情報保護學會論文誌
第 21 卷 第 4 號, 2011. 8

통합 보안정책 알고리즘 적용에 따른 최적화 방어 시스템 구축에 관한 연구

서 우 석[1†], 전 문 석[2‡]
[1]숭실대학교 일반대학원, [2]숭실대학교

A Study on Building an Optimized Defense System According to the Application of Integrated Security Policy Algorithm

Woo-seok Seo,[1†] Moon-seog Jun,[2‡]
[1]Soongsil Graduate School, [2]Soongsil University

요 약

본 논문은 다양한 네트워크 보안장비들이 갖는 고유의 보안정책들을 하나의 시스템 내에 단일 알고리즘으로 구현함으로써 네트워크를 기반으로 하는 공격 발생 시 최적의 통합 보안정책에 대한 연구이다. 실험을 위한 정책들은 Firewall, VPN(Virtual Private Network), IDS(Intrusion Detection System), IPS(Intrusion Prevention System)가 갖는 고유의 방어정책을 상호 조합하는 과정을 통해 최적의 보안 시스템을 구현하기 위한 실험을 한다. 또한, 보안정책 설정에 따른 시스템 부하와 빠른 탐지, 신속하고 효율적인 방어를 위한 통합 메커니즘 설계 및 네트워크 인프라 구현 기반을 확보하는데 의의가 있다.

ABSTRACT

This study is conducted to examine the optimal integrated security policy based on network in case of attacks by implementing unique security policies of various network security equipments as an algorithm within one system. To this end, the policies conduct the experiment to implement the optimal security system through the process of mutually integrating the unique defense policy of Firewall, VPN(Virtual Private Network), IDS(Intrusion Detection System), and IPS(Intrusion Prevention System). In addition, this study is meaningful in that it designs integrated mechanism for rapid detection of system load caused by establishment of the security policy and rapid and efficient defense and secures basic network infrastructure implementation.

Keywords: Integrated Security Algorithm, Security Policy, Parallel process, Sequence process, Defense rate, Infringement rate, Obstruction rate

I. 서 론

네트워크를 기반으로 하는 보안 침해사고는 매년 지속적으로 증가하고 있으며, 침해대응을 위한 보안 솔루션은 새로운 복합적 보안정책 구현 알고리즘(이하 "보안 알고리즘"이라 한다.)과 정책을 개발하는 단계에서 다양한 보안 장비가 갖는 특화된 보안정책을 조합함으로써 최적의 정책설정 알고리즘과 시스템구현을 위한 단계로 변화하고 있다. 이러한 변화는 전혀 새로운 공격기법보다는 기존 공격패턴과 특성을 이용한 변

접수일(2010년 11월 23일), 수정일(2011년 5월 16일), 게재확정일(2011년 6월 23일)
† 주저자, ssws2003@yahoo.co.kr
‡ 교신저자, ijcsns@gmail.com

화된 침해가 많다는 것이다. 추가적인 공격에 대한 방어정책 구현보다는 과거에 많이 이용되어진 공격패턴을 완벽하게 분석하는 형태로 변화했다. 과거에는 Firewall, VPN(Virtual Private Network), IDS(Intrusion Detection System), IPS(Intrusion Prevention System)를 특정한 공격에 대한 방어목적으로 단계별로 구축하였으나, 현재는 하나의 시스템 내에 4가지 방어정책을 통합하는 형태로 발전하고 있다. Firewall은 Firewall-IDS, VPN-IPS와 같이 한 번의 구축으로 2가지 이상의 보안정책 구현을 위한 통합된 형태로 진화하고 있다. 그러나 특화된 보안 장비만의 보안정책 고유기능을 완벽히 분석하지 않고 단순히 2가지 이상의 기능만을 적용하고자 하는 개발로 인해 시스템 성능 대비 최적의 보안정책 구현에 대한 새로운 취약점이 발생했다.

따라서 본 논문에서는 기존 보안장비 또는 신규로 설계되어지고 개발되어지는 솔루션에 대한 최적화를 위한 기반과 최적화를 통한 최종 보안정책 등의 적용에 효율성을 극대화 하고자 하며, 기본방향은 다수의 장비 또는 솔루션을 단일 시스템 내에 일원화하고 집약함으로써 그 결과를 얻고자 한다. 또한, 적용 시스템 성능과 보안정책 병렬처리를 위한 다양한 실험을 통해서 다차원 정책 적용에 대한 문제점과 표준화된 정책구현이 절실하게 필요한 시점이 되었다[1][2].

본 논문의 구성은 2장에서는 기존에 운영되었던 네트워크 인프라 구성기법에 대해 분석하고, 3장에서는 네트워크 보안장비 기능과 인프라 기반의 사례 분석에 대해 설명하며, 4장에서는 네트워크 보안장비 구현을 위한 최적화 기반의 인프라를 제안한다. 5장에서는 실험을 통한 결과를 도출하고, 마지막으로 6장에서는 논문의 결론과 향후 과제를 제시한다.

II. 관련연구

2.1 최근 네트워크 보안장비 현황

다양한 침해패턴들이 특이성과 고유성을 가지고 공격하는 기법이 날로 증가함에 따라 보안정책과 정책구현 알고리즘은 많은 기술적인 진보를 했다. 또한, 최근에는 네트워크 인프라 내에 구축되어진 보안장비들을 종합 관제함으로써 새로운 장비 추가보다는 활용도 면에서 많은 기술적인 부문이 변화되었다.

ESM(Enterprise Security Management) 역시 기존 네트워크 보안 인프라를 활용하는 면에서 구성하는 통합 관제 보안 시스템이다. [표 1]은 현재 가장 많이 운영되어지는 보안장비에 대한 현황이다[3][4].

[표 1] 최근 보안장비 현황

구분	과거 운영 보안기기 형태 (개별운영)	현재 운영 보안 솔루션 형태 (통합운영)
내용	1. Firewall 2. VPN 3. IDS 4. IPS 5. ESM	Security Unit Integration

* 적용 순서 : 1 ~ 5

2.2 네트워크 보안장비 인프라 구성 분석

최근 보안장비들은 서로 다른 보안정책을 동일 시스템 상에서 구현 가능한 모델을 제시하고 있으며, TCP/IP 계층 모델 프로토콜 기반 하에서 유사기능을 통합구현 가능한 보안정책 기반의 네트워크 보안장비 비중이 가장 높다. 하지만 보안정책으로 탑재되어지는 보안정책 구현 알고리즘 구동방법에 따라 시스템 성능과 비례 또는 반비례 하는 상관관계를 갖는다. 따라서 해당 보안정책 구현 알고리즘 통합에 따른 최적화 분석이 요구되어 진다.

분석방법으로는 보안 정책 운영에 따른 시스템 성능 대비 최적의 알고리즘 구현비율을 실험하고 분석한다. 이때 발생 가능한 중복성과 서비스 프로세스 운영 시 각 단계별 프로세스 로딩과 적용을 위한 준비단계에 침입 가능한 취약성까지도 분석범주에 포함한 객관적인 분석수치를 확인해야 한다[5][6].

III. 네트워크 보안장비 기능과 인프라 기반의 사례 분석

3.1 각 장비별 기능과 운영 모드

각각의 보안장비마다 [표 2]와 같이 고유한 특성화된 기능과 운영 모드를 가진다. 보안장비별 각 고유한 기능을 내부 시스템에 보안 프로그램을 탑재함에 따라 구현이 가능한 기능별로 분류하고 또한, 운영모드의 경우는 각 보안장비인 Firewall, VPN, IDS, IPS가 시스템에 탑재되어진 고유한 기능과 특화된 기능을 수행하는 솔루션을 관리 및 모니터링 등의 향후 최종

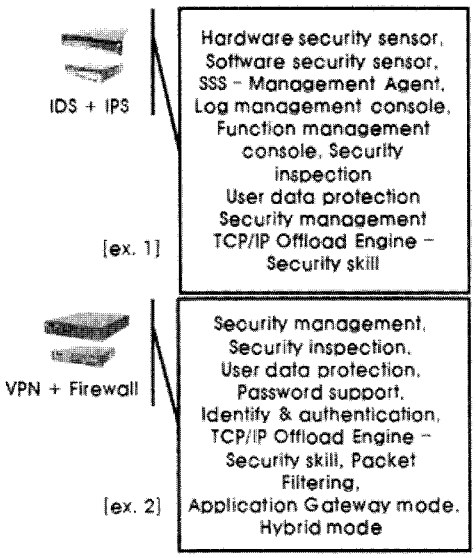
침해결과와 운영 상의 문제점을 보고서화 가능한 부분을 운영모드로 구성했다. 따라서 최종 실험과 제안에 있어서 각 보안장비별 기능과 관리모드에 따른 간략한 보고서를 통해서 통합 보안정책 알고리즘 적용에 따른 최적화 방어 시스템 구축에 유연성을 가지게 된다. 제안되어지는 최적화 방어 시스템 구현에 앞서 과거에는 각 분류된 방어정책을 보안정책 구현 알고리즘으로 구현하고 실제 장비에 탑재함으로써 공격 패턴에 따른 단위별 방어를 한다[7].

〔표 2〕 보안장비별 기능과 운영 모드

구분	기능	운영모드
Firewall	Access Control, Network Address ,Translation) Authentication, Audit record, Trace function	Packet Filtering, Application Gateway mode, Hybrid mode
VPN	Tunnelling protocol, Fix Communication line concept, Extranet and Wild Intranet	Security management, Security inspection, User data protection, Password support, Identify & authentication, TCP/IP Offload Engine-Security skill
IDS	Raw Data Collection 〔 HIDS / NIDS 〕, Data Reduction and Filtering, Analyis and Intrusion , Detection 〔wrong use detection / beat all detection 〕	Hardware security Sensor, Software security Sensor, SSS-Management Agent, Log management console, Function management console * SSS : Software security sensor
IPS	Virtual Patch, Bad traffic, Deny〔Known traffic〕, VoIP-Defense, Network stability, solubility security, Security flat-form embodiment	Security inspection, User data protection, Security management, TCP/IP Offload Engine-Security skill

3.2 최적화 보안장비 인프라 구성을 위한 사례분석

특정한 보안 기능을 구현하는 단일 보안정책 구현 알고리즘 형태가 시스템 성능 향상에 따라 통합 구현을 통한 관리의 용이성과 빠르고 효과적인 보안정책 구현 알고리즘 형태로 〔그림 1〕과 같이 변화하고 있다. 하지만 변화의 범주가 극히 제한적이고 다양한 보안정책 통합에 따른 객관적인 성능 대비 방어결과가 최적화 및 표준화 되어 있지 않다.[8][9][10].



〔그림 1〕 통합 보안 알고리즘 탑재 장비 운영형태

IV. 네트워크 보안장비 구현을 위한 최적화 기반의 인프라 제안

4.1. 장비별 보안 인증 최적화 기반 제안

통합 보안정책 구현 알고리즘 적용에 따른 최적화 보안 구현과 최종 제안 시스템 구현을 위한 1차적인 통합 범주는 〔표 3〕과 같다. 통합 범주는 PP(Parallel process)와 SP(Sequence process)로 분류하고 각각의 통합 가능한 보안 구현부문을 제안한다.

** PP(Parallel process) 구현 방안*

〔표 3〕에서 제안되어진 침해 방어를 위한 솔루션 또는 장비에 대한 구현을 위한 방안으로 병렬형태를 적용하는 경우에는 동시에 적용되어지는 각 장비마다 고유의 방어 특성과 특화된 방어 정책과 솔루션을 일

시에 적용함으로 짧은 시간에 빠른 방어결과를 도출하고자 하는 방안이다. 다만, 이와 같은 경우에는 대량의 침해 공격이 발생시에는 현저한 속도의 저하가 발생 가능하다. 따라서 무조건 병렬형태를 적용하는 단순한 실험이 아닌 최종 실험결과에 따른 최적화된 방안을 제안한다.

Parallel_process={Select_one_over(Firewall, VPN, IDS, IPS)||In-packet_rate||Policy_Process_Speed(per sec)}

** SP(Sequence process) 구현 방안*

〔표 3〕에서 제안되어진 침해 방어를 위해 제안하는 SP 형태의 경우에는 각 고유한 방어정책과 처리기술을 탑재한 보안장비를 순차적으로 구성함으로써 각 단계별(a~d) 필터링 등의 처리결과를 다시 다음 단계에서 또 다른 정책에 의해 제어하는 형태를 제안하는 방안을 적용한다.

a) Sequence_process={Select(Firewall)}
b) Sequence_process={Select(VPN)}
c) Sequence_process={Select(IDS)}
d) Sequence_process={Select(IPS)}
e) Sequence_process'={Regulation(In-packet_rate)}
f) Sequence_process''={Policy_Process_Speed(per sec)}
g) roof{a~d}

〔표 3〕 네트워크 보안 장비 구축 범주

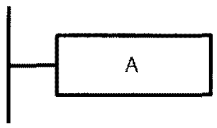
등급	Firewall	VPN	IDS	IPS
Firewall	-	SP	SP	SP
VPN	PP	-	SP	SP
IDS	PP	PP	-	SP
IPS	PP	PP	PP	-

또한, 통합, Parallel, Sequence는 〔그림 2〕와 같이 Process Flow를 3가지 경우로 구분하고 실험을 통한 최적화와 표준화된 보안정책 구현 알고리즘을 탑재한 시스템을 제안한다.

Parallel Flow의 경우는 Parallel-Process-AREA와 Sequence Flow가 같은 특징인 Series-Process-AREA를 갖는다. 따라서 최종 통합 Flow를 구현하기 위한 선택적 Flow는 Parallel 구

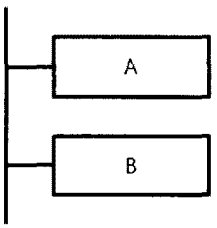
[Integration process Flow]

[1] Firewall+VPN
[2] Firewall+IDS
[3] Firewall+IPS
[4] Firewall+VPN+IDS
[5] Firewall+VPN+IPS
[6] Firewall+VPN+IDS+IPS



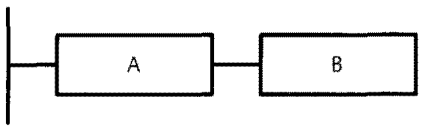
[Parallel process Flow]

[1] VPN and Firewall
[2] IDS and Firewall
[3] IDS and VPN
[4] IPS and Firewall
[5] IPS and VPN
[6] IPS and IDS



[Sequence process Flow]

[1] Firewall + IDS
[2] Firewall + IPS
[3] Firewall + IDS + IPS
[4] VPN + IDS
[5] VPN + IPS
[6] VPN + IDS + IPS
[7] IDS + IPS



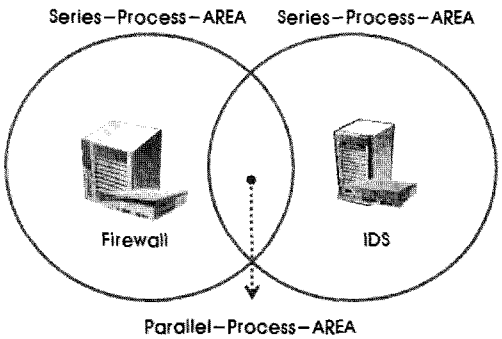
〔그림 2〕 Process Flow

현을 적용한 것이다. 또한, 최종 통합 보안 알고리즘 구현을 위한 최적화 기반의 인프라는 Parallel Flow이다. Parallel Flow에 속하는 Parallel-Process-AREA는 제안한 다양한 보안정책 또는 장비의 조합을 병렬형태로 구성함으로써 한번의 접근제어를 기반으로 다양한 보안정책을 수행하고 그 결과를 얻는 방식의 범주에 속하는 모든 방법을 말한다. 따라서 해

당 영역내에 속하는 모든 Process Flow의 경우는 하나의 통합된 시스템 내에 단일 알고리즘을 기반으로 다수의 정책을 구현하는 형태로 구성한다. 다만, 공격과 방어를 통한 성능에 대한 실험을 통해서 최종 제안 부문을 확인해야 한다.

4.2. 병렬구성 기반의 방어 인프라 제안

통합 보안 알고리즘 구현을 [그림 3]과 같이 간략화한 Parallel Flow 구현도의 Parallel-Process-AREA를 통해 최적화 기반의 인프라를 제안한다.



[그림 3] Parallel 구현도

또한, [그림 3]의 Firewall과 IDS 보안 기능을 상호 AREA로 구분해서 통합 보안정책 구현 알고리즘을 구성한다. [표 4]는 Parallel Flow AREA 구성에 대한 기능부문을 2가지의 형태로 구성한 것을 나타낸다.

[표 4] Parallel Flow AREA 구성

구분	Series -Process-AREA	Parallel -Process-AREA
Firewall	Access Control, Network Address, Translation, Authentication, Audit record, Trace function	기능조합 [Firewall +IDS]
Web - Firewall	Raw Data Collection [HIDS / NIDS], Data Reduction and Filtering, Analyis and Intrusion, Detection [wrong use detection / beat all detection]	

V. 최적화 제안 인프라의 운영을 위한 부하와 공격에 대한 방어 실험

5.1. 실험환경

공격을 시행하는 Attack 시스템은 CentOS를 탑재한 서버로 구현하고 공격 툴은 SQL-Injection과 TCP, UDP Flooding 공격을 6가지 통합 보안정책 구현 알고리즘인 Parallel Flow에 시행함으로써 공격기법에 따른 방어기법의 방어결과를 도출한다. 또한, [그림 4]와 같이 통합 Process Flow 상에 공격을 통해 방어비율(Defense rate)인 각 보안장비 또는 보안 솔루션 설정 정책의 가동률, 침해비율(Infringement rate)인 실제 불법적인 침해 접근 대비 총 연결 Session 비율을 반영한 비율, 차단비율(Obstruction rate)인 방어비율 상의 정책 또는 방어 솔루션 가동률 대비 침해비율의 상관관계로 최종 정책설정 비율을 100%로 설정하고 정책을 무력화한 침해비율을 제외한 비율에 대한 실제 침해로 인한 사고비율을 구하고 등급 선정 표에 의해서 시스템 성능을 측정한다.

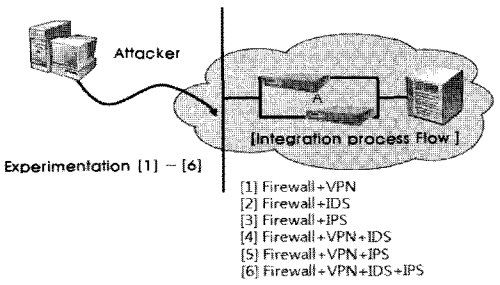
** 방어비율(Defense rate)*

초기 네트워크 인프라를 구성하는 시점 또는 기존 보안장비를 활용함으로써 재구성시에 각 보안장비 초기 정책설정 비율에 의거 정책을 반영하는 비율을 의미한다.

Defense_rate = {Unit_Policy_Setting_rate} - Depending on condition (Setting of Security manager skill)

** 침해비율(Infringement rate)*

전체 접근 Session 값을 100%로 기준을 설정하



[그림 4] 실험환경

고 불법 접근하는 Session 값을 비율로 환산함으로써 최대 침해 건수는 1이지만, 장애비율(Hindrance_counter) 테이블을 등급별로 G[grade]-1 ~1, G-2 2~4, G-3 5~7, G-4 8~10, G-5 11~ 와 같이 초기값을 설정한 상태에서 최대 침해 비율 "1"에 대한 침해결과에 최종 침해로 인한 장애 값까지 합산한 값으로 구성. 단, Hindrance_counter 테이블의 초기값은 다양한 장비 또는 솔루션 운영과 관리에 따른 결과에 따라 값이 설정이 변경 가능하므로 향후 여러 다른 환경에서 실험을 통한 결과를 얻을 수 있도록 향후연구에 적용함으로써 표준화 Hindrance_counter 테이블을 연구해야 한다.

Infringement_rate={(Infringement_session_counter/all_access_session_counter)+hindrance_counter

** 차단비율(Obstruction rate)*

방어비율과 실험을 위한 Hindrance_counter 테이블의 초기값에 의한 침해비율을 기준으로 전체 접근비율 대비 장애로 인한 비율을 각 등급별로 5% 내외의 차단비율로 구성한다.

Obstruction_rate={Defense_rate||Hindrance_counter_initial_table_value||each_grade ±5%}

5.2. 보편화된 네트워크 공격 방어를 위한 인프라 적용 결과 분석

6가지 통합 보안 알고리즘 구현을 실험한 결과 〔표 5〕와 같은 3가지 보안 등급 판정을 위한 선정 등급에 의거 〔표 6〕와 같은 각각의 실험 지표 비율과 등급이 결정되었다. 통합 보안정책 구현 알고리즘 구현은 무조건 다수의 보안 알고리즘을 탑재한다고 해서 침해방어에 대한 최적화가 이루어지는 것이 아니며, 공격에 대한 시스템 부하 량과 처리 성능에 따라 급격히 변화가 발생한다. 따라서 통합 보안정책 구현 알고리즘을 탑재하고 운영하기 위한 시스템에 정책과 알고리즘에 대한 Load-Balancing이 반드시 필요하다.

또한, 다양한 보안장비 조합(실험을 통한 다양한 옵션 형태의 보안기기 조합)에 따른 최적화된 통합 보안 알고리즘을 구현한 시스템은 각 단위별 보안장비의 고유한 보안정책을 기준으로 실험을 시행한 결과로써

〔표 5〕 등급 선정 표

〔단위 : %〕

등급	1	2	3	4	5
방어비율	100~95	94~90	89~85	84~80	79~
침해비율	~2	3~5	6~8	9~11	12~
차단비율	~5	6~10	11~15	16~20	20~

미시적인 최적화를 위한 제반사항을 등급형태로 분리하여, 제안한 것이다.

통합 보안 알고리즘을 구현한 시스템에 대한 실험결과인 〔표 6〕의 각 보안장비 조합에 따른 최적화 시스템 구현을 위한 등급구분은 각 방어, 침해, 차단비율에 해당하는 방어 등급을 가장 기본적인 선정등급으로 보안 인프라 구성을 해야만이 가장 최적화된 보안 인프라를 구성 가능하다.

분석결과에 따른 예를들면, Firewall+VPN+IPS 구성의 경우 기본으로 하는 통합 보안 시스템은 해당 기기들이 지원 가능한 고유한 보안기능을 최소한 2등급의 방어비율로 지원 가능한 정책을 대상으로 90%(90~94%) 이상의 기능을 활용하고 장애 발생 가능 비율을 구성하는 테이블 상에서 2% 초과 6% 미만의 비율의 침해 가능성과 10%(3등급 차단비율의 15%이내까지 비율 폭 확대 가능) 내외의 차단비율로 구성을 하면, 가장 기본적인 고유한 방어기능을 가지고 미시적인 최적화 시스템 구성이 가능하다.

따라서, 실험결과에 따른 각 구성별 방어, 침해, 차단비율의 최적화 선정 범위는 방어(2등급), 침해(2등급), 차단(3등급)까지 가능하다. 이는 다양한 보안 기기들의 정책적용 솔루션 선정과 보안기기의 하드웨어 선정 범위에 따라 다소 등급간의 혼용범위가 확대 또는 축소되는 경우도 발생하며, 향후 지속적인 연구를 통해서 실험을 위한 솔루션과 기기에 대한 표준화 역시 요구된다.

〔표 6〕 통합 보안 알고리즘을 구현한 시스템에 대한 실험결과

〔단위 : 등급〕

구성	방어비율	침해비율	차단비율
Firewall+VPN	1	1	1
Firewall+IDS	1	1	1
Firewall+IPS	1	1	1
Firewall+VPN+IDS	1	2	2
Firewall+VPN+IPS	2	2	3
Firewall+VPN+IDS+IPS	3	4	5

따라서 공격에 대한 시스템 부하 량과 처리 성능을 감안한 최종 최적화 구현은 다차원의 조건들을 반영한 통합 보안정책 구현 알고리즘을 구현해야 만이 최적의 방어가 가능하다.

VI. 결론

본 논문에서는 다양한 보안정책 구현 알고리즘을 탑재한 보안장치에 대해서 특화된 기능과 실행코드를 알아보았다. 또한, 통합 보안 알고리즘을 구현하기 위해 기능조합 Firewall+VPN를 비롯한 6가지 형태에 대한 실험을 시행함으로써 최적의 통합 보안정책 구현 알고리즘 등급과 실험을 통한 시스템 성능 비율을 확인했다. 물론 공격에 대한 부하 량이 통합 보안정책 구현 알고리즘을 탑재하고 운영하는 시스템의 방어정책에 대한 척도로 밝혀졌다. 로드밸런싱 역시 반드시 필요한 탑재 솔루션임을 재차 확인했다.

향후 연구방향으로는 확장된 실험환경과 새로 개발되어지는 다양한 보안장치의 초기 도입 이전의 지속적인 보안성능 연구와 최적화 모델에 대한 연구를 각 보안 장치의 보안정책 구현 알고리즘 기능으로 구분하고 구분되어진 범주를 기준으로 다양한 네트워크 인프라에 적용하여 누적된 정보를 표준화된 통합 보안정책 구현 알고리즘 형태로 구현하는 것이다.

또한, TCP/IP Layer 전 계층에 대해서 보안장비별로 구분해서 실험을 통한 결과를 지속적으로 연구가 추가되어야하며, 실험을 위한 솔루션과 기기에 대한 표준화 역시 요구되고 마지막으로 최적화를 통한 보안장비 통합 시 보안정책 구현 알고리즘을 탑재함으로써 가장 표준화된 시스템을 구현하도록 6가지 경우를 포함한 통합보안관리 시스템인 ESM(Enterprise Security Management)까지 다양한 보안장비에 대해 다각도의 실험이 필요하며, 실험을 위한 기초자료인 Hindrance_counter 테이블의 초기값에 대한 다양한 설정값을 구하는 연구가 이루어져야 한다.

참고문헌

[1] Gouda, M.G and Liu, A.X, "Structured firewall design," Computer networks, vol.51, no.4, pp.1106-1120, Mar. 2007.

[2] Zeeshan A, Imine A, and Rusinowitch M, "Safe and Efficient Strategies for Updating Firewall Policies," Lecture notes in computer science, vol.6264, pp.45-57, Aug. 2010.

[3] Quttoum, A.N, Otrok, H, and Dziong, Z, "A collusion-resistant mechanism for autonomic resource management in Virtual Private Networks," Computer communications, vol.33, no.17, pp.2070-2078, Nov. 2010.

[4] Hubballi N, Roopa S, and Ratti R, "An Active Intrusion Detection System for LAN Specific Attacks," Lecture notes in computer science, vol.6059, pp.129-142, June 2010.

[5] 천준호, 장근원, 전문석, 신동규, "DDoS 공격에 대한 방화벽 로그 기록 취약점 분석," 한국정보보호학회논문지, 17(6), pp.143-148, 2007년 12월.

[6] 김정덕, 김건우, 이용덕, "융합보안의 개념 정립과 접근방법," 정보보호학회지, 19(6), pp.68-74, 2009년 12월.

[7] Erete I, "Browser-Based Intrusion Prevention System," Recent advances in intrusion detection: 12th international symposium, Lecture notes in computer science, vol.5758, pp.371-373, 2009.

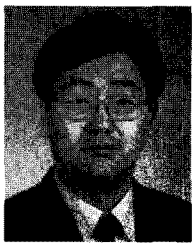
[8] 박순태, 이완석, 노봉남, "주요정보통신기반시설 보호를 위한 취약점 분석.평가 관리 방안," 정보보호학회지, 19(6), pp.32-40, 2009년 12월.

[9] Qiu X and Paterson R, "An Innovative Network Security Vulnerability Modeling Method and Tool," IEEE communications magazine, vol.48, no.1, pp.104-108, Jan. 2010.

[10] Yuan H, "A Network Security Risk Assessment Method Based on Immunity Algorithm," Trans-Tech Publications, pp.948-953, May. 2010.

〈著者紹介〉

서 우 석 (Woo-seok Seo) 종신회원
2006년: 숭실대학교 정보과학대학원 정보통신융합학과 석사
2009년 9월~현재: 숭실대학교 컴퓨터학과 박사과정
〈관심분야〉 정보보호, 네트워크 보안, 방화벽, Router & Network Design



전 문 석 (Moon-seog Jun) 종신회원
1981년 2월: 숭실대학교 전자계산학과 졸업
1986년 2월: University of Maryland Computer Science 석사
1989년 2월: University of Maryland Computer Science 박사
1986년 9월~1989년 12월: University of Mary 강사
1989년 3월~7월: Morgan State University 조교수
1989년 9월~1991년 2월: New Mexico State University Physical Science Lab. 책임연구원
1991년 3월~현재: 숭실대학교 정교수
〈관심분야〉 정보보호, 네트워크 보안, 전자여권, 암호학