JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 7: 861~868, Jul. 2019

IDC용 소형 통합보안라우터의 실시간 트래픽쉐이핑과 IPS의 융합 구현

양승의[1] · 박기영[2] · 정회경[3*]

A Convergence Implementation of Realtime Traffic Shaping and IPS on Small Integrated Security Router for IDC

SeungEui Yang[1] · Kiyoung Park[2] · HoeKyung Jung[3*]

[1]CTO, HHOME & INTERMEDIA, HANJIN OFFICETEL 812Ho, Yuseong-gu, Daejeon 34187, Korea
[2]Graduate Student, Department of Computer Engineering, Paichai University, Daejeon 35345, Korea
[3*]Professor, Department of Computer Engineering, Paichai University, Daejeon 35345, Korea

요 약

최근 들어 빅데이터와 사물인터넷 그리고 인공지능 등 다양한 서버 기반의 서비스가 온라인상에서 이루어지고 있다. 이에 따라 안정적인 서버 운영을 지원하는 IDC(Internet Data Center)의 수요도 커지고 있다. IDC는 안정적인 회선과 전력공급시설을 갖춘 서버 입주시설로써 효율적으로 구분되어진 랙 단위 서브네트워크 상에 서버를 20~30대씩 묶어 관리하는 시설이다. 여기서는 랙 단위로 서버들의 보안, 방화벽, 트래픽 등을 효율적으로 관리해주는 방법이 필요하다. 즉 라우터, 방화벽, IPS 그리고 회선속도를 제어해 주는 트래픽쉐이핑 기능과 최근 관심 분야인 VPN 기술까지 지원해야 한다. 이를 지원하기 위해 3~5종의 상용 장비를 채택할 경우 도입비용은 물론 운용관리에 큰 부담일 수 있다. 따라서 본 논문에서는 5가지 기능을 하나의 랙 단위 소형 통합보안라우터에 구현하는 방법을 제시하고, 특히 IDC에서는 필수 기술인 트래픽 쉐이핑과 IPS를 융합 구현하며 이에 따른 효용성도 제시하고자 한다.

ABSTRACT

Various server-based services such as big data, IoT and artificial intelligence have been made online. As a result, the demand for IDC to support stable server operation is increasing. IDC is a server-based facility with a stable line and power supply facility that manages 20 to 30 servers in an efficiently separated rack-level subnetwork. Here, we need a way to efficiently manage servers security, firewall, and traffic on a rack-by-rack basis. Including traffic shaping capabilities that control routers, firewalls, IPS, and line speeds, as well as VPN technology, a recent interest. If three or five kinds of commercial equipment are adopted to support this, it may be a great burden to the management cost as well as the introduction cost. Therefore, in this paper, we propose a method to implement the five functions in one rack-unit small integrated security router. In particular, IDC intends to integrate traffic shaping and IPS, which are essential technologies, and to propose the utility accordingly.

키워드 : 라우터, 방화벽, 트래픽쉐이핑, IDS, OpenWRT

Keywords : router, firewall, traffic shaping, IDS, OpenWRT

Received 30 April 2019, **Revised** 30 April 2019, **Accepted** 22 May 2019

*** Corresponding Author** Hoekyung Jung(E-mail:hkjung@pcu.ac.kr, Tel:+82-42-520-5640)
Professor, Department of Computer Engineering, Paichai University, Daejeon 35345, Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.7.861 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

전통적인 웹서버, 스트리밍, 인트라넷 그리고 최근의 빅데이터, 클라우드 등 많은 서비스가 서버 기반에 운영되고 있다. 또한 사무실이 없는 온라인 비즈니스도 서버를 기반으로 개발, 영업, 기획, 마케팅, 판매 등이 이루어지고 있다. 이에 해킹에 안전하고 안정적인 서버운영이 사업성공의 필수적인 요소가 되고 있으며, 이를 지원해주는 기술서비스가 바로 인터넷 데이터 센터(IDC)이다. IDC는 작은 공간에 많은 서버를 유치해야 하기 때문에 랙 단위로 라우터, 스위치 등 통신 장비와 20여대의 슬림 서버를 슬롯형태로 패키징 하여 운영한다. 이렇게 함으로써 좁은 공간에 효율적인 통신 인프라, 전원관리 등을 제공하여 저렴한 비용에 고성능 서버를 운영할 수 있도록 한다. 여기서 중요한 문제는 네트워크 단위 혹은 서버 단위, 좀 더 세부적인 서비스 단위의 해킹 및 공격을 모니터링하고 방어하는 서비스를 제공해야하는데 있다. 또한 특정 서버에 문제가 발생했을 경우 동일한 네트워크에 있는 다른 서버들에 피해를 주지 않도록 해야 한다. 본 논문에서는 이를 해결하기 위해 그림 1과 같이 랙 단위의 소형 라우터를 기반으로 IPS 방화벽 그리고 네트워크별, IP별, 서비스 포트별로 세부적으로 트래픽을 제어할 수 있는 “개방형플랫폼 기반 데이터센터용 랙단위 통합 VPN 라우터”를 개발하고자 한다.

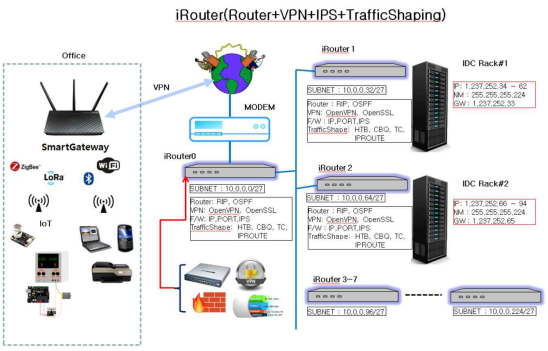

Fig. 1 Integrated VPN router configuration diagram

Ⅱ. 연구의 차별성 및 필요성

본 논문에서 제안하는 통합보안라우터는 랙단위 통합 네트워크 장비로써 라우터, VPN, 방화벽은 물론 트래픽쉐이핑과 IPS까지 모두 지원하는 장비이다. 시스코, 씨큐아이 등 비슷한 통합보안 장비가 있지만 대형장비이고 수천만원에서 1억이 넘는 고가의 장비이다. 본 연구에서는 랙단위 IDC용으로 적합하게 소형화 설계를 하고 실시간 다중큐잉 트래픽쉐이핑 기술과 IPS를 융합 구현하여 차별성을 가지도록 한다.

2.1. 통합(라우터+VPN+IPS방화벽+트래픽 쉐이퍼)의 필요성

네트워크 장비를 통합해서 얻을 수 있는 가장 큰 장점은 경제성이다. 5개의 기능을 하나로 만들면 비용을 1/5 정도로 줄일 수 있다. 또한 각 장비에서는 목적에 따라 네트워크 패킷을 레이어 2~5까지 필요한 레벨로 분리해서 분석하고 재조합하기 때문에 5개의 장비에서 중복 분석하는 것 보다 하나의 장비에서 하는 것이 효율적이다. 반면 하나의 장비에서 5가지 기능을 구현 하려면 관련 원천 기술을 모두 확보해야 하고, 타겟의 프로세싱 성능이 우수해야 한다. 각 원천 기술은 OpenWRT 기반에 RIP(Routing Information Protocol), OSPF(Open Shortest Path First), OpenVPN, SSL, 다중큐잉 커널, IPS 등으로 이에 대한 구현 기술은 이미 확보하고 있다. 또한 프로세싱 성능은 IDC에서 랙 단위의 25대 정도의 서버를 처리하면 되기 때문에 MediaTek이나 Atheros의 상용 네트워크 프로세서 정도의 성능에서도 가능하여 개발 비용이나 CPU 수급 등에 문제는 없을 것이다.

2.2. 실시간 트래픽 쉐이퍼의 필요성

IDC센터를 운영하기 위해서 가장 필요한 기술 중 하나가 바로 트래픽 쉐이핑 기술이다. 다양한 서비스를 하는 고객들의 서버 시스템을 IDC에 집중해 놓고 운영하다 보면 서버문제, 해킹문제, 트래픽문제, 바이러스 문제 등이 다양하게 일어 날 수 있다. 이는 문제를 유발시킨 서버는 물론 같은 네트워크에서 운영되는 다른 서버들에게 까지 피해를 주게 되어 심각한 서비스 품질 저하를 일으킬 수 있다. 개발하고자 하는 실시간 트래픽 쉐이퍼는 네트워크 트래픽 상황을 네트워크별, IP별, 서비스 포트별로 INBOUD, OUTBOUND 모두 모니터링 하고 대역폭을 조절할 수 있게 하여 트래픽 문제가 발생하더라도 전체적인 서비스 품질은 보장할 수 있도록 한다.

2.3. 라우터 및 IPS방화벽의 필요성

랙 단위로 라우터를 구성하여 다양한 고객의 다양한 서비스(100M공유, 10M 전용 등) 요구에 맞추어 네트워크를 분리 운영하여 효율적이고 경제적인 IDC 운영이 되도록 할 수 있다. 또한 네트워크 침입시도에 대해서는 패킷 분석을 통해 라우터 단에서 패킷을 차단할 수 있도록 하여 서버의 피해를 줄일 수 있게 한다.

2.4. VPN의 필요성

원격지 근무나 본사와 지사 간 안전한 네트워크 공유를 위한 VPN 서비스 요구는 꾸준히 커지고 있다. 또한 사물인터넷의 확산과 함께 기업내부의 센서 및 제어장치들을 안전하게 모니터링 하고 접근할 수 있는 서비스의 요구가 많아지고 있다. 이에 대한 서비스를 네트워크 VPN으로 제공 할 수 있다.

2.5. OpenWRT 플랫폼 필요성

이러한 통합 네트워크 장비를 개발하기 위해서는 하드웨어 및 소프트웨어 플랫폼이 중요하다. 지원 타겟 하드웨어가 다양하여 특정 타겟에 종속되지 말아야 하고 RIP, OSPF, OpenVPN, SSL, 다중큐잉, IPS 등 관련 커널 및 프로토콜 스택의 구현에 문제가 없어야 한다. 이를 만족시키는 우수한 플랫폼 중 하나가 OpenWRT이다. 선행연구에서는 OpenVPN과 다중큐잉 및 실시간 트래픽 쉐이핑에 대해서 구현 경험을 보유하고 있고 본 연구에서도 활용되고 있다.

Ⅲ. 통합 VPN 라우터

본 장은 통합 VPN 라우터 개발 과정을 서술한다. 선행 연구에서 다루었던 OpenWRT 플랫폼 구축과 VPN 프로토콜 구현은 간단히 설명하고, 새로운 라우터 프로토콜 구현 그리고 실시간 트래픽 쉐이핑과 IPS의 대표적인 기술인 snort를 구현하고 결합하는 방법은 구체적으로 제시한다.

3.1. OpenWRT 플랫폼 구축

통합 VPN 라우터는 VPN과 라우터프로토콜은 물론 IPS, 트래픽쉐이핑 등 핵심 프로토콜들이 모두 구현되어야 한다. 자칫 메모리, CPU부하가 커질 수 있기 때문에 효율적인 커널 튜닝이 필요하고 CPU 및 메모리 성능도 만족할 만한 타겟을 선정해야 한다.

3.1.1. OpenWRT 타겟 하드웨어 플랫폼 구현

게이트웨이를 구현하기 위한 타겟 하드웨어는 양산비용 측면에서 다양한 선택이 가능하다. 본 논문에서는 수급이 원활하며 가성비가 우수한 타겟 시스템을 선택하였다. 소형 통합 VPN 라우터로 양산비용이 저렴하고 성능은 snort 및 트래픽 쉐이핑 까지 가능하도록 구현하였다. 타겟 시스템에 대한 하드웨어/소프트웨어 스펙은 표1과 같다[1, 2].

Table. 1 Hardware / Software Specifications

Target	H/W Spec	S/W Spec
MT7621	- DualCore 880Mhz - Flash:16MB - RAM:128MB - LAN/WAN: 1G - WIFI: 802.11AC /N/G/B/A 2.4G/5G - USB3.0, PCI-E, MicroSD	- OpenWRT 14.07 / 15.05 - RIP, OSPF, Zebra, OpenVPN, iproute, snort, LuCi

3.1.2. OpenWRT 타겟 소프트웨어 플랫폼 구현

Linux에서 버전의 중요성은 커널 및 지원 디바이스 그리고 관련 프로토콜의 성능과 호환성 그리고 안정성 보장 등에 있다. OpenWRT도 리눅스 배포본 중에 한 종류이며 특히 네트워크 장비의 임베디드 플랫폼으로 유명한 것 중 하나이다. 데스크탑이나 서버용 Linux의 업그레이드도 큰 노력이 수반되지만 임베디드 시스템에서의 버전 업그레이드는 보안, 성능, 안정성은 물론 새로운 프로토콜 지원, 새로운 하드웨어 타겟 플랫폼 및 모듈 지원 등 그 중요성은 일반 Linux의 경우보다 훨씬 크다. 본 연구에서 사용한 최신의 Chaos Calmer 15.05의 특징은 커널 업그레이드, 시스템 안정성 향상, 버그 패치, 새로운 하드웨어 모듈 지원 등이 있고, 반면에 많은 프로토콜 및 패키지 들이 업그레이드 되었기 때문에 하위 호환에 주의를 해야 한다. 본 연구에 필요한 RIP, OSPF, VPN, IPS 등의 프로토콜은 이전 버전부터도 안정적인 동작이 가능하기 때문에 큰 문제는 없었다. 다만 실시간 트래픽쉐이핑을 위한 커널 튜닝과 타겟 플랫폼의 세밀한 설정과 컴파일은 여전히 중요한 부분이라 할 수 있다 [2-4].

3.1.3. 관련 프로토콜 스택 구현

선행연구에서 구현된 프로토콜 기술로서 필수 프로토콜을 기술하면 다음과 같다.

- VPN 터널링은 OpenVPN 기반에 네트워크 계층3에서 구현되는 OpenSSL로 구현하였다[5].
- 다중큐잉을 통한 트래픽쉐이핑

  ToS, QoS를 단일 큐잉에서 구현하는 기존의 네트워크 장비들과 달리 본 연구에서는 다중큐잉 지원 커널을 지원한다. 선행연구에서 구현되었고 본 연구에서는 IPS와 융합 구현을 할 것이다[1,6,7,8].

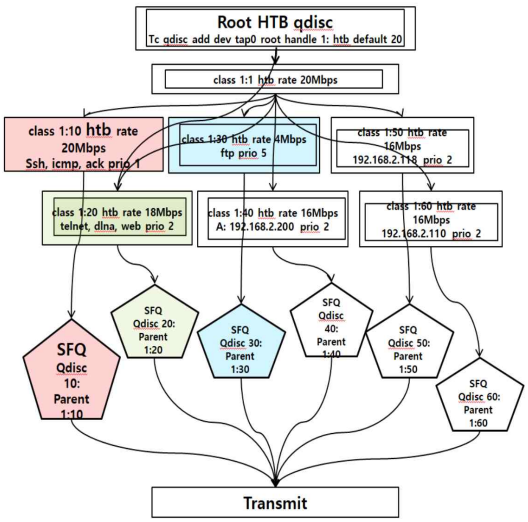

Fig. 2 Multiple-Queuing Traffic Shaping

다중 큐잉을 지원하기 위해서는 OS의 네트워크 커널에서 CBQ, SFQ, HTB 등을 지원하도록 커널 수정을 해야 하기 때문에 안정성 및 성능을 보장하기 위해서는 적절한 튜닝기술을 적용해야 한다. 본 연구에서는 다중 큐잉과 터널링을 지원하도록 커널을 수정하고 프로그램을 구현 하였다. 또한, 그림 2에서 보듯이 서로 다른 특성의 CBQ, SFQ, HTB 큐를 구성하고 각 큐에 서비스 포트별, IP 주소별로 할당하여 동작할 수 있도록 하였다[8].

3.1.4. RIP, OSPF 구현

대표적인 라우팅 프로토콜은 RIP(Routing Information Protocol)와 OSPF(Open Shortest Path First) 가 있다. RIP와 OSPF는 대표적인 IGP(Interior Gateway Protocol)로써 하나의 AS(Autonomous System)내의 라우터들끼리 라우팅 정보 교환을 위한 라우팅 프로토콜이다. 또한 AS들 간의 라우팅 정보 교환을 위해서는 EGP(Exterior Gateway Protocol)가 있고 EGP에는 BGP(Border Gateway Protocol)가 대표적인 프로토콜이다. 그림 3은 라우팅프로토콜에 대해 보여주고 있다.

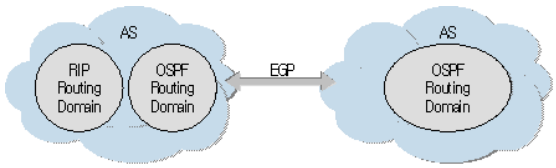

Fig. 3 Routing protocol

OpenWRT에서 RIP, OSPF를 구현하기 위해서는 라우팅 매니저인 zebra 패키지를 준비해야한다. zebra 패키지를 다운로드하여 설치하면 ripd(RIPv1,2), ospfd (ospfv2), bgpd, ripngd(IPv6), ospfd6d(IPv6) 라우팅 프로토콜을 지원하는 데몬(daemon) 들이 설치된다. 그림 4는 zebra의 실행구조를 보여준다. 이 데몬 들은 반드시 zebra와 연동되어야 하며, 단독으로 실행 될 수 없다. zebra의 중요한 특징 중의 하나는 CLI(Command Line Interface)를 지원하는 것인데 이 CLI는 VTYSH라는 쉘(Shell)을 이용함으로써 사용 가능하다. VTYSH는 putty를 이용하여 연결하게 되며 연결 하고자 하는 포트번호는 사용자가 /etc/service 파일을 수정함으로써 접근 가능하다. VTYSH를 이용하면 시스코라우터 설정과 동일하게 외부에서 putty을 이용하여 ripd, ospfd, zebra의 환경 설정이 가능하다[3].

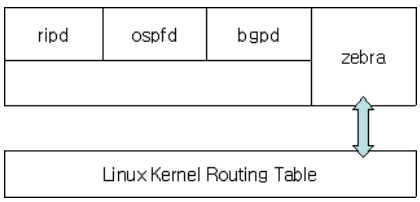

Fig. 4 Execution structure of 'zebra'

zebra는 현재 quagga로 버전이 업그레이드 되었고, Network->Routing and Redirection->quagga-> 로 이동하여 quagga-ospfd, ripd, vtysh, zebra 등을 선택하여 커널설정이 가능하다.

커널 컴파일이 성공적이라면 타겟 펌웨어를 업그레이드하고 구성하려는 라우팅구조에 맞게 zebra.conf, ripd.conf, ospf.conf 환경설정파일을 작성하면 최대 15 HOP 까지 라우팅을 구성할 수 있다.

3.1.5. IPS 구현

IPS는 방화벽에 이은 진화한 보안 솔루션이다. 네트워크 공격에 대한 방화벽의 차단이 실패하였을 경우에도 피해를 최소화하고 관리자의 부재 시에도 해킹에 적절히 대응해 주는 보안 솔루션이다. 즉 IPS는 방화벽이 단순한 룰에 따라 불법 침입을 차단하는데 따른 보안상의 한계점을 극복할 수 있게 한다.

IPS에는 크게 2가지 방법이 있다. 첫 번째, 오용침입탐지라고 불리는 Misuse IPS는 기본적으로 일어나서는 안 될 행위 패턴을 설정하고 패턴과 일치하는가를 확인하는 방법이다. 두 번째, 일어날 수 있는 극히 정상적인 사용에 대해서 사용자나 그룹, 프로그램, 시스템 리소스에서 비정상적인 행위가 일어나는 지를 탐지하는 Anomaly IPS 방법이 있다. 정확한 동작을 위해서는 다양한 침입패턴, 오용패턴코드를 적용하여 실시간 공격형태분석과 실제로 침입탐지와 오용탐지까지 찾아내는 것이 중요하다. 여기서 생각해봐야 하는 중요한 트레이드 오프는 바로 오탐에 대한 다음 2가지 시각이다.

- false positive : 실제 공격이 아닌데 IPS가 공격으로 잘못 판단하는 경우
- false negative : 실제 공격이 일어났지만 IPS가 이를 공격으로 생각하지 않는 경우

이러한 2가지 오탐은 모두 문제가 있다. false positive의 경우 정상적인 사용자 까지 불편을 야기하고, false negative의 경우 실제 공격에 대응을 못하는 문제를 가지고 있다. 여기서 어떤 방법을 선택해야할까 하는 것은 어려운 고민거리다. 이에 대한 해결방안은 다음 장에서 설명을 하고자 한다.

침입을 탐지하기 위해서는 나의 취약점과 침입 유형을 파악하고 있어야 한다. 침입이란 일반적으로 컴퓨터가 사용하는 자원의 무결성, 기밀성, 유효성을 저해하는 일련의 행위나 컴퓨터 시스템의 보안 정책을 파괴하는 행위를 침입이라고 정의한다. 표 2는 일반적인 침입수법의 분류를 나타낸다.

Table. 2 Invasion technique

Name	Attack Rule
Social Engineering	Deceptive administrators or users
Impersonation	Retrieving the privilege of users
Exploits	Using System Security Vulnerability
Transitive Trust	Trusted host or network disguise
Data Driven	attack program, trojan, backdoor, virus
Infrastructure	protocol/system Feature Vulnerability
DoS	Denial of Service
DDoS	Distributed Denial Of Service

OpenWRT에서 지원하는 대표적인 IPS는 snort이다. snort는 위에서 언급한 침입수법에 대한 IPS기능을 지원한다. 구현은 Network -> Firewall -> snort , snort-mysql 등을 선택하여 커널설정이 가능하다[9,10].

커널 컴파일이 성공적이라면 타겟 펌웨어를 업그레이드하고 snort.conf, local.rules 등 환경설정파일에 IPS 관련 로그, 패턴, 룰셋 등을 설정하면 원하는 동작을 구성할 수 있다.

Ⅳ. 트래픽 쉐이핑과 IPS

Snort의 기능은 막강하다. 유사한 솔루션 중 snort가 제일 오래되고 다양한 플러그인이 가능하기 때문에 IDS, IPS 보안솔루션과 접목하여 지능형 방화벽 개발이 가능하다. 물론 여기서 가장 중요한 부분은 룰셋이다. 해킹 및 공격의 방법은 나날이 새롭게 진화하기 때문에 IDS, IPS 방화벽은 여기에 발 빠르게 쫓아 갈 수 있어야 한다. 실제로 이제까지 나타난 다양한 공격 방법에 대한 룰셋이 공개되어 있고 이를 적용할 수 있다. 하지만 룰셋 자체를 이해하는 데에는 많은 시간과 실험과정이 필요하다. snort 및 관련 룰셋에 대한 매뉴얼만 봐도 방대한 기술에 대한 이해가 필요하기 때문에 본격적인 구현을 위해서는 더욱 깊이 있는 분석이 필요하다.

하지만 아무리 snort가 막강하고 룰셋을 잘 적용했다고 하더라도 3.1.5에서 언급한 2가지 오탐인 false positive와 false negative는 발생할 수밖에 없다. 룰셋을 엄격하게 적용하면 정상적인 사용까지 차단시키는 문제가 발생하고 느슨하게 적용하면 침입을 허용하는 문제가 발생한다. 또한 룰셋을 너무 엄격하게 적용할 경우 속도

딜레이가 발생하여 응답성이 떨어질 수도 있다.

본 논문에서는 이를 해결하고자 룰셋을 느슨하게 적용하여 빠른 검출이 가능한 패턴은 즉시 차단시키고 의심스러운 침입공격에 대해서는 허용을 하는 대신 트래픽 쉐이핑을 통해서 전체 네트워크에 문제를 일으키지 못하게 하는 방법이다. 또한 이런 의심 패킷의 트래픽에 대해서는 별도 모니터링을 하면서 공격으로 판단이 되면 차단시키도록 하여 룰셋을 느슨하게 하면서도 트래픽을 제어하면서 내부문제를 발생시키지 않고 천천히 확실히 잡아낼 수 있는 방법이라고 할 수 있다.

4.1. 실시간 트래픽 쉐이핑 및 IPS 계산

실시간 트래픽 쉐이핑 계산은 선행연구에서 CPU부하량 계산과 패킷DROP율 계산 그리고 다중큐잉에서 큐잉당 트래픽 계산에서 제시한 방법을 적용하며 여기서는 구체적인 설명을 생략한다[1]. 여기에 IPS 룰셋에서 다음과 같이 확장 적용하여 의심패킷에 대해서는 별도의 제한된 큐잉에 보내고 모니터링 하면서 공격확인이 되면 차단시키는 방법을 적용한다.

1) IPS룰셋

IPS와 트래픽 쉐이핑의 상호동작을 확인하기 위해서 다음의 공격을 가정한다. 보통 공격의 전초단계인 포트스캔이나 DOS공격의 하나로 대표적인 TCP SYNC-FIN 공격의 예를 들겠다.

- 룰설정

```
#vi local.rules
.....
alert tcp any any -> 192.168.219.0/24 any (flags: SF; ack: 0; msg:"SYNC-FIN packet detected"; sid: 2000013; )
.....
```

- 의미 분석

위의 예는 공격에 대해서 alert 메시지를 발생 시키라는 룰셋이다. 발생 조건은 tcp 프로토콜에 대하여/ 발생지는 모든 주소에서 모든 TCP 서비스포트에 대하여/ 목적지는 C 클래스192.168.219.0 네트워크로 가는 모든 TCP 프로토콜에 대하여/ flag 가 SF(SYNC-FIN) 이면서 ACK 값이 0인 패킷이다. 이런 조건이 만족되면 “SYNC-FIN packet detected” 라는 메시지를 로깅하게 된다. TCP flag가 SYNC-FIN 이면서 ACK 값이 0인 경우는 보통의 경우 발생하지 않는다. 이런 경우는 해킹툴의 앞단에서 실행되는 TCP 포트 스캐너가 동작할 경우 나타나는 현상이다.

- 해당되는 패킷 생성방법

외부 PC(192.168.1.66)에서 다음 명령으로 TCP 80번 포트면서 flag SYNC-FIN 인 패킷을 생성시킨다.

```
$sudo nping --tcp -p 80 --flags syn,fin 192.168.219.122
Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2015-10-17 22:44 KST
SENT (0.0509s) TCP 192.168.1.66:33239 > 192.168.219.122:80 SF ttl=64 id=48684 iplen=40 seq=1932467804 win=1480
.....
```

- alert 메시지 로깅 확인

```
$sudo tail -f /var/log/*
Oct 17 13:44:35 192.168.1.1 snort: message repeated 4 times: [ [1:2000013:0] SYNC-FIN packet detected {TCP} 192.168.1.66:33239 -> 192.168.219.122:80]
.....
```

위와 같이 IPS룰셋을 설정하고/ nping으로 패킷을 룰셋에 걸리도록 발생시키고/ tail 명령으로 로그 데이타를 모니터링하면/ snort룰셋에 정한대로 alert 메시지를 확인할 수 있다. 공격이 확실하면 DROP이나 REJECT 할 수 있지만 우선은 alert 로그만 남기고 다음 의심패킷관리에서 처리하도록 한다.

2) 의심패킷관리

별도의 프로세스를 통해서 snort에서 발생시킨 alert 메시지를 모니터링 한다. 의심패킷을 찾으면 우선 대역폭이 제한된 큐에 넣고 해킹체크함수가 판단하게 한다. 해킹 아님이 판단되면 큐에서 빼내서 정상패킷으로 돌리고/ 해킹으로 판단이 되면 일정시간 해당소스의 모든 패킷은 DROP(or REJECT) 시키고/ 판단되지 않으면 큐에 머물면서 후속패킷에 대해 다시 판단을 받으며 모니터링 할 수 있도록 한다.

이렇게 함으로써 false positive 오탐율은 0%까지 낮출수 있고, false negative 오탐율은 40%까지 상승할 수

있지만 제한된 트래픽 큐잉에서 의심패킷관리를 받으며 정확한 판단을 할 수 있는 점과 특히 다른 장비의 대역폭 피해를 받지 않는 장점이 있다.

여기서는 INBOUND 에 대한 테스트만 했지만 트래픽쉐이핑은 양방향 모두 가능하기 때문에 외부 공격외에도 내부 서버의 바이러스 감염에 의한 OUTBOUND 트래픽에 대한 큐잉도 가능하기 때문에 실질적인 트래픽 쉐이핑이 큰 효과를 발휘할 수 있다.

```
main() {
 while(1) {
  if (alert message? == yes) {
  callback (do ManageSuspectPacket(&Packet); ) }
 }}
ManageSuspectPacket( *Packet ) {
 n = SendPacketToQueing(Q1, Packet);
 while(1){
 if (CheckHack(n) == NO)
    DEQUE PACKET;  EXIT;
else  if (CheckHack(n) == YES)
    DROP/REJECT PACKET SOURCE A WHILE; EXIT;
else  if (CheckHack(n) == NOT DETERMINED)
    STAYQUE PACKET;
 }
}
```

4.2. 성능 분석

본 연구의 성능은 표 3과 같다. false negative 오탐의 경우 1차에서는 40% 이지만 모두 제한된 대역폭의 큐에 존재하기 때문에 전체 네트워크의 속도저하는 없다. 그리고 2차 탐지를 거치면 10% 이내의 오탐만 남게 된다. 여기서 오탐율 0%, 10%, 40%는 모두 설정을 통해 조정할 수 있다. 중요한 점은 다른 장비에 회선속도 저하를 유발하지 않는다는 것이며, 장비의 성능과 운용 전략에 맞추어 오탐율을 조정할 수 있다는 것이다. 탐지 알고리즘의 성능이 우수하면 빠르고 정확하게 차단시킬 수 있겠지만 우수하지 못해도 트래픽 쉐이핑 기술로 다른 장비에 주는 피해를 최소화 할 수 있다.

Table. 3 False rate Performance analysis

	Item	Result
1	false positive rate	0%
2	false negative rate 1st run	40%
3	false negative 2nd run	10%
4	Network slowdown During Attack	NONE

침입 탐지 및 차단에 대한 기술은 2000년대 초반부터 많은 발전을 해왔고, 다중 큐잉을 이용한 트래픽 쉐이핑 기술도 2010년대 중반부터 IDC의 회선 관리 및 비용 책정을 위해 도입되기 시작하였다. 하지만 이 두가지 기술을 융합하여 침입 탐지 후 바로 차단에 들어가지 않고 트래픽 쉐이핑 큐에서 세부탐지를 거쳐 오탐율을 줄이고 이 시간동안 공격에 의한 회선속도 피해도 최소화 하는 방법은 아직 찾아진 바 없으며 본 기술에 대해서는 특허출원 중에 있다.

Ⅴ. 결 론

30년 전부터 IT분야에서도 비용대비 효용은 바로 상용화를 판단하는 척도로 사용되고 있다. IT분야 중 특히 보안에 대해서는 더욱 그러하다. 해킹을 막기 위해서 장비를 도입하다보면 방화벽, IDS, IPS, VPN, 바이러스, 백도어, 인증, 감리, 포렌식.. 끝도 없고 비용은 감당하기 어렵다. 불행한 것은 이렇게 해도 100% 안전한 장비는 만들 수 없다. 목표를 90% 안전한 시스템에 두면 적절한 비용에 운영이 가능하지만 여기서 1%씩 더 안전한 시스템으로 올리기 위해서는 그 비용은 기하급수적으로 늘어난다. 여기서 선택할 수 있는 방법이 바로 트래픽 쉐이핑이다. 목표는 90%에 두고 나머지 10%의 문제는 실시간 트래픽쉐이핑을 통한 관리와 주변 피해를 최소화하고 탐지된 위협에 대해서는 모니터링하면서 관리해 주는 방법이다.

본 논문에서는 바로 이러한 목적에 따라 실시간 트래픽쉐이핑과 IPS를 접목한 데이터센터용 소형 통합 VPN 라우터를 만들었다. 향후 연구과제로 의심패킷을 관리 및 분석하는 알고리즘을 업그레이드하고 의심 패킷의 분석에 인공지능 기법까지 도입시킨다면 오탐율을 더욱 낮출 수 있고 점점 더 지능화 되고 있는 침입공격에 대해서도 대응 할 수 있는 방법이 될 것이다.

ACKNOWLEDGEMENT

This work (Grants No. S2594297) was supported by project for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Ministry of SMEs and Startups in 2018.

REFERENCES

[1] S. E. Yang, I. S. Kang, B. O. Go, and H. K. Jung, "A Realtime Traffic Shaping Method for VPN Tunneling on Smart Gateway Supporting IoT," *The Journal of Korea Institute of Information and Communication Engineering*, vol.21, no.6, pp. 1121-1126, 2017.

[2] (2015, May). "OpenWrt Chaos Calmer 15.05," [Internet]. Available:http://www.openwrt.org.

[3] K. Ishiguro. (2017, March). "A routing software package for TCP/IP networks" [Online]. Available:https://www.guagga.net, Ouagga 1.2.0.

[4] T. Jin, "OpenWrt Development Guide," Wireless Networks Lab, CCIS, MEU. Retrieved, Oct. 2013.

[5] Open VPN [Internet]. Available::http://openvpn.net/.

[6] The Linux Foundation. Retrieved. (2014, January). "Introduction to iproute2" [Online]. Available: http://www.linuxfoundation.org.

[7] B. Hubert. (2012, May). "Linux Advanced Routing & Traffic Control HOWTO" [Online]. Available: http://lartc.org/,DocBook Edition.

[8] S. E. Yang, B. O. Hog, J. K. Choi, and H. K. Jung, "Wired/Wireless Gateway System Supporting LAN-to-LAN VPN with Multi-Queuing Realtime Traffic Shaping," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 19, no. 5, May. 2015.

[9] The Snort Project, (2018, January). "SNORT Users Manual," [Online]. Available: https://www.snort.org, SNORT 2.9.12.

[10] F. Alam. (2015, March). "Intrusion Detection & SNORT," APRICOT2015, [Online]. Available: https://nsrc.org/workshops.

양승의(Seungeui Yang)

1989년 홍익대학교 전자계산학과(이학사)
1991년 홍익대학교 전자계산학과(이학석사)
2016년 배재대학교 컴퓨터공학과(공학박사)
1991년 ~ 1996년 국방과학연구소 연구원
1996년 ~ 2003년 (주)인터미디어 대표
2007년 ~ 2009년 (주)코아트리 이사
2010년 ~ 2014년 CEWIT Korea 연구위원
2013년 ~ 2016년 유넷(주) 이사
2016년 ~ 현재 인터미디어 이사, 행복을만드는집 이사
※관심분야 : OpenWRT, Embedded Linux, VPN, UPnP, DLNA, OLSR, USN, IPROUTE, IoT, snort

박기영(Kyyoung Park)

1997년 침례신학대학교 신학전공(문학사)
2002년 목원대학교 공공정책학과(문학석사)
2019년 배재대학교 컴퓨터공학과(공학석사)
2019년 ~ 현재 배재대학교 컴퓨터공학과(공학박사)
※관심분야 : Linux, Network, Embedded Linux System

정회경(Hoekyung Jung)

1985년 광운대학교 컴퓨터공학과(공학사)
1987년 광운대학교 컴퓨터공학과(공학석사)
1993년 광운대학교 컴퓨터공학과(공학박사)
1994년 ~ 현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 멀티미디어 문서정보처리, IoT, Machine Learning, BigData, Embedded System