https://doi.org/10.7840/kics.2024.49.9.1337

Network Address Translation 환경에서 내부망 웹 서비스 공격 트래픽 부하 개선 가능한 IPS와 NAT세션 매핑정보활용 방화벽 차단룰 자동 설정 시스템 연구

손 병 홍◆, 유 명 식°

A Study on the Automatic Configuration System for Firewall Blocking Rules Using IPS and NAT Session Mapping Information to Improve Network Web Service Attack Traffic Load in a Network Address Translation Environment

Byeong-hong Son◆, Myungsik Yoo°

요 약

인터넷 웹 서비스 환경에서 Layer 7 공격의 경우 웹 서버 앞에 설치되는 IPS나 WAF 장비에서 공격을 차단한다. 라우터에서 IPS나 WAF 내부 구간에는 공격 트래픽이 여전히 유입되고 네트워크 부하와 보안 위협이 발생한다. IPS나 WAF를 모니터링하여 관리자가 인입단 방화벽에 차단룰 설정이 가능하나, 실제 환경에서는 공격이 동적으로 변화하고, Network Address Translation 환경에서는 공격 IP/Port가 변경되어 수동으로 차단 설정하는 것이 불가능하다. 본 연구에서는 NAT환경에서 IPS Layer 7 공격 차단 정보와 NAT 세션 정보를 실시간으로 수집 분석하여 방화벽 자동차단 설정 시스템을 개발하여, 내부망 부하현상 및 보안위협이 개선됨을 실험을 통하여 확인하였다.

Key Words : web Service Attack, NAT Session Table, Firewall, Blocking

ABSTRACT

In an Internet web services environment, Layer 7 attacks are blocked by an IPS or WAF device that is installed in front of the web server. Attack traffic still flows from the router to the IPS or WAF internals, causing network load and security threats. By monitoring the IPS or WAF, administrators can set blocking rules on the ingress firewall, but in real-world environments, attacks change dynamically, and attack IP/Ports change in a network address translation environment, making it impossible to manually set blocking rules. In this study, we developed a firewall carrier setting system by collecting and analyzing IPS Layer 7 attack blocking information and NAT session information in real time in a NAT environment, and confirmed through experiments that the internal network load phenomenon and security threats are improved.

◆ First Author : Soongsil University Department of AI IT Convergence, swimsun@naver.com, 정회원
° Corresponding Author : Soongsil University School of Electronic Engineering, myoo@ssu.ac.kr, 종신회원
논문번호 : 202405-081-0-SE, Received March 27, 2024; Revised June 10, 2024; Accepted June 17, 2024

Ⅰ. 서 론

인터넷 환경에서 외부의 공격을 차단하기 위해 개별적인 목적에 맞는 보안장비들이 사용되고 있다. 그림 1의 Anti DDoS(Distributed Denial of Service), IP(Internet Protocol)/Port 차단을 위한 방화벽(Firewall), 침입 탐지 방지 목적의 IPS(Intursion Prevention System), 웹 어플리케이션 공격 차단용 WAF(Web Application Firewall)로 구분된다. 대부분의 대형 인터넷 서비스 인프라 환경에서 보안장비의 구성은 DDoS, 방화벽, IPS ,WAF로 구성되며 장비별 방어 특성으로 공격을 차단한다. IPS/WAF와 같은 보안장비는 OSI(Open Systems Interconnection Reference Model) Layer 7(Application) 보안장비로 활용되며, 공격이 발생하는 경우 IPS나 WAF에서 Layer 7 필터링이 진행되고, 보안관리자는 필터링되는 정보를 모니터링 확인하여 Layer 4(Transport) 및 Layer 3(Network)에서 원천 차단하기 위해 방화벽에 차단 설정하여 내부망인 방화벽과 IPS/WAF 사이에 부하와 보안 위협 개선 활동을 수행한다.

근래의 보안 공격들은 복잡하고 동적으로 진행된다. 특히 NAT(Network Address Translation) 환경에서 공격 IP와 Port 변호가 실시간으로 변경되는 경우 보안관리자가 변경 전 정보를 찾아 방화벽에 차단룰을 설정하는 것은 현실적으로 불가능하다. 또한 보안장비 협업하여 정보를 취합하여 대응에도 시간이 소요된다.

보안장비 차단 및 이벤트 정보를 통합적으로 관제[3]하기 위해 개발된 SIEM(Secuirty Information and event Manager) 또는 ESM(Enterprise Security Management)을 사용하기도 하지만 이 역시 관리자가 정보를 확인하여 방화벽에 룰을 설정하는 수동적인 방법을 수행하여 IPS/WAF까지의 내부 네트워크에 공격 트래픽에 의한 병목 현상과 보안위협을 실시간으로 적용하기 어려운 실정이다.

본 논문에서는 Layer 7 공격 트래픽이 NAT에서 IP와 Port 정보가 변경되고 내부망 IPS에서 차단되는 환경으로 차단 정보와 NAT 세션 정보를 실시간으로 수집하여 공격자 정보를 복원하고, Layer 3 방화벽에 실시간 자동 차단룰을 설정하여 내부망 네트워크에 발생하는 부하현상 및 보안 위협을 개선하는 시스템을 제시하고 개발하여 검증함에 목적이 있다.

Anti DDoS	Firewall	IPS	WAF
. Distributed Denial of Service Attack . Monitor Traffic to Measure available bandwidth/Session	. Inspects and filter incoming and outgoing network traffic predetermined rules . IP/Port/Protocol	. Detects and Blocks malicious code/intrusion attempts . Signature / Behavior Based	. SQL-Injection, Cross-Site Scripting(XSS), Cross-Site . Pattern/Signature /Behavior

그림 1. 보안장비 차단특성
Fig 1. Security Device Blocking Attributes

Ⅱ. 기존 연구 및 제안 시스템

2.1 기존 연구 및 제안 시스템 적용기법

기존의 연구는 보안장비의 차단 및 이벤트 정보를 통합관제하여 보안 탐지 및 보안대응 업무 개선을 위한 내용이 주류를 이루고 있으며 차단 로그를 수집하여 불필요한 중복제거 위험도 자동 분류 비정상 통신을 연구하거나[1], 보안 강화를 위해 필요한 상시적인 업무의 반복적 대응 자동화에 중점을 두고 있으나[2], 본 연구는 Layer 7 보안장비에서 차단된 정보와 Layer 4의 NAT IP와 Port의 원본 정보를 분석하여 Layer 3 방화벽에 자동으로 차단룰을 설정하는 시스템으로 기존 연구와 차별성이 있다.

제안 시스템은 Layer 4 NAT 장비에서 변환되기 전/후의 TCP 서비스의 IP와 Port 정보를 수집하고, IPS 장비의 차단 로그를 수집 분석하여 IP와 Port 정보를 생성한다. NAT 장비에서 수집된 변환된 IP와 Port 정보를 Layer 7 IPS 차단 IP와 Port 정보를 대조하여 NAT에서 변경되기 전의 공격 IP와 Port 정보를 복원하여 네트워크 Layer 3 방화벽에 실시간으로 차단 정책을 적용하는 Layer 연계 시스템으로 본 논문에서 Orchestration 시스템으로 가칭한다.

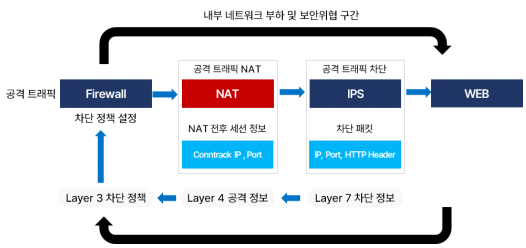

그림 2. 제안 시스템
Fig 2. Proposal System

2.2 제안 시스템 실험 구성

실험 시스템은 구성의 단순화를 위해 WAF를 제외하고 공격성 User-Agnet를 분석하여 HTTP 요청을 차단하는 장비를 ㉠IPS로 한정하여 IPS에서 차단되는 정보를 수집하는 구성 하고 내부 네트워크 구간 병목 및 보안위협 개선을 위한 보안장비 연계 자동적용 Ⓑ Orchestration 프로그램을 개발하였다.

그림 3 및 표 3의 구성과 같이 본 실험을 위한 VM 구성용 Ⓐ호스트 서버에 정상 사용자 및 공격 트래픽 발생을 위해 JMeter[4]를 이용한여 ㉠일반 사용자는 User-Agent 정보를 Mozilla/5.0으로 VM을 구성하고, ㉡공격 사용자는 User-Agent를 Attack로 설정하여 부하 발생을 위한 VM으로 구성된다. 정상 사용자 트래픽은 JMeter 40Thread Ramp-Up 1Sec 주기로 동작하도록 설정 하고, 공격 트래픽은 JMeter 80Thread Ramp-Up 1Sec 주기로 정상 대비 공격 사용자 Thread를 두배로 설정한다. IPS 차단 및 NAT 세션 정보를 수집하여 Firewall에 차단 정책을 적용하는 보안장비 구성 및 ⒷOrchestration 프로그램이 포함된 호스트 서버는 4개의 물리 ㉣Bridge Adapter로 구성되고 ㉤Firewall VM은 두 개의 가상 NIC를 Bridge 구성하여 nftables 설정으로 방화벽 차단 기능을 수행한다. ㉥NAT Gateway VM은 두 개의 가상 NIC에 192.168.20.0/24 와 192.168.40.0/24 네트워크를 구성하고 iptables postrouting maquerade 설정으로 192.168.20.0/24 네트워크에서 발생하는 HTTP Web 요청 트래픽을 192.168.40.1 IP로 변환한다. NAT 세션 변환 전/후 정보는 conntrack[7]을 이용하여 실시간 업데이트 정보를 수집하는 구성이다.

㉦IPS VM은 두 개의 가상 NIC에 snort inline으로 구성되며 User-Agent가 Attack로 발생한 트래픽을 차단하는 설정은 “drop tcp any any → any any (msg: “MALWARE User Agent”; flow:to_server,established; content:“Attack”; http_header; classtype:trojan-activity; sid:1000002;)”이며, 두 개의 가상 NIC에 패킷을 수집하여 차단된 트래픽 IP/Port 정보는 ⒷOrchestration 프로그램이 snort log에서 수집한다. ㉧Web Server VM은 192,168.40.50:3000으로 구성된 서비스이다.

ⒷOrchestration 프로그램은 ㉦IPS VM에서 차단된 공격 트래픽 사용자 정보를 수집하고, NAT Gateway VM에서 수집된 NAT 세션 정보와 매핑 하여 원천 사용자 공격 IP/Port 정보를 분석하여. 방화벽에 자동으로 차단 설정을 하여 Firewall과 IPS 사이에서 구간 부하 및 공격 트래픽을 차단하는 기능으로 구성되어 있다.

그림 4 및 표 1에서 Orchestration 소프트웨어 프로그램은 NAT Session Table을 생성 초기화하고, conntrack 로그를 수집 분석하는 Thread_01과 Snort IPS 차단 로그를 수집 분석하는 Thread_02를 실행시키는 Main Thread로 구성되어 있다.

Thread_01은 NAT Session Table 추적에 사용되는 conntrack 로그정보를 수집하고 “[NEW]” 패턴 정보가 확인되면 신규 세션으로 판단하여 NAT Session Table에서 기존 정보가 존재하는지 확인하여 없는 경우 신규 테이블로 Insert한다.

“[NEW]” 패턴이 아닌 경우 NAT Session Table에서 기존 정보가 존재하는지 확인하여 있는 경우 Update한다. Thread_02에서 Layer 7 IPS 차단 정보 수집을 위해 Snort IPS 로그에서 수집된 차단정보가 NAT Session Table에서 확인되면 Layer 3 방화벽에 nftables로 차단룰을 설정하고 세션 정보를 Delete한다.

본 논문에서는 NAT 환경에서 L7 공격에 대한 IPS 장비의 공격 차단에도 내부 네트워크 부하가 존재함을 실험으로 증명하고 IPS차단 대비 IPS/NAT/Firewall을

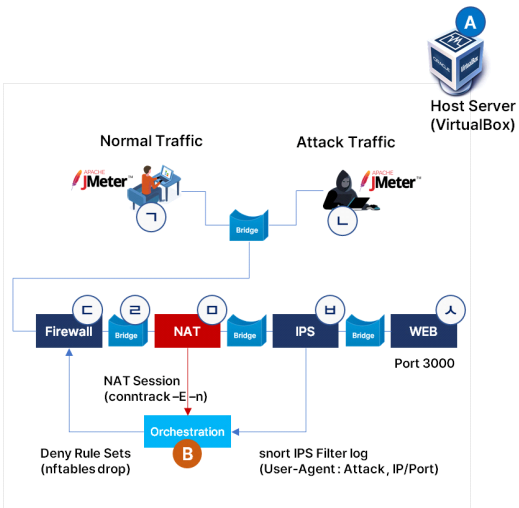

그림 3. 실험 시스템 구성도
Fig 3. Experimental System Configuration Diagram

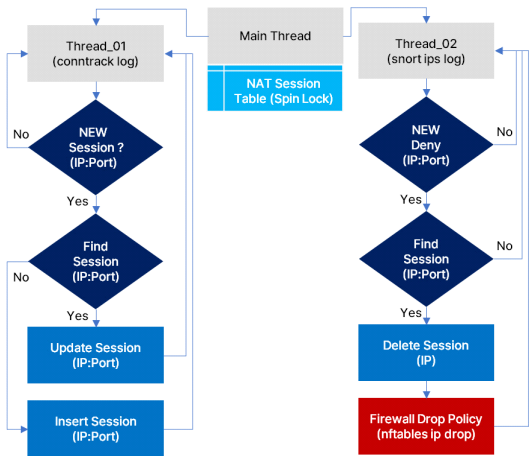

그림 4. Orchestration 프로그램 블록 다이어그램
Fig 4. Orchestration Program Block Diagram.

표 1. Orchestration 프로그램 의사코드
Table 1. Orchestartion Program Sudo Code

Thread	Sudo Code
Main Thread	spinlock.nat_table.init(); Thread_01.run(); Thread_02.run();

Thre ad_01
. conntrack log
. nat table
	while(conntrack log){
	if(packet arrived true){
	if(conntrack tcp status "[NEW]' true){ parsing.ip_port();
	if(nat_table.find() true)
	spinlock.nat_table.update();
	else
	spinlock.nat_table.insert();
	} else {
	if(nat_table.find() true)
	spinlock.nat_table.update();
	}
	}
	}

Thread_02
. snort ips log
. nat table
. nftables ip drop
	while(snort ips log){
	if(deny packet arrived true){
	if(ips tcp status "{TCP}' true)
	{ parsing.ip_port();
	if(nat_table.find() true){
	spinlock.nftables.ip_drop();
	spinlocl.nat_table.delete();
	}
	}
	}
	}

이용한 제안 시스템의 부하 감소 및 정상 부하의 개선 비율을 직관적으로 확인하기 위해 JMeter를 이용하여 정상 부하는 40Thread, 공격 부하는 80Thread로 정상 대비 공격을 2배 비율로 실험하는 설정을 하였다.

표 2. JMeter 부하 발생 및 공격 트래픽
Table 2. JMter Load Generation and Attack Traffic

Category	JMeter Thread (Load Generation)	User-Agent
Normal User	40 Thread / Ramp-Up 1Sec	Mozilla/5.0
Attack User	80 Thread / Ramp-Up 1Sec	Attack

표 3. 실험 시스템의 설정 및 기능
Table 3. Experimental System Configuration&Function

Category		Configuration/Function
Ⓐ	Host Server (Orchestration Program)	[Configuration] Physical NIC Bridge Adapter 4EA
㉠	Normal Traffic (JMeter)	[Configuration] Virtual NIC 1EA IP : 192.168.20.40 Load IP : 192.68.20.100~109 JMeter HTTP User-Agent ; Mozilla/5.0
㉡	Attack Traffic (JMeter)	[Configuration] Virtual NIC 1EA IP : 192.168.20.20 Load IP : 192.68.20.110~119 JMeter HTTP User-Agent ; Attack
㉢	Firewall	[Configuration] inbound nic ; enp08s outbound nic ; enp09s bridge nic : FW · enp08s:enp09s packet filter ; nftables traffic monitoring : pcount · libpcap&PF_RING[6]
㉣	Bridge Adapter	VirtualBox Bridge Adapter
㉤	NAT Gateway	[Configuration] inbound nic : enp0s8 · Network 192.168.20.0/24 · Gateway 192.168.20.1 outbound nic : enp0s9 · Network 192.168.40.0/24 · Gateway 192.168.40.1 NAT : · iptables postrouting masquerade : · 192.168.20.0/24→192.168.40.1 NAT Session monitoring : · conntrack
㉥	IPS	[Configuration] inbound nic : enp0s8, oubound nic : enp0s9 packet filter : snort[5] inline · enp08s:enp09s traffic monitoring : pcount · libpcap&PF_RING
㉦	WEB Server	[Configuration] HTTP Web Service Login Page 192.168.40.50:3000
Ⓑ	Orchestration Software Program	[Data Collector] · conntrack TCP Session Log · IPS Deny TCP Session

Ⅲ. 실 험

표 4 ❶단계에서 정상 HTTP와 공격 HTTP 요청이 동시에 발생하고 있는 단계이며, 공격 HTTP 부하가 발생하고 HTTP Layer 7 User-Agent 정보가 Attack인

표 4. 실험 단계별 정상 및 공격 트래픽 결과
Table 4. Normal and Attack traffic results by Experimental phase

Phase	DROP Attack Traffic (18:36:30~19:06:53)		Traffic (Firewall - NAT - IPS)			
			Normal Traffic (avg/sec)		Attack Traffic (avg/sec)	
	IPS	Firewall	Count	KByte	Count	KByte
❶	non	non	4,811	2,618	9,708	5,097
❷	DROP	non	7,275	3,927	6,311	518
❸	DROP	DROP	14,111	8,101	0	0

공격 요청을 IPS에서 차단 되기 전 단계이다. 그림 5 / 그림 6 / 그림 7 / 그림 8의 ❶단계에서 정상 HTTP 요청과 공격 HTTP 요청에 WEB Server가 응답하고 있으며 트래픽이 일정하고 유지되고 있다.

그림 5 / 그림 6 / 그림 7 / 그림 8의 ❷단계에서 HTTP Header의 Layer 7 User-Agent Attack 정보를 차단하는 정책이 적용되어 공격 HTTP 요청이 필터링 되는 단계로 ❶→❷에서 정상 HTTP Packet Count가 약 50% 향상되었으며 IPS가 정상적으로 동작함을 확인 할 수 있지만 공격 HTTP Packet Count는 약 35%만 감소함을 확인 할 수 있다.

그림 5 / 그림 6 / 그림 7 / 그림 8의 ❷단계에서 정상 HTTP Packet Count는 약 6,000에서 14,000까지 일정하지 않으며 이러한 결과는 User-Agent가 Attack으로 확인된 Layer 7 Packet만 차단되어 외부 유입 공격은 여전히 내부 구간에 ❶단계 대비 약 65% 비율로 부하를 발생시킨다.

❸단계에서 IPS에서 차단된 정보를 활용하여 방화벽 정책에 적용하기 위해서는 NAT Gateway에 의해 공격 HTTP 요청의 IP정보가 192.168.40.1 단일 IP로 변경되어 방화벽 차단 정책에 적용하지 못하는 문제를 표 5와 같이 NAT Gateway의 수집된 Connection Tracking

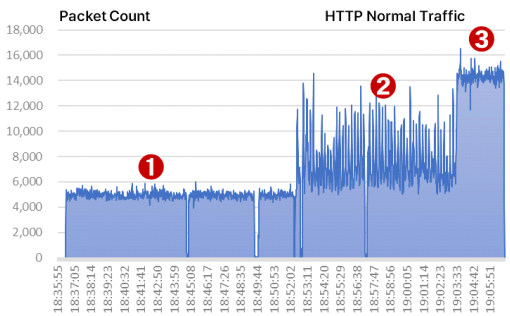

그림 5. 실험 단계별 정상 패킷 수 추이
Fig 5. Normal packet counts by experimental phase.

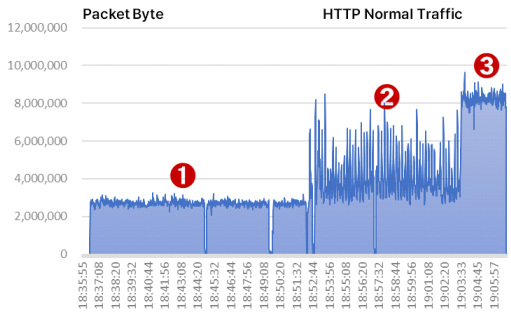

그림 6. 실험 단계별 정상 패킷 byte 추이
Fig 6. Normal packet bytes by experimental phase.

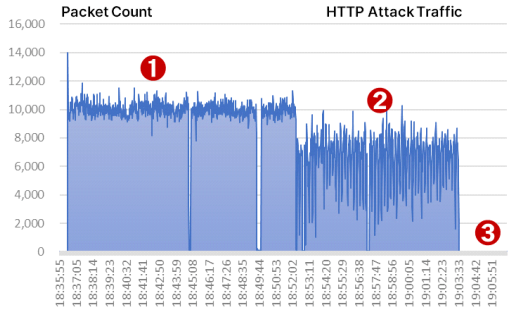

그림 7. 실험 단계별 공격 패킷 수 추이
Fig 7. Attack packet counts by experimental phase.

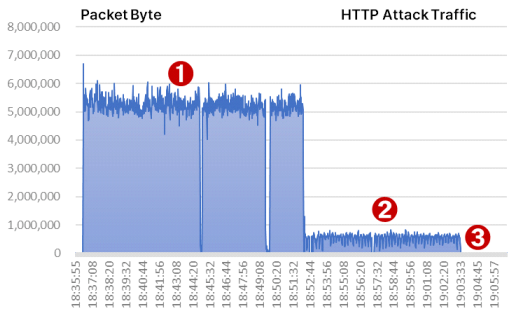

그림 8. 실험 단계별 공격 패킷 byte 추이
Fig 8. Attack packet bytes by experimental phase.

표 5. NAT 세션 테이블(데이터 일부)
Table 5. NAT Session Table(Part of Data)

NAT Session Table(conntrack)		DROP Target IP
Before NAT IP:Port	After NAT IP:Port (IPS Filter)	
192.168.20.115:5097	192.168.40.1:50971	192.168.20.115
192.168.20.116:60898	192.168.40.1:60898	192.168.20.116
192.168.20.113:56118	192.168.40.1:56118	192.168.20.113
192.168.20.117:62149	192.168.40.1:62149	192.168.20.117
192.168.20.118:50421	192.168.40.1:44645	192.168.20.118

Session 정보로 공격자 원천 IP/Port 정보를 찾아 방화벽 차단 정책이 적용되었으며 ❸단계는 ❶단계 대비 공격 HTTP Packet Count가 100% 차단되고 정상 HTTP Packet Count가 초당 평균적으로 4,811→14,111로 9,300개 증가하여 그림 9 및 그림 10에서 IPS & NAT & Firewall 연계 차단으로 부하가 개선됨을 확인하였다.

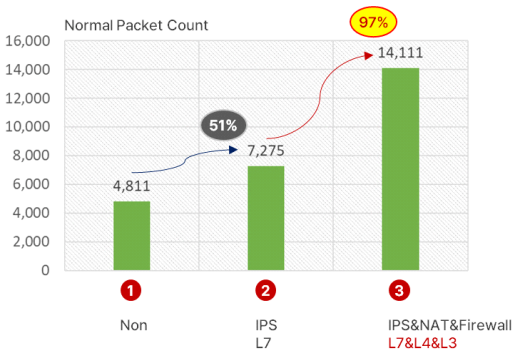

그림 9. 실험 단계별 정상 패킷 평균 추이
Fig 9. Normal average packets by experimental phase

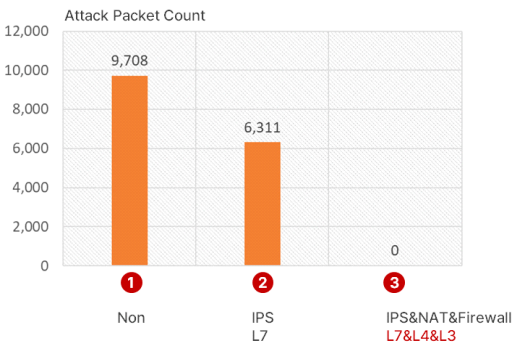

그림 10. 실험 단계별 공격 패킷 평균 수 추이
Fig 10. Attack average packets by experimental phase.

Ⅳ. 결 론

본 논문에서는 Layer 7 공격 트래픽이 내부 구간의 IPS에서 차단 가능하지만 원천 차단되지 못하고, 내부 네트워크 구간에서 발생하는 부하 현상과 보안 위협을 개선하고자 공격 IP/Port가 NAT에 의해 변경되어 원천 공격 정보를 운영자가 차단하기 어려운 환경에서 운영자의 개입 없이 Layer 7 IPS, Layer 4 NAT Session Table, Layer 3 방화벽을 연계하여 공격 차단을 설정하는 시스템을 개발하고 실험하여 내부 네트워크 부하가와 보안 위협이 개선됨을 확인하였다.

본 논문에서는 VM을 이용한 실험 환경으로 구성하였으나 고부하 테스트가 가능한 별도로 분리된 장비의 물리적 구성 및 네트워크 장비의 ACL(Access Control List) 정보, Layer 7 웹 크롤링 정보 등의 다양한 데이터를 수집 연동하여 네트워크 세그먼트 단위 및 구간별 차단이 가능한 통합 차단 시스템으로 발전시키고자 하며, 제안 시스템에서 적용된 NAT Session Table 정보 취득 방법은 iptables conntrack를 이용하여 메모리와 CPU가 사용되어 오버헤드가 발생한다. 향후 실험에서는 물리적 상용 네트워크 장비 및 SNMP(Simple Network Management Protocol)를 이용한 환경을 구성하여 NAT Session Table 정보 취득시 제안 시스템 구성에서 발생 가능한 오버헤드를 비교하고 최소화 가능한 시스템으로 적용하고자 한다.

References

[1] S. H. Choi and J. Choi, "A control method of abnormal communication using SIEM in a network segregation environment," *Sogang University*, 2023.

[2] J. S. Choe, "A methodology for internal security response process automation base on SOAR in SIEM," Chung-Ang University, 2021.

[3] Hyeong Joo, "A study on the efficient security control methods using SIEM and threat intelligence system," Sungkyunkwan University, 2019.

[4] Apache Software Foundation, *JMeter User's Manual*, 2024. (https://jmeter.apache.org/usermanual/index.html)

[5] The Snort Team, *Snort3 User Manual*, 2024. (https://github.com/snort3/snort3/releases/download/3.1.83.0/snort_user.html)

[6] PF_RING, *PF_RING Documentation*. (https://www.ntop.org/guides/pf_ring/)

[7] Jay Schulist, *CONNTRACK Manual*. (https://www.netfilter.org/projects/conntrack-tools/conntrack-manpage.html)

손 병 홍 (Byeong-hong Son)

2001년 2월 : 홍익대학교 전자전기공학과 학사

2021년 8월 : 숭실대학교 IT융합학과 석사

2022년 9월~현재 : 숭실대학교 인공지능IT융합학과 지능형메카트로닉스융합전공 박사과정

<관심분야> TCP/IP Communication, AI Object Detection, Robotics

[ORCID:0000-0002-5366-9467]

유 명 식 (Myungsik Yoo)

1989년 2월 : 고려대학교 전자공학 학사

1991년 2월 : 고려대학교 전자공학 석사

2000년 6월 : SUNY at Buffalo Dept. of EE 박사

2000년 9월~현재 : 숭실대학교 전자정보공학부 교수

<관심분야> Visible Light Communication, Cloud Systems, Sensor Network. Edge Computing