져온다.



(그림 3) ScienceDMZ 네트워크 구성도

그림 3은 ScienceDMZ의 구성도이다. ScienceDMZ의 네트워크 구조를 구성하기 위해서는 기존에 사용해오던 네트워크 구조에서 일반 인터넷 망과 연구를 위한 연구망 망을 분리하여 구성해야 한다. 이를 위해 일반 망에 존재하는 기존 보안장비를 구성했던 내부 네트워크에 설치되어 있던 데이터 전송 서버를 Border Router에 그림 3과 같이 새롭게 연결하여 DTN 서버를 구성하였을 때 보안장비들을 우회하여 성능이 향상되며, 일반 인터넷 망과의 트래픽 혼재를 막을 수 있다.



(그림 4) 개별 기관간 ScienceDMZ 네트워크 구성

그림 4는 KISTI와 각 기간과의 네트워크를 ScienceDMZ으로 구축한 구성을 보여준다. KISTI와 타 기관 간에 통신을 수행할 때, 각 기관의 border router을 거쳐 내부 비즈니스 영역으로 들어가지 않고 바로 DTN 서버가 있는 영역으로 통신이 되도록 경로를 갖는다. 이는 비즈니스 영역에 있는 일반적인 보안장비를 거치지 않아 전송성능에 저하에 대한 영향을 받지 않는다. 또한 이는 비즈니스 영역에서 발생하는 트래픽들에 대한 작은 단위의 네트워크 커넥션을 피할 수 있는 장점이 있다. ScienceDMZ는 이와 같이 비즈니스 영역과 과학데이터 영역에 대한 전송구간을 달리하기 위한 네트워크 구성을 기본적으로 가진다.

네트워크 구성뿐 아니라 ScienceDMZ는 DTN 이라는 고속의 데이터 전송을 위한 전용 서버를 갖춰야 한다. DTN을 구성하기 위해서는 다음과 같이 몇 가지를 고려해야 한다. CPU의 경우는 멀티코어 보다는 단일코어의 클럭 속도가 성능에 더 많은 영향을 주며, 스토리지의 경우 고속의 디스크기반 저장장치 보다는 고속의 SSD 또는 NVMe SSD가 실제 전송성능에 많은 영향을 끼친다. 그리고 네트워크 인터페이스 카드의 경우 40G 또

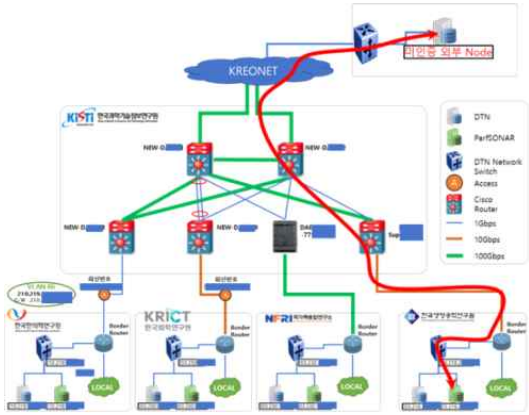
는 100G NIC을 사용하여 1Gbps 이상의 고대역 전송환경을 필요로 하는 서비스에 대해 대응할 수 있도록 한다.

이런 하드웨어적인 부분 외에 DTN을 구성하기 위해서는 시스템 튜닝이 필요로 하며, 네트워크적인 튜닝과 하드웨어적인 튜닝으로 나뉜다. 네트워크 튜닝의 경우 MTU(maximum transmission unit) 사이즈 튜닝과 txqueuelen 사이즈 튜닝을 이용하여 높은 대역폭에서 사용되는 환경으로 설정할 수 있다. MTU 사이즈의 경우 DTN서버에서만 설정을 변경해 주는 것이 아니며, 중간 네트워크에 있는 모든 스위치 및 네트워크의 MTU 사이즈를 맞추어야만 정확한 네트워크 성능을 보장받을 수 있다.

스토리지 역시 실제 Disk to Disk의 성능을 최대한 끌어올려려면 저장매체의 읽고 쓰는 속도를 높여야 한다. 저장매체별 일반적인 읽기, 쓰기 속도는 다음과 같다(HDD < Sata < SSD < NVMe SSD).

제안된 R&E Together에서는 DTN 서버와 더불어 효율적인 데이터 전송을 위한 별도의 전송도구인 Globus Online[14]을 사용하였다. Globus Online은 전송에 참여하는 종단 호스트들 간에 대용량 데이터의 고속 전송 기능을 SaaS(Software as a Service) 방식으로 제공하는 소프트웨어 기반 클라우드 플랫폼 서비스이며, 3자간 파일 전송 기능을 통해 전송 요청, 종단간 파일 전송 및 전송완료 공지의 단계로 전송 과정의 단순화 및 사용자 편의성을 제공한다. 실제 데이터 전송부분은 Grid FTP를 기반으로 동작하도록 구현되어 있고, Grid FTP는 일반적인 파일 전송 프로토콜들에 비해 병행성(Concurrency), 병렬성(Parallelism)의 수준을 조절하여 다수의 TCP 스트림들을 동시에 활용하여 전송할 수 있도록 함으로써 고대역의 ScienceDMZ 네트워크 자원의 활용도를 극대화하여 높은 전송성능을 기대할 수 있다.

3.2 접근제어정책 적용범위



(그림 5) R&E Together 전체 네트워크 구성도

그림 5와 같이 ScienceDMZ로 구축된 네트워크의 특징은 과학 연구데이터의 전송구간에는 기존의 방화벽 및 보안을 위한 장비들이 존재하지 않는다. 그 이유는 구축된 네트워크의 대역폭을 최대한 사용하기 위해 망 전송성능을 저하하는 요소인 보안장비들을 우회하여 트래픽이 흐르도록 되어있다

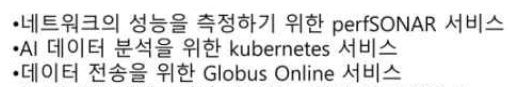
만약 이러한 네트워크에 접근제어정책이 수립되지 않는 상황에서는 border router에 직접 연결된 DTN(Data Transfer Node)에 외부에서 접속이 가능하여 연구데이터에 대한 유출 및 외부에서의 공격에 대한 대비를 하지 못하는 상황이 발생한다.

이러한 상황을 해결하려면 ScienceDMZ로 구축된 네트워크의 각 엔드포인트에 접근할 IP 및 서비스 port를 사전에 정의하여 각 엔드포인트 방화벽에 적용하여야 한다.

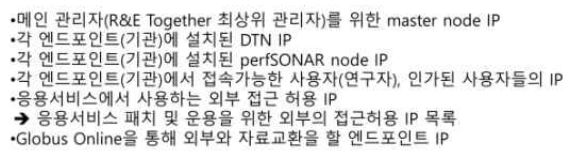
기본적인 접근제어정책은 인가된 서비스 및 사용자들만이 접속을 허용할 수 있도록 구성하는 것이 원칙이며, 그 외 모든 port, IP는 접근을 허용치 않는다.

본 절에서는 이러한 접근제어 정책을 세우기 위해 어떠한 요소들을 고려하여 실제 운용하고 있는 네트워크에 적용하였는지 설명한다.

구축한 환경에서는 크게 3가지의 기능을 하는 서비스가 있으며, 서비스 제공을 위한 접근허용 IP 리스트는 다음과 같다.



(그림 6) 서비스를 위한 네트워크 포트



(그림 7) 서비스 사용을 위한 접근허용 IP 정보

이러한 요소들에 대해 서비스 및 사용자 그룹이 추가될 때 마다 접근제어정책의 복잡도는 점점 더 증가하게 된다. 한 기관에서도 다양한 연구그룹이 있으며 이 연구그룹 별로 사용하는 서비스도 다르기 때문에 각 기관의 DTN에 위치한 방화벽의 설정은 네트워크를 운용하는 동안 지속적으로 변경이 발생한다.

기본적으로 허용된 서비스 및 사용자만 통신이 가능하게 하는 ScienceDMZ 네트워크 구조상 사전에 양 기관이 사용할 서비스 및 사용자 그룹에 대해서 공유가 필요하며 이를 기반으로 접근제어정책을 수립하게 된다. 하지만 네트워크의 규모가 커질수록 연결되는 기관(DTN)이 많아질수록 관리해야할 prot 및 IP정보는 늘어나게 되며 사전에 이러한 정보들이 공유가 되지 않아 사용자들의 서비스 이용에 문제가 발생할 수 있다. 과학연구데이터의 특성상 지속적인 연결성이 필요한 서비스도 있지만 연구데이터의 전송 이벤트 발생 시에만 단대단으로 데이터를 전송하거나 여러 기관에 1:n 형식으로 데이터의 이동이 있는 경우가 많다. 이러한 경우 각각의 기관(DTN 관리자)가 각 이벤트가 일어날 때 마다 서로의 방화벽 설정을 설정하는 것은 비효율 적이며 지속적으로 네트워크 운용에 대한 공수가 추가로 들어간다.

이러한 문제점을 해결하기 위해 본 논문에서는 중앙의 master 노드에서 모든 기관(DTN)에서 사용하는 서비스 port 및 사용자그룹 IP를 수집하여 일괄적으로 모든 기관(DTN)에 적용하는 방법을 적용하였다. master 노드는 모든 기관(DTN)에 접속하여 방화벽의 설정을 변경할 수 있도록 권한을 주고, 서비스 및 사용자 그룹의 변경이 있을 때 모든 기관에 일괄적으로 적용하여 서비스의 중단 및 사용자 그룹의 변경이 용이하도록 하였다.

3.3 접근제어정책 적용 및 구현

그림 5에서 보듯이 각 엔드포인트(기관)에 위치한 DTN의 방화벽에는 일관되게 서비스 port 및 접근허용 IP에 대한 정책이 수립되어 있어야 한다. 하지만 노드 및 서비스가 추가될 때마다 모든 엔드포인트에 동일한 정책(혹은 개별적인 정책)을 일괄적용 하는 것은 네트워크를 운용하는데 있어 많은 공수를 요구하게 되며, 노드의 수가 늘어갈수록 유지보수의 어려움은 추가된다. 본 논문에서 기술하는 환경에서는 이러한 문제를 해결하기 위해 Red Hat Ansible[15]를 이용하여 접근제어정책 적용에 대한 자동화를 구축하였고 많은 공수를 줄일 수 있었다.

KREONET R&E Together 서비스 사용 port

번호	서비스	용도	TCP Port	UDP Port
1	perfSONAR Node	SSH 사용 포트	2204	
2	perfSONAR Toolkit Ports	management interface	80, 443	
3		esmond	80, 443	
4		Lookup Service	8090	
5		owamp (control)	861	
6		owamp (test)	8760-9960	8760-9960
7		twamp (control)	862	
8		twamp (test)	18760-19960	18760-19960
9		pscheduler(https), globu sonline(https)	443	
10		traceroute		33434-33634
11		simplestream	5890-5900	
12		nuttcp	5000, 5101	
13		perf3	5201	
14		perf2	5001	
15		ntp		123
16	kubernetes	Master API 정보 교환 사용 포트	6443	
17		SSH 사용 포트	2219	
18		Kubernetes etcd API 사용 포트	2379-2380	
19		kubernetes kubelet API 사용 포트	10250	
20		kubernetes scheduler 사용 포트 10251/tcp	10251	
21		kubernetes scheduler 사용 포트 10252/tcp	10252	
22		kubernetes 외부 서비스 및 모니터링을 위한 사용 포트	30000-32767	
23	Globus Online	154.237.254.192/29) GridFTP control channel traffic	2811	
24		(Any) GridFTP data channel traffic	50000-51000	
25		154.237.254.192/29) MyProxy traffic	7512	
26		MyProxy traffic	443	

(그림 6) 각 서비스에 사용하는 port 명세

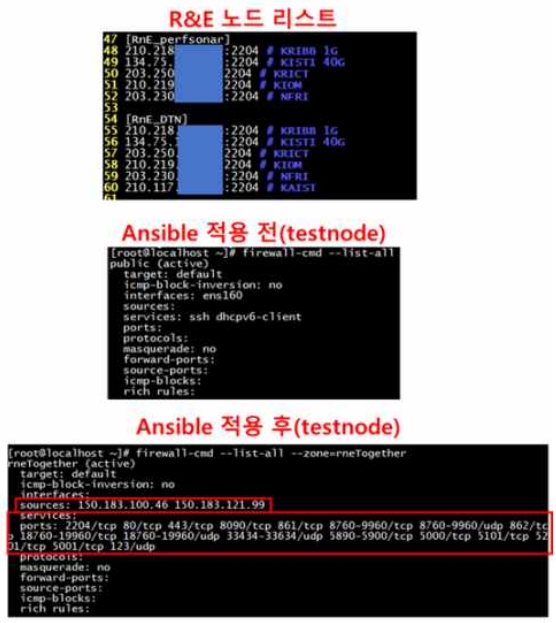
Red Hat Ansible의 특징은 Agent-less구조라서 클라이언트 프로그램을 호스트에 설치할 필요 없으며, SSH 접속 가능한 호스트라면 대부분 Ansible로 태스크 실행 가능하다. 적용하기 쉬운 언어인 YAML 형식의 언어로 playbook를 기술할 수 잇으며, 실행 태스크를 작성하기만 하면 되므로 복잡한 구문을 기억할 필요가 없다. 또한 공개된 다양한 모듈을 이용하여 작업의 효율성을 제공하며 멱등성(idempotence)을 제공하여 같은 조작을 몇번이고 수행하더라도 같은 결과가 얻어지는 성

질을 가진다. 애드혹(Ad-hoc) 명령이 가능하여 ansible 명령이라는 단일 모듈만을 실행하는 명령 입력을 제공하여 Playbook을 작성하지 않더라도 ansible 명령을 터미널에서 실행하는 것만으로도 모듈 실행 가능하다. 본 논문에서는 ansible를 이용하여 구축된 환경에 대한 서비스 및 접근 IP에 대한 플레이북(playbook)를 사전에 설정하여 구축하였다.

(그림 7) 사전에 구축된 플레이북 일부

이러한 ansible의 활용을 통해 접근제어정책의 구성 및 적용에 있어 많은 이점이 있었다. 기존에는 특정 기간에만 사용하는 서비스 및 사용자에 대해서 효율적인 접근제어정책 적용이 어려움이 있었다. 예를 들어 특정서비스를 일정 기간에 사용자들이 이용하고자 한다면, 사전에 사용자에게 A노드에서 B노드의 특정서비스(port)에 대한 사용계획을 접수하여 개별 노드에 각각 방화벽을 업데이트해야 하는 문제들이 있었지만, 사용자의 사용전에 사전에 작성한 playbook을 용도별로 작성하여 각 노드에 적용시키거나 등 ansible의 활용을 통해 사용자의 요구를 쉽게 수용할 수 있었다.

- 신규 접근 허용 IP 및 port에 대한 정책을 사전에 작성하여 쉽게 배포가 가능
- 항시 사용하지 않는 서비스 및 IP 에 대해 상황별로 사전에 접근제어정책 수립 가능
- 접근제어 정책 적용 결과에 대한 피드백 확인 가능



(그림 8) ansible을 활용하여 방화벽 업데이트 결과

4. 결 론

대용량 과학데이터 전송을 위해 많은 인프라들이 필요하며, 네트워크는 물론이다. 하지만 비용적으로나 여러가지 이유로 네트워크 용량을 무한히 증설하기는 쉽지 않다. (네트워크 구축비용, 전송장비, 보안장비 구축 비용, 연구기관의 보안정책 때문에 회선추가에 대한 사전 심의(상위 보안감사기관 검토 등)) 즉, 기존의 네트워크를 최대한 활용하는 방식이 필요하여 본 구조는 ScienceDMZ 네트워크 구조를 적용하므로 연구트래픽 및 비즈니스 트래픽 분리가 가능하며, 연구데이터의 고속전송이 가능하였다.

하지만 보안적인 측면에서 기존의 보안장비를 활용하지 못하기 때문에 안전한 접근제어정책이 필수적이다. 본 논문에서는 이러한 접근제어정책을

효율적으로 적용하여 안전한 대용량 과학데이터 전송을 위한 방안을 제시하였다.

그 결과로 각 서비스, ip 별로 사전에 접근제어 정책을 수립해놓을 수 있었으며, ansible 활용으로 인해 중앙집중방식으로 접근제어정책 수립 및 적용이 수월하였다. 그리고 ScienceDMZ 구조가 적용된 네트워크에 있어 효율적인 접근제어정책 적용에 대한 사례가 되었다.

본 논문에서는 이러한 접근제어정책에 대해서 ansible의 도움을 받아 많은 공수를 덜 수 있었지만 결국 관리자의 수작업이 필요한 상황이다. 향후 연구과제로는 사용자들의 요구사항에 대해서 보다 나은 단계의 자동화를 제공할 수 있도록 사용자의 요청 서비스, 전송포인트에 대해서 자동으로 보안정책까지 적용될 수 있는 통합된 R&E Together 네트워크 자동화 플랫폼에 대한 연구가 있다.

참고문헌

[1] 최명석, 이승복, 이상환, "국내 과학기술분야 연구기관의 과학데이터 관리 현황." 한국콘텐츠학회논문지 제17권, 제12호, pp. 117-126, 2017.

[2] 한국천문연구원(KASI), https://www.kasi.re.kr/

[3] 한국항공우주연구원(KARI), https://www.kari.re.kr/

[4] 한국생명공학연구원(KRIBB), https://www.kribb.re.kr/

[5] 한국핵융합에너지연구원(KFE), https://www.kfe.re.kr/

[6] ESNET, https://www.es.net/

[7] Dart, Eli, et al. "The science dmz: A network design pattern for data-intensive science." Scientific Programming Vol. 22, No. 2, pp. 173-185, 2014.

[8] PRP(Pacific Research Platform), https://pacificresearchplatform.org/

[9] NRP (National Research Platform), https://pacificresearch platform.org/nrp/

[10] DTN (Data Transfer Node), https://pacificresearch platform.org/nrp/

[11] APRP (Acia Pacific Reasearch Platform) https://aprnet.org/

[12] GRP (Global Reasearch Platform) http://www.theglobalresearchplatform.net

[13] KREONET, https://www.kreonet.net/

[14] Globus Online, https://www.globus.org/

[15] Red Hat ansible, https://www.redhat.com/en/resources/ansible-automation-platform-brief

〔저자소개〕

권 우 창 (Woo-chang Kwon)
2011년 2월 : 안동대학교 컴퓨터공학과 석사
2015년 9월~현재: 한국과학기술정보연구원(KISTI) 연구원
email : wckwon@kisti.re.kr

이 재 광 (Jae-kwang Lee)
1984년 2월: 광운대학교 전자계산학과(이학사)
1986년 2월: 광운대학교 전자계산학과(이학석사)
1993년 2월: 광운대학교 전자계산학과(이학박사)
1993년 8월 ~ 현재: 한남대학교 컴퓨터공학과 정교수
email : jklee@hnu.kr

김 기 현 (Ki-Hyeon Kim)
2016년 2월 : 강원대학교 컴퓨터과학과 석사
2017년 2월~현재: 강원대학교 텀퓨터과학과 박사
2016년 2월~현재: 한국과학기술정보연구원(KISTI) 연구원
email : kkh1258@kisti.re.kr