Journal of the Korea Academia-Industrial cooperation Society
Vol. 16, No. 5 pp. 3462-3468, 2015

http://dx.doi.org/10.5762/KAIS.2015.16.5.3462
ISSN 1975-4701 / eISSN 2288-4688

통신 대역폭 논리영역 적용 기반의 네트워크 보안구간 안정화 연구

서우석[1*]
[1]주식회사 이지서티

A Study on Stabilizing a Network Security Zone Based on the Application of Logical Area to Communication Bandwidth

Woo-Seok Seo[1*]
[1]**The Security Headquarters, EASYCERTI Co., Ltd.**

요 약 2014~2015년 현 시점에서 발생되고 있는 수많은 네트워크 장애와 침해는 ISP(Internet Service Provider)가 제공하는 통신라인 등을 통해 접근하는 공격성향의 불법접근이 문제의 근원으로 나타나고 있다. 이와 같은 네트워크 기반의 공격에 대비한 방어방법으로 네트워크 통신을 위한 안정화 구조와 이에 준하는 다양한 정책 및 물리적 보안 장치와 솔루션들이 구현되고 구축되고 있다. 따라서 통신 대역폭 상의 논리영역을 구성하는 등의 네트워크 보안구간을 확보하기 위한 기초 연구자료와 네트워크 보안시장의 또 다른 연구 주제인 통신라인의 확충을 위해 제시되는 과제를 제안하고 네트워크 통신 대역폭을 이용한 능동적인 통신 대역폭 연동 패러다임이 물리적 보안을 이끄는 한 영역으로 필요성이 대두되어 졌음을 인지하는 과정이 필요해 졌다. 추가적으로 현재 통신사들이 제공하는 통신용량을 기준으로 이를 세분화된 조직 영역으로 재분할하고 분할된 각 영역별 통신 용량의 논리적 가상화를 적용함으로써 가시적 보안구조 구성 형태의 자료들을 특정한 물리적 정보 범주에 모두 제한하는 것이 필요하다. 이는 기존의 물리적 구조를 논리영역 적용 기반의 네트워크 보안구간을 제안함으로써 물리적 네트워크 통신 구조를 설계하는 기초자료로 제공 되어질 것이다.

Abstract Regarding countless network disorders or invasions happening nowadays from 2014 until 2015, illegal access intended to attack through the communication line provided by ISP (Internet Service Provider) appears to be the source of the problem. As a defensive way to prevent such network-based attacks, not only stabilization structures for network communication but various policies as well as physical security devices and solutions corresponding to those have been realized and established. Therefore, now is the time to gain foundational research data to secure network security sections by producing logical area on communication bandwidth or such, suggest tasks to expand the communication line which is another research topic in the network security market, and recognize the fact that the active communication bandwidth linkage paradigm using network communication bandwidth is needed as one of the areas that can realize physical security. Additionally, it is necessary to limit the data in the forms of organizing visible security structures into a certain range of physical information by re-dividing communication capacity being currently provided by telecommunicators into subdivided organizational areas and applying the logical virtualization of communication capacity in each of the areas divided. By proposing a network security section based on a logical field application in place of the existing physical structure, basic data that designs a stable physical network communication structure will be provided.

Key Words : Communication Bandwidth, Logical security, Secure area

*Corresponding Author : Woo-Seok Seo(EASYCERTI)
Tel: +82-10-7766-3055 email: ssws2000@nate.com
Received February 7, 2015 Revised (1st March 5, 2015, 2nd March 31, 2015 3rd April 27, 2015)
Accepted May 7, 2015 Published May 31, 2015

1. 서론

네트워크 통신 구조를 이용한 정보의 흐름을 표현하는 단위인 대역폭을 다양한 형태의 서비스 부문으로 분리 및 제공을 하는 ISP(Internet Service Provider) 업체들이 있다. 최소 Mega 단위로부터 Giga에서 Tera에 이르는 대역폭을 지원하는 안정된 네트워크 통신 인프라 서비스가 다양한 기업과 기관에서 임대 또는 영구 구매 등을 통해서 운영하고 있다. 하지만 이러한 전문 네트워크 대역폭을 가진 구조에 대한 침입 차단 등의 부가 서비스가 함께 제공됨에도 불구하고 여전히 침해로부터 보안 안전성을 완전히 확보하지는 못한 상태이다. 따라서 본 논문에서는 제안하고 이를 기반으로 서비스 제공시 발생하는 보안사고 대비 보안침해 차단 비율에 대한 안정성 기반 운영 적정성까지 보장하는 제안을 제시하고자 한다[1].

이와 같은 보안성 확보를 위한 기본적인 틀로써는 통신 대역폭을 논리적인 영역으로 재구성하고 이를 다시 논리영역이라는 명칭 하에 네트워크 보안 등급을 구분 적용함으로써 기존에 제공되던 네트워크 인프라에 대한 큰 변화와 수정 없이 수용 가능하도록 제안하고자 한다.

이에 본 논문의 구성은 2장에서는 네트워크 접근 공격 유형, 논리적 네트워크 영역 단계적 분할 및 네트워크 대역폭과 보안구간 상호연계에 대해 분석하고, 3장에서는 접근권한 단계별 계층과 분류와 접근권한 추론모드 분석, 네트워크 정보보호 접근권한 추론모드 표준화를 제안하고, 4장에서는 논리적 통신 대역폭 구성과 운영정책 구현과 보안구간 제한 표준화 기반의 네트워크 보안구간 안정화 운영모드 구현과 분석 결과를 도출한다. 마지막으로 5장에서는 논문의 결론과 향후 연구 과제를 제시한다.

2. 관련연구

2.1 네트워크 접근 공격 유형

정보보호를 위한 다양한 방어방법들이 학회 또는 기업과 기관에 현존하고 있으며, 방어방법의 범주는 네트워크와 시스템 그리고 제반기기 또는 환경으로 구성을 나눌 수 있다. 하지만 가장 많은 공격 대상으로 급부상하고 있는 환경조건인 네트워크에 대한 접근부문 권한 공격을 1차적인 침해형태로 판단한다. 다만 최초의 공격성향은 기초적인 분석이 가능하지만 제2, 제3의 추가적인 공격의 문제점에 대한 분석이나 인식은 쉽게 판단되지 않는다[2,3].

또한 추가적인 네트워크 공격성향은 Passive 형태의 공격과 Active 형태의 공격으로 크게 분리되어지며, 한 단계 하위의 세부적인 구성으로는 네트워크 통신 방해, 네트워크 송수신 정보 가로채기, 정보의 정합성 훼손, 기초자료 및 정보의 굴곡으로도 분리된다. Table 1은 Active 형태의 공격성향으로 정보의 정합성 훼손에 준하는 공격현황을 보여주고 있다[4].

Table 1. Status of detecting malicious code in network

Criteria	2013			2014		
	Oct.	Nov.	Dec.	Jan.	Feb.	Mar.
Malicious code detection	155,936	176,759	125,723	113,283	82,896	283,687

※ The number of detected malicious codes is identified by a vaccine program for personal users of a major Korean vaccine company (data of the first-quarter of 2015 are not included as the data are not collected)

특정 침해에 대한 단순한 보안 제품과 솔루션을 갖는 제3의 보안시장은 다양한 공격성향에 대해 재해석이 필요한 네트워크 기반의 변형된 공격들이 발생하고 있다[5,6].

2.2 논리적 네트워크 영역 단계적 분할

통상 통신 라인을 네트워크 구간이나 또는 네트워크 대역폭으로 표현한다. 구간의 경우는 송신지와 수신지 간의 전체 통신 데이터의 수용 용량을 의미하지만 대역폭의 경우는 송신 및 수신지 간의 거리와 구간과는 무관하게 단편적으로 일시 송시되는 순간 용량을 의미하는 차이가 있다[7].

따라서 네트워크 용량은 2가지 또는 그 이상의 정의와 쓰임 및 구성에 따라 다양하게 그 형태와 구성을 정의한다. 이처럼 네트워크는 그 모양과 형태가 정의에 따라 Table 2와 같이 재정립이 가능한 유기적인 살아 있는 논리적인 영역과 형태를 갖는다.

Table 2. Partition according to stages of network area

Criteria	A-Area	B-Area	C-Area	D-Area
Segmentation area	Packet Destination -IP[ex.192]	Packet Destination -IP[ex.172]	Packet Destination -IP[ex.10]	Packet Destination -IP[ex. Broadcasting]

※ A, B, C, D-Area : Arbitrarily reorganized segmentation area

보안을 비율 대비 상당한 등급이상의 조건으로 구성하고자 하는 경우 이를 물리적인 전체 통신량으로 구성하는 단일 네트워크에서는 보안영역을 재 정의하고 구성하는 부분은 불가하지만 이를 논리적인 영역으로 분리하고 정의 하는 것은 솔루션 또는 이 외의 간단한 환경설정만으로도 구성이 가능하다. 이는 논리적인 보안정책의 단순 조정으로도 공격 또는 침입조건에 대한 다변화가 가능한 척도로 사용된다[8].

2.3 네트워크 대역폭과 보안구간 상호연계

다양한 네트워크 통신 서비스를 제공하는 통신 업체들은 네트워크 인프라와 연계되어진 보안 서비스를 제공함으로써 자유롭게 선택해서 사용 가능하도록 제안하고 있다. 다만 각각의 서비스는 별개의 금액을 요구하는 형태로 서비스 또한 별개의 제공이 가능하다. 따라서 많은 기관과 기업들 중에는 보안 분야의 서비스가 자체적으로 구성되어 있지 않는 경우 최적의 서비스를 선택해서 사용이 가능하다.

Table 3은 가장 흔히 그리고 가장 많이 제공 되어지는 네트워크 서비스 속도와 보안 구간을 보여준다.

Table 3. Support Type of network communication speed and security zone

Criteria	10base-X	100base-X	FDDI	1000base-X	10Gbase-X
Speed	10 Mbit/Sec 1.25 MB/Sec	100 Mbit/Sec 12.5 MB/Sec	100 Mbit/Sec 12.5 MB/Sec	1 Gbit/Sec 125 MB/Sec	10 Gbit/Sec 1.25 GB/Sec
Security	Arbitrary security section DMZ		-	Arbitrary security section DMZ	

추가적으로 통신 네트워크 보안 서비스를 제공하는 경우 보안기술로는 SSH(Secure Shell) 접속기술, HTTPS(hypertext transfer protocol over Secure Sockets Layer, HTTP over SSL) 통신 보안 프로토콜, NAT(Network Address Translation) 접속 IP영역 분리 등과 같은 형태의 서비스가 있다[9].

2.4 목적별 물리적 통신 라인 분리

지난 물리적인 통신라인 대역폭 확장에 따른 속도 보장과 같은 분야는 다소 하드웨어적인 인프라 구축을 위한 대표적인 형태였다. 하지만 보안성 강화를 위한 기반 기술로 망을 분리하는 망분리 기술을 이용한 사용분야별 또는 기관의 성격에 따른 조건별 분리를 통한 물리적 이원화 망 구성으로 서로 다른 망의 속도 보장 형태를 제공하는 방식과 스위칭 기술을 이용한 차세대 이더넷의 물리적 전송 통신 등이 존재한다[10,11].

3. 통신 대역폭 논리영역 적용 기반의 네트워크 보안구간 안정성 제안

현재 운영되는 통신 네트워크 서비스의 경우는 주어진 영역을 하나로 보고 이에 접근이 가능한 권한을 다수에게 또는 서비스가 필요한 요구자들에게 제공을 하는 형태의 서비스를 제공하고 있다. 다만 이러한 서비스의 문제점으로는 단, 한 번의 권한 접근 자가 침해를 받아 악성코드 등의 Back-Ground 공격성 스크립트를 가진 경우 전체 통신 네트워크 전체가 침해의 대상으로 공격에 따른 영역 분리가 불가능하다는 단점이 있다. 따라서 전체 통신 네트워크 영역을 논리적으로 성능과 연계된 비율로 재분리하고 이들 영역에 각각의 통신 네트워크 가상 아이디를 부여함으로써 접근권한과 접근영역의 재조정을 시행함으로써 침해를 차단한다.

따라서 본 논문에서는 기존 제공하고 운영되던 네트워크 통신 대역폭에 대한 정량적 비율을 논리적인 영역으로 재구성함으로써 통신 대역폭을 논리적인 영역으로 분리하고 각각의 영역을 네트워크 보안구간과 연계하는 제안을 한다.

3.1 접근권한 단계별 계층과 분류

제안하는 보안구간 안정화를 갖춘 통신 대역폭 논리적 영역으로 분리를 진행함으로써 분리된 각각의 영역을 네트워크 보안구간과 연계하는 방식으로 Fig. 1과 같이 정의한다. 단, 정의된 논리적 통신 네트워크 영역은 4개로 제한되어 있으나, 이는 특정한 네트워크 서비스를 진행하는 특정 서비스 대역폭에 적용되어 있는 것이다. 따라서 이와 다른 통신 네트워크 서비스에 대한 논리적인 영역 구분도 상관관계상 크게 구분 범주를 벗어나지 않으므로 동일한 조건으로 등급을 구분해도 안정화된 영역 보안 구성이 가능하다.

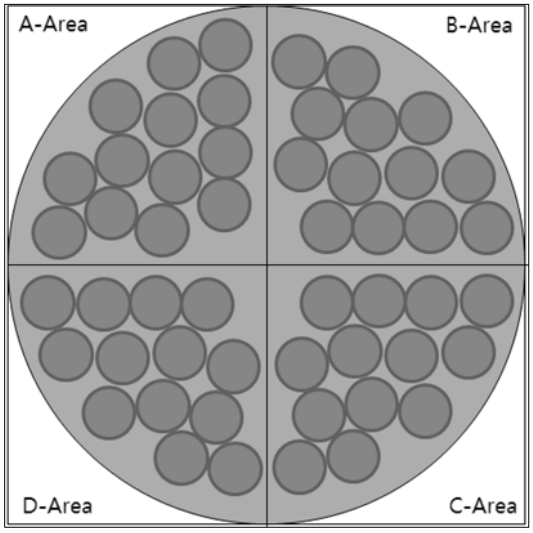

Fig. 1. Categorization of access authority for each network communication area and zone

*** 통신 대역폭 논리적 영역 구성 (특정 ISP 제공 사업자 서비스에 준함)**

- 전체 통신 대역폭 : 100M=25M * (4-a)개 영역
- 각 분할영역 사이의 발생 전체 공간 크기 : a
- 분할 영역별 크기 : (25M * n개 영역)-a
- 세부 조정 영역 크기 : 1Packet-size인 128byte

3.2 접근권한 추론모드 분석

다양한 ISP(Internet Service Provider) 사업자들이 제안하고 상품으로 제공 및 제안하는 통신 네트워크 제품과 솔루션들을 확인해 보면, Table 4와 같이 전체 통신 대역폭 외 3가지 기본 서비스 구성 논리적 영역 분리 구성이 가능하다. 물론 이러한 기본 통신 네트워크 논리적 분리 추론 방법론은 추론범주 영역을 가상으로 구성하되 해당 서비스를 제안하는 통신사만의 통계치 또는 해당 통신 네트워크를 단순 정량적 분리 방식인 2분법을 활용해서 단계적 상향 조건 변화를 이용 가능하다.

Table 4. Extent of network access authority deduction

Criteria	Total Communication Bandwidth	Total Space Extent Between Each Segmentation Area	Each Segmentation Area Extent	Tuning Area Extent
Inference category (Area)	100M=25M * (4-a) area	A (Arbitrary integer)	(25M * n area) -a	1Packet-size; 128byte

*** 통신 네트워크 영역 분리 -2분법 정의**

- Dichotomy, 2개의 서브 영역으로 분류하는 것으로 통신 네트워크 기준 구성방법의 대역폭을 데이터 송수신 전송 비율 대비 하나의 영역에 대해 또 다른 서브 영역으로 2분화 그룹 분류하는 것

다만, 통신 네트워크 논리영역에 대한 접근권한에 대한 가상화 영역 선정 추론 방식의 경우는 통상 L4 장비에 의해 서비스 정책을 제한하고 이외의 침입에 대한 보안성 확보는 일상적으로 방화벽을 활용한다. 따라서 통신 네트워크 인프라 구성을 위한 방화벽 구조와 구현에 대한 이해가 필요한 상황이다.

*** 가상화 논리영역 접근권한 추론정책 구현 방화벽 구조(구축 형태)**

- Screening Router : 통신 Packet 분석 및 Packet Filtering을 통한 접근제어 보안 Router 또는 Firewall
- Bastion Host : 소프트웨어적인 접근차단 구성으로 외부로부터 접속에 대한 1차 연결 호스트이며, 로깅 및 모니터링 정책 또한 구현되는 접근 허용과 차단 기능이 존재하는 Firewall 기능 구현
- Screened Host : Screened Subnet 또는 DMZ

3.3 네트워크 정보보호 접근권한 추론모드 표준화 제안

네트워크 보안성까지 확보하는 통신 네트워크 논리영역 적용 정책을 재정립함으로써 다양한 서비스 인프라 구조 적용상의 효율성과 보안정책 구현과정인 최적화 보안 등급을 확보하는 표준화 제안이 가능하다. 따라서 최적의 표준화 통신 네트워크 논리영역 구성을 위한 하나의 방안으로 Fig. 2와 같은 개별 네트워크 접근권한 추론 범주 표준화가 우선적으로 이루어져야 한다. 물론 가상화 방안을 기반으로 하고 있기 때문에 다소 추상적인 면이 강한 안정화 보안구간이라 칭하기도 하지만, 추론에 의한 영역을 세분화하고 접근권한 및 접근영역에 대한 등급을 영역으로 제한하는 등의 물리적인 차원과 논리적인 면이 융합된다면, 표준화 세부 보안영역을 제한 가능해진다.

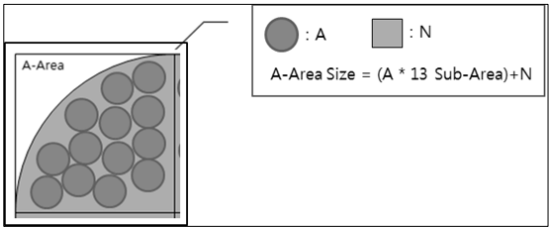

Fig. 2. Standardization of deduction category of separate network access authority

추후 각 2분법에 의해 세분화 되어 나누어진 영역에 대한 증명이 반드시 이루어져야 한다.

*** 표준화 제안 아이디어**

- Idea 기본 조건 : 통신량의 기본 단위는 Packet으로 크기의 변화가 없는 일정한 정해진 크기로 제안
- Idea-01 : 각 Area별 통신 량 재구성을 기반으로 1차 Load-Balancing 진행
- Idea-02 : 통신 대역폭 2차 Load-Balancing의 구성 방안으로는 A-Area를 통신 유입되는 경로로써 이후 통신량에 따라 B, C, D까지 운영

4. 네트워크 보안구간 안정화 운영에 따른 결과

네트워크 보안구간 안정화 운영이 본 논문에서 가장 최종적으로 얻고자 하는 결과로써 이러한 안정성을 확보한 통신 네트워크 논리영역 구성을 위한 지속적인 실무 적용과 향후 최종 제안하는 안정성 확보 보안성에 대한 객관성과 효율성을 확보함으로써 논리적 제안 방법은 최적의 결과를 이끌어올 것이다.

4.1 논리적 통신 대역폭 구성과 운영 정책 구현

최종 제안되어지는 통신 네트워크 논리영역의 보안 안정성 확보 기준의 대역폭 구성과 운영정책에 따른 최적의 구현결과를 도출하기 위한 제안으로 Table 5와 같이 이원화된 두 영역인 논리적 통신 대역폭과 물리적 대역폭 간의 운영정책 및 분할영역 매핑이 필요하다.

Table 5. Operation policy and partition domain for logical communication bandwidth and physical bandwidth

Criteria	10base-X	100base-X	FDDI	1000base-X	10Gbase-X
Speed	10 Mbit/Sec 1.25 MB/Sec	100 Mbit/Sec 12.5 MB/Sec	100 Mbit/Sec 12.5 MB/Sec	1 Gbit/Sec 125 MB/Sec	10 Gbit/Sec 1.25 GB/Sec
Applied Segmentation Area	A, B, C, D -Area(ALL)	A, B, C, D -Area(ALL)	A, B, C, D -Area(ALL)	A, B, C, D -Area(ALL)	A, B, C, D -Area(ALL)
Inference Category	Total communication bandwidth : 100M=25M * (4-a) area Total space extent between each segmentation area : a Eacy segmentation area extent : (25M * n area)-a Tuning Area Extent : 1Packet-size; 128byte				
Policy1	1st Load-Balancing process based on traffic reorganization of each area				
Policy2	As the 2nd Load-Balancing organizing method of communication bandwidth, A-Area is used as a communication inflow route. Afterward, B. C. and D will be used depending on traffic.				
Security	Arbitrary security section DMZ		-	Arbitrary security section DMZ	

제공되는 통신 네트워크 서비스 대역폭을 기준으로 다양한 네트워크 토폴로지를 선정 및 각각의 토폴로지가 제안하는 접속 방식을 기준으로 논리적 적용영역을 구성한다. 물론 구성 시에는 반드시 제안하는 통신 네트워크 논리영역에 대한 분할 추론범주가 제시되어야 하며, 이를 기준으로 영역에 대한 운영 정책인 접속 아이디어를 선정 및 보안 정책과 연동 등을 구상해야 한다. 이러한 과정이 끝나면, 최종 분석결과에 대한 신뢰도를 향상 시킬 수 있다.

4.2 네트워크 보안구간 안정화 운영모드 구현과 분석 결과

제안하는 환경을 기준으로 하는 제반형태를 구성한 최종 결과는 Table 6과 같은 통신 네트워크 논리영역 구성과 적용분할 영역, 운영정책과 최적화된 보안정책을 적용함으로써 단계적 보안 등급에 대한 서비스별 선정과 비율 표준화 단계가 결정되었다.

2분법에 의해 본 논문에서 제안한 4개의 논리영역 최종 비율 결정은 다양한 서비스별 대역폭에 따라 적개는 2개로부터 많게는 지속적인 성능 확인과정을 거쳐서 증가가 가능하다. 물론 최대 분리 가능한 논리영역의 개수가 곧 보안성을 확보하는 척도는 아니지만, 접근 논리 영역의 분리는 직접적인 침해에 대한 단순 접근을 1차적으로는 차단하는 효과가 있다.

Table 6. Analysis result of stabilization following realization of stabilizing operation mode of network security zone

Criteria	10base-X	100base-X	FDDI	1000base-X	10Gbase-X
Speed	10 Mbit/Sec 1.25 MB/Sec	100 Mbit/Sec 12.5 MB/Sec	100 Mbit/Sec 12.5 MB/Sec	1 Gbit/Sec 125 MB/Sec	10 Gbit/Sec 1.25 GB/Sec
Applied Segmentation Area	A-Area	A, B-Area	A, B, C, D -Area	A, B, C -Area	A, B, C, D -Area(ALL)
Management Policy	1. 1st Load-Balancing process based on traffic reorganization of each area 2. As the 2nd Load-Balancing organizing method of communication bandwidth, A-Area is used as a communication inflow route. Afterward, B. C. and D will be used depending on traffic.				
Security Policy	1. Application of each section and limitation to accessible network section 2. Network extent mapping of each section : Inverse proportion to speed (limitation to accessible area)				
Applied Analysis Result	Security level A-	Security level A--	Security level A	Security level A+	Security level A++

이처럼 본 논문의 표준화된 결과 값을 바탕으로 다른 다양한 통신 네트워크 인프라 또는 서비스 등에 적용하는 단계적 확장 실험이 필요하다. 또한 Fig. 3은 제안하는 본 논문이 원하는 결과 도출 값에 대한 시각적 확인을 위한 방안으로 도식을 제안하고 각 논리영역별 분포도 또한 확인할 수 있도록 구성을 포함하고 있다.

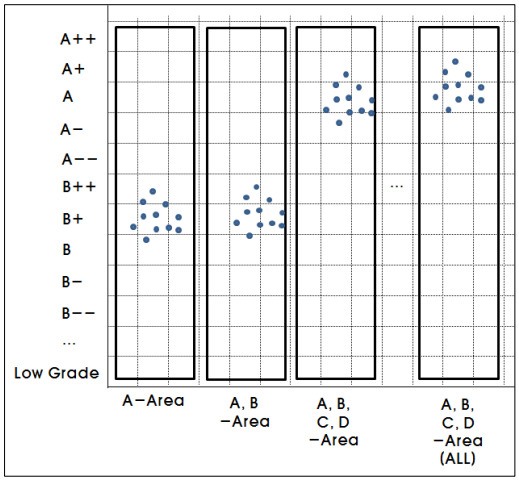

Fig. 3. Relationship between network security level and network security zone

5. 결론

본 논문에서는 현재 제공되는 네트워크 통신상의 물리적 기반시설에 대한 용량을 활용하는 기업과 기관들의 현황과 구성 방법 등을 확인함으로써 네트워크 통신라인을 통한 침해와 불법적인 접근에 대한 보안성 강화를 위한 방법론 및 표준화 접근제어 등이 자세히 논리적인 증명으로 제시되고 있다.

이와 같은 통신 대역폭 상의 논리영역 가상화 기반의 형태는 하나의 통신 용량을 가진 단일 인프라를 재구성하는 부분에서 세부적으로 또는 단계적으로 영역을 분리하고 각 나누어진 영역마다 최상위 용량의 1:N의 비율을 적용하는 단순 산출조건으로 구성만을 분할하는 등의 접근제어를 제안함으로써 네트워크 보안구간을 안정화하는 기초자료를 파악하는 것이며, 이는 네트워크의 물리적인 구성과 운영 형태를 논리영역과 연계하는 인프라 재구성과 같은 접근제어로써 물리적인 네트워크 보안 안정화 운영을 이루는 방안이기도 하다.

이처럼 정보보안의 한 범주인 네트워크 통신 인프라에 대한 물리적인 구간 가상화와 가상화 구간에 대한 통신 비율에 대한 조정으로 제3의 불법적인 접근에 대해서 접근 가능한 영역의 축소를 통해 단순하지만 가장 간단한 방법으로 그 공격의 비중과 Hit 수를 최소화 한다.

향후 연구방향으로는 최초 제공되는 ISP(Internet Service Provider)의 단일 통신영역과 비율을 서로 다른 통신사간의 통신 라인의 조합으로 묶어서 단위 또는 단계적 하위 네트워크 통신 대역폭에 대한 제한을 없앤 형태의 제안과 연구가 필요하다.

References

[1] H. J. Suh, “An Improved Algorithm of Distributed QoS in Real-time Networks”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 7 No. 1, pp.53-60, 2012.

[2] S. H. Hong, “Analysis of DDoS Attack and Countermeasure: Survey”, Journal of digital convergence, Vol. 12 No. 1, pp.423-429, 2014.

[3] S. H. Yoon, H. M. An, M. S. Kim, “Study on Classification Scheme for Multilateral and Hierarchical Traffic Identification”, Korea Information Processing Society, Vol. 3 No. 2, pp.47-56, 2014.

[4] Korea Internet & Security Agency, “3 March Incident Response Internet statistics”, pp.141, 2014.
[5] J. Y. Seo, M. J. Lee, “An Extened Virtual LAN System Deploying Multiple Route Servers”, Korea Institute of Information Scientists and Engineers, Vol. 29 No. 2, pp.117-128, 2002.
[6] H. D. Lee, H. T. Ha, H. C. Baek, C. G. Kim, S. B. Kim, “Efficient Detction and Defence Model against IP Spoofing Attack through Cooperation of Trusted Hosts”, Journal of the Korea Institute of Information and Communication Engineering, Vol. 16 No. 12, pp.2649-2656, 2012.
DOI: http://dx.doi.org/10.6109/jkiice.2012.16.12.2649
[7] H. J. Lee, H. T. Lee, H. S. Shin, “A Study On Ubiquitous Sensor Network Technologies”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 4 No. 1, pp.70-77, 2009.
[8] Y. G. Bae, C. H. Yoon, G. J. Kim, “TCP Congestion Control of Transfer Rate-based in End-to-End Network Systems”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 1 No. 2, pp.102-109, 2006.
[9] S. Jung, M. J. Lee, “An Efficient Multipath Routing with Dynamic Load Balancing”, Korea Institute of Information Scientists and Engineers, Vol. 28 No. 3, pp.406-416, 2001.
[10] Y. H. Lee, S. J. Yoo, “The Construction of Logical, Physical Network Separation by Virtualization”, Convergence security journal, Vol. 14 No. 2, pp.25-33, 2014.
[11] J. W. Youn, J. H. Kim, J. Y. Shin, K. J. Kim, “A Design and Implementation of OTU4 Framer for 100G Ethernet”, The journal of Korea Information and Communications Society, Vol. 36 No. 12, pp.1601-1610, 2011.

서 우 석(Woo-Seok Seo) **[정회원]**

- 2006년 8월 : 숭실대학교 정보과학대학원 정보통신융합학과 (공학석사)
- 2013년 3월 : 숭실대학교 일반대학원 컴퓨터학과 (공학박사)
- 2006년 4월 ~ 2012년 12월 : 서울특별시용산구시설관리공단 전산총괄
- 2012년 12월 ~ 현재 : 주식회사 이지서티 보안사업본부 이사, 개인정보보호센터 센터장

<관심분야>
정보보호, 네트워크 보안, Network Design, 개인정보