# Network Address Translation 환경에서 공격 트래픽에 의한 내부 구간 병목현상 개선 가능한 웹방화벽 및 NAT세션 매핑정보활용 방화벽 연계제어 시스템 연구

손병홍, 유명식*

숭실대학교

bhson@sysone.co.kr, *myoo@ssu.ac.kr

# A Study on Firewall Integration Control Systems for Improving Internal Segment Bottleneck Caused by Attack Traffic in Network Address Translation Environments, Utilizing Web Firewalls and NAT Session Mapping Information.

Byeonghong Son, Myungsik Yoo*

Soongsil University.

요 약

인터넷 환경에서 외부 공격의 차단을 담당하는 보안장비들은 공격의 특성에 따라 전문적으로 차단하는 별도의 장비들로 구성되어 있다. 공격의 특성에 따라 차단하는 장비의 위치가 달라 일반적인 보안장비 구성상 제일 뒷단에 설치하는 WAF에서만 탐지 차단 가능한 공격이 들어오는 경우 라우터에서 WAF 구간 까지의 내부 구간에는 공격 트래픽으로 인해 네트워크 병목 현상 및 보안 위협이 존재하게 된다. WAF 를 모니터링하여 관리자가 인터넷의 인입단에 있는 Firewall에 차단룰을 설정 할 수 있으나 실제 환경에서는 동적으로 변화하는 공격에 대해 관리자 사람이 눈으로 보고 직접 설정하기는 불가능하다. 특히 Network Address Translation 환경에서는 차단 되는 IP 의 NAT 전 원래 공격 IP 를 찾아 룰을 설정하는것이 불가능하다. 본 연구에서는 외부 공격에 의해 내부 보안장비에서 차단되는 정보와 NAT 세션 정보를 실시간으로 수집 분석하여 인터넷 인입단인 Firewall 에 직접 자동으로 차단 룰을 설정하여 네트워크 구간 병목 및 보안위협 개선 가능한 시스템을 개발하였다. 실험을 통하여 Firewall 자동 룰 설정으로 병목 현상 및 보안위협이 개선됨을 확인 하였다.

## Ⅰ. 서 론

인터넷 환경에서 외부의 공격을 차단하기 위해 개별적인 목적에 맞는 보안장비들이 사용되고 있다. 대량 분산 트랙픽 발생으로 서비스를 중단하는 DDoS(Distributed Denial of Service), IP(Internet Protoco)/Port 차단을 위한 Firewall, 침입 탐지 방지 목적의 IPS(Intursion Prevention System), 웹 어플리케이션 악성 공격 차단용 WAF(Web Application Firewall) 로 구분된다. 대부분의 대형 인터넷 서비스 인프라 환경에서 보안 장비의 구성은 DDoS -> Firewall -> IPS -> WAF 로 구성되며 개별 장비에서 공격을 차단한다. IPS나 WAF와 같은 보안 장비는 대부분 내부 서비스의 뒤쪽에 위치하는 보안장비로 차단 가능한 공격이 발생하는 경우 일반적으로 보안관리자는 보안장비의 화면 또는 로그등을 모니터링하여 공격자 정보를 확인하고 서비스 네트워크의 앞쪽에 위치한 보안장비인 Firewall에서 공격자를 차단하는 룰을 설정하여 Firewall과 WAF 사이의 내부 네트워크에 발생하는 공격성 트래픽에 의한 병목현상과 보안 위협을 개선하려는 시도를 한다.

근래의 보안 공격들은 매우 복잡하고 다이나믹하게 발생을 하며, 특히 NAT(Network Address Translation) 환경에서 공격 IP와 Port 변호가 변경되어 보안 관리자들이 Firewall에 수동으로 차단 룰을 설정하는 것이 어려운 상황이며 각 보안장비 마다 유지보수 인력들과 협업하여 관련 정보를 취합하여 적용이 필요하다. 특히 NAT 환경에서는 공격 IP 및 Port 번호가 변경되어 관리자가 원천 공격 정보를 파악하여 차단 룰을 설정하기 어려운 상황이다.

그림 1. 보안 장비별 차단 특성

| DDoS | Firewall | IPS | WAF |
|---|---|---|---|
| 분산서비스공격<br>인터넷 트래픽의 폭주 공격<br>서비스거부 세션 잠식<br><br>트래픽, 세션(Syn), ResReq 특성 | 허용하지 않은 IP, Port의 취약점 공격<br><br>IP/Port 차단정책 | 악성 바이러스 / 코드를 이용하여 해킹 또는 서비스 장애 유발<br><br>패턴/Signature | 웹 애플리케이션에 특화된 IPS<br>SQL-Injection, XSS(악성코드첨부)<br><br>패턴/행위/Signature |

차단 및 이벤트 정보를 통합적으로 관제하기 위한 용도로 개발된 SIEM(Secuirty Information and event Manager) 또는 ESM(Enterprise Security Management)[3]을 사용하기도 하지만 이 역시 관리자가 정보를 확인하여 Firewall 등에 룰을 설정하는 수동적인 방법을 수행하여 내부 네트워크에 발생하는 공격 트래픽에 의한 병목 현상과 보안위협을 실시간으로 적용하기 어려운 실정이다.

본 논문에서는 공격 트랙픽이 차단되는 보안장비의 위치가 서비스 인프라의 뒤 쪽에 위치하는 하고 NAT 환경으로 공격자의 IP 와 Port 정보가 변경되는 환경에서 차단 정보와 NAT 세션 정보를 실시간으로 수집하여 공격자 정보를 복원하여 보안장비의 앞 쪽에 위치한 Firewall 에 실시간 자동으로 룰 설정하여 내부 서비스 네트워크에 발생하는 구간 병목 현상 및 보안 위협을 개선하는 시스템에 대한 방법을 제시 및 개발과 검증에 목적이 있다.

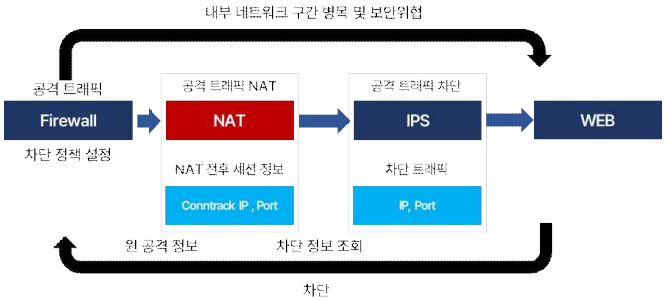
## Ⅱ. 기존 연구 및 제안 시스템

### 2.1 기존 연구 및 보안&NAT장비 연계 적용기법

기존의 연구는 보안 장비의 차단 및 이벤트 정보등을 통합관제하여 보안 탐지의 개선과 보안대응 업무 개선을 위한 내용이 주류를 이루고 있으며 차단 로그를 수집하여 불필요한 중보제거 및 위험도 분류를 자동으로 분류시켜 비정상 통신점검 방안을 연구하거나[1], 보안을 강화하기 위해 필요한 상시적인 업무의 반복적 대응을 자동화 하는데 중점을 두고 있으나 [2] 본 연구는 보안장에서 차단된 정보와 NAT된 IP와 Port의 원본 정보를 확인하여 서비스 네트워크의 인입 지점에 위치한 Firewall 장비에 차단 룰을 실시간 및 자동으로 연계 설정하는 것으로 기존 연구와 차별성이 있다.

제안 시스템은 NAT 장비에서 변환되기 전/후의 TCP 서비스의 IP와 Port 정보를 수집하고, 네트워크의 뒤 쪽에 위치한 보안장비의 차단 정보를 수집하기위해 차단 전/후 네트워크 패킷을 수집 분석하여 차단 IP와 Port 정보를 생성한다. NAT 장비에서 수집된 변환후 IP와 Port 정보와 보안장비에서 차단된 IP와 Port 정보를 대조하여 원 공격 IP와 Port 정보를 찾아 내어 네트워크 인입단의 Firewall 장비에 실시간으로 차단 정책을 적용하는 시스템으로 본 논문에서 Orchestration 시스템으로 가칭한다.

그림 2. Orchestration 시스템(제안 시스템)




### 2.2 제안 시스템 실험 구성

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

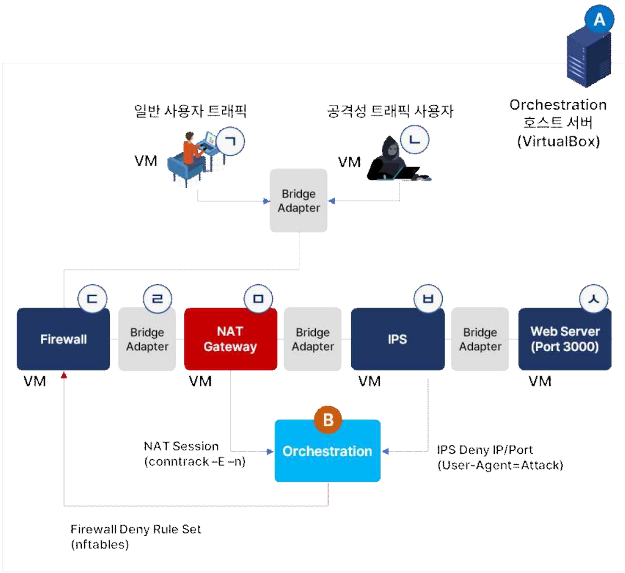
그림 3 및 표 2의 구성과 같이 본 실험을 위한 VM 구성용 Ⓐ호스트 서버에 정상 사용자 및 악성 트래픽 발생을 위해 JMeter[4]를 이용한여 ㄱ 일반 사용자는 User-Agent 정보를 Mozilla/5.0으로 VM을 구성하고, ㄴ 악성 사용자는 User-Agent를 Attack로 설정하여 부하 발생을 위한 VM으로 구성된다.

정상 사용자 트래픽은 JMeter 40Thread Ramp-Up 1Seconds 주기로 동작하도록 설정을 하고, 악성 트팩픽은 JMeter 80Thread Ramp-Up 1Seconds 주기로 동작하도록 설정한다.

IPS 차단 및 NAT 세션 정보를 수집하여 Firewall에 차단 정책을 적용하는 보안장비 구성 및 ⒷOrchestration 프로그램이 포함된 호스트 서버는 4개의 물리 ㄹBridge Adapter로 구성되고 ㄷFirewall VM은 두 개의 가상 NIC를 Bridge 구성하여 nftables 설정으로 방화벽 차단 기능을 수행한다.

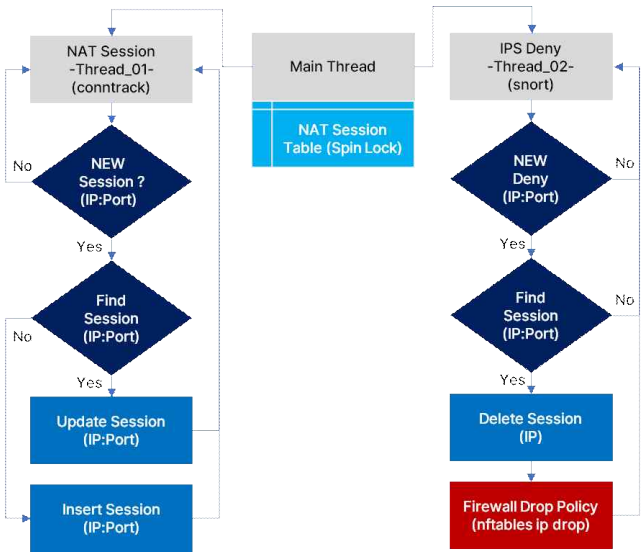
ㅁNAT Gateway VM은 두 개의 가상 NIC에 192.168.20.0/24 네트워크와 192.168.40.0/24 네트워크를 구성하고 iptables postrouting maquerade 설정으로 192.168.20.0/24 네트워크에서 발생하는 HTTP Web 요청 트래픽을 192.168.40.1 IP로 변환한다. NAT 세션 변환 전/후 정보는 conntrack을 이용하여 실시간 업데이트 정보를 수집하는 구성이다..

그림 3. Orchestration 시스템 실험 구성도




ㅂIPS VM은 두 개의 가상 NIC에 snort inline으로 구성되며 HTTP Web 트래픽 중에 User-Agent가 Attack로 발생한 트래픽을 차단하는 설정이며, 두 개의 가상 NIC에 패킷을 수집하여 차단된 트래픽 IP/Port 정보는 ⒷOrchestration 프로그램이 snort log를에서 수집한다.

그림 4. Orchestration Program




ㅅWeb Server VM은 192,168.40.50:3000으로 Web Service를 제공하는 구성이다.

ⒷOrchestration 프로그램은 ㅂIPS VM에서 차단된 공격 트래픽 사용자 정보를 수집하고, NAT Gateway VM에서 수집된 NAT 세션 정보와 매핑 하여 원천 사용자 공격 IP/Port 정보를 분석한여. Firewall에 자동으

로 차단 설정을 하여 Firewall과 IPS 사이에서 구간 병목현상 및 보안위협 트래픽을 차단하는 기능으로 구성되어 있다.

표 1. 보안장비 Orchestration 시스템 구성 및 설정/기능

| 종류 | | 구성 및 설정 | 비고 |
|---|---|---|---|
| A | 실험 구성용 호스트 서버 및 Orchestration 프로그램 탑재 | [구성]<br>Physical NIC Bridge Adapter 4EA | |
| ㄱ | 정상 사용자 트래픽 발생 서버 | [구성]<br>Virtual NIC 1EA<br>IP : 192.168.20.40<br>부하발생 IP : 192.68.20.100 ~ 109<br>[JMeter 설정]<br>HTTP 호출 User-Agent : Mozilla/5.0 | VM<br>JMeter[4] |
| ㄴ | 악성 트래픽 발생 서버 | [구성]<br>Virtual NIC 1EA<br>IP : 192.168.20.20<br>부하발생 IP : 192.68.20.110 ~ 119<br>[JMeter 설정]<br>HTTP 호출 User-Agent : Attack | VM<br>JMeter |
| ㄷ | Firewall | [설정]<br>inbound nic : enp08s<br>outbound nic : enp09s<br>bridge nic : FW(enp08s:enp09s)<br>packet filter : nftables<br>traffic monitoring : pcount<br>(libpcap&PF_RING) | nftables<br>libpcap/PF<br>_RING[6] |
| ㄹ | Bridge Adapter | VirtualBox Bridge Adapter | VirualBox<br>Bridge<br>Adapter |
| ㅁ | NAT Gateway | [설정]<br>inbound nic : enp0s8<br>. Network 192.168.20.0/24<br>. Gateway 192.168.20.1<br>outbound nic : enp0s9<br>. Network 192.168.40.0/24<br>. Gateway 192.168.40.1<br>NAT<br>.iptables postrouting masquerade<br>.192.168.20.0/24 -> 192.168.40.1 | ip_routing<br>iptables<br>(MASQUE<br>RADE)<br>conntrack |
| ㅂ | IPS | [설정]<br>inbound nic : enp0s8,<br>oubound nic : enp0s9<br>packet filter : snort inline<br>(enp08s:enp09s)<br>traffic monitoring : pcount<br>(libpcap&PF_RING) | inline<br>snort[5]<br>(afpacket) |
| ㅅ | WEB Server | [설정]<br>HTTP Web Service 192.168.40.50:3000 | Login<br>Page |
| B | Orchestration Program | [데이터 수집]<br>. IPS Deny TCP Session<br>. NAT Session | |

## Ⅲ. 실험

실험 결과 표 2의 ❶ 단계에서 정상 HTTP와 악성 HTTP 요청이 동시에 발생하고 있는 단계이며 악성 HTTP 요청대비 정상 HTTP 요청에 병목이 발생하고 있으며 HTTP User-Agent가 Attack인 악성 HTTP 요청을 Layer7 필터가 가능한 IPS에서 차단 정책이 적용되기 전 단계로 그림 5/그림 6의 정상 HTTP 요청과 악성 HTTP 요청에 WEB Server가 정상

표 2. 실험 단계별 보안장비 NAT연계 및 자동차단 적용 결과

| 단계 | IPS 악성 HTTP 차단 | Firewall 악성 HTTP 차단 | 내부 구간 트래픽 Firewall <-NAT-> IPS | | | |
|---|---|---|---|---|---|---|
| | | | 정상 트래픽(평균) | | 악성 트래픽(평균) | |
| | | | Count | KBytes | Count | KByte |
| ❶ | 차단 X | 차단 X | 4,811 | 2,618 | 9,708 | 5,097 |
| ❷ | 차단 O | 차단 X | 7,275 | 3,927 | 6,311 | 518 |
| ❸ | 차단 O | 차단 O | 14,111 | 8,101 | 0 | 2 |

적으로 응답하고 있으며 트래픽이 일정하고 유지되고 됨. 그림 ❷ 단계에서 HTTP Header의 Layer7 User-Agent Attack 정보를 차단하는 정책이 적용되어 악성 HTTP 요청이 필터링되는 단계로 ❶->❷에서 정상 HTTP Packet Count가 약 50% 향상되었으며 IPS가 정상적으로 동작함을 확인 할 수 있지만 악성 HTTP Packet Count는 약 35% 정도 감소함을 확인 할 수 있으며 그림 5/6에서 정상 HTTP Packet Count 추이가 약 6,000에서 14,,000 까지 범위로 불안정하게 처리됨을 확인 활 수 있다. 이러한 결과는 User-Agent가 Attack으로 확인된 Packet을 차단하고 악성 HTTP 요청에 사용된 나머지 Packet들은 여전히 내부 구간에 ❶ 대비 약 65% 비율로 악성 HTTP Packet Count 가 발생하다. ❸ 단계에서 IPS에서 차단된 정보를 활용하여 Firewall 정책에 적용하기 위해서는 NAT Gateway에 의해 악성 HTTP 요청의 IP정보가 192.168.40.1 단일 IP로 변경되어 Firewall 차단 정책에 적용하지 못하는 문제을 표 3과 같이 NAT Gateway의 수집된 Connection Tracking Session 정보로 공격자 원천 IP/Port 정보를 이용하여 자동으로 Firewall에 차단정책이 적용되었으며 ❷->❸에서 ❶ 대비 악성 HTTP Packet Count가 100% 차단되고 정상 HTTP Packet Count가 초당 평균적으로 4,811에서 14,111건으로 9,300건이 증가되어 병목현상이 개선됨을 확인하였다.

그림 5. NAT&방화벽 연계 실험 결과 정상 HTTP Request Packet Count

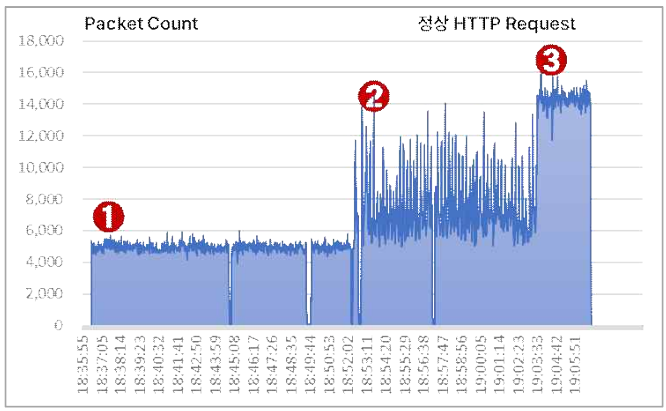


그림 6. NAT&방화벽 연계 실험 결과 정상 HTTP Request Packet Byte

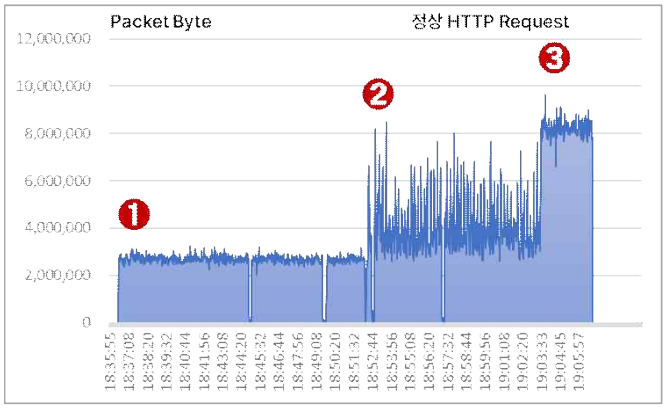



표 3. NAT Session 테이블(전체 중 일부 발췌)

| Firewall 차단정책 | NAT Session Table(conntrack) | | 차단 대상 IP |
|---|---|---|---|
| | 원본 공격자 IP:Port | NAT 변환 IP:Port | |
| DROP | 192.168.20.115:5097 | 192.168.40.1:50971 | 192.168.20.115 |
| DROP | 192.168.20.116:60898 | 192.168.40.1:60898 | 192.168.20.116 |
| DROP | 192.168.20.113:56118 | 192.168.40.1:56118 | 192.168.20.113 |
| DROP | 192.168.20.117:62149 | 192.168.40.1:62149 | 192.168.20.117 |
| DROP | 192.168.20.118:50421 | 192.168.40.1:44645 | 192.168.20.118 |

그림 7. NAT&방화벽 연계 실험 결과 악성 HTTP Request Packet Count

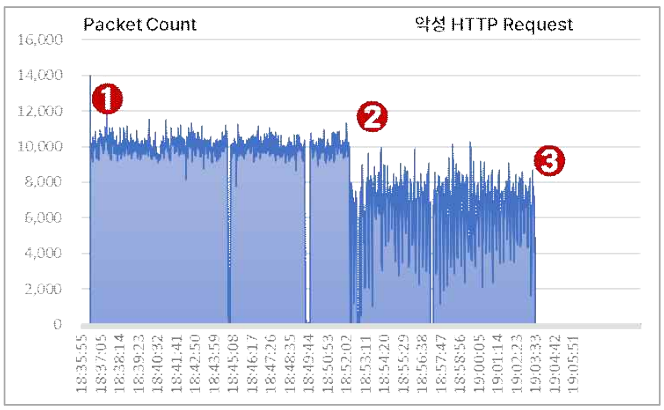
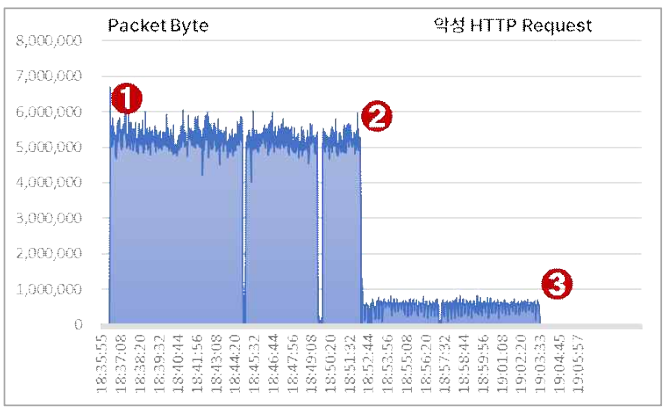



그림 8. NAT&방화벽 연계 실험 결과 악성 HTTP Request Packet Byte




## Ⅳ. 결론

본 논문에서는 공격성 트래픽이 내부 구간의 IPS 장비에서 방어가 가능하지만, 원천 차단되지 못하고 내부 네트워크 구간에서 발생하는 부하 현상을 개선하고, IP/Port 가 실시간으로 변화되는 공격과 NAT장비에 의해 원천 공격 정보가 변경되어 운영자가 차단하기 어려운 환경에서 운영자의 개입없이 자동으로 IPS, NAT Session Table, Firewall의 보안장비간 정보를 연계하여 자동으로 Firewall에 원천 공격 차단룰을 설정하는 시스템을 개발 및 실험하여 내부 네트워크 부하가 개선 가능함을 제시하였다.

본 논문에서는 VM을 이용한 실험 환경으로 구성하였으나 고부하 테스트가 가능한 별도로 분리된 장비의 물리적 구성과, 실제 환경의 다양한 네트워크 장비들에서도 ACL(Access Control List)로 적용 가능한 세션 데이터 수집 및 자동 차단 시스템으로 발전시키고자 한다.

## 참 고 문 헌


[1] 최선혜. "SIEM을 이용한 망분리 환경에서의 비정상 통신 점검 방안 연구." 국내석사학위논문 서강대학교 정보통신대학원, 2023. 서울

[2] 최정수. "SIEM 환경에서 SOAR 기반의 내부 보안대응 업무 자동화 방법론." 국내석사학위논문 중앙대학교 보안대학원, 2022. 서울

[3] 전형주. "SIEM과 威脅 시스템을 活用한 效率的인 保安管制 方案 硏究." 국내석사학위논문 성균관대학교 정보통신대학원, 2019. 서울

[4] "JMeter User's Manual," https://jmeter.apache.org/usermanual/index.html

[5] "snort3," Snort 3 is the next generation Snort IPS (Intrusion Prevention System)

[6] "PF_RING," High-speed packet processing framework, https://github.com/ntop/PF_RING