소형 통합보안라우터의 실시간 트래픽쉐이핑과 IPS의 융합

김도안[1] · 송현옥[2] · 이성옥[3] · 양승의[4] · 정회경[1*]

[1]배재대학교 · [2]다솜정보 · [3]㈜클로벌인재개발 · [4]HHOME & INTERMEDIA

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

Doan Kim[1] · Hyunok Song[2] · Sungok Lee[3] · Seungeui Yang[4] · Heokyung Jung[1*]

[1]PaiChai University · [2]DASOMSOFT · [3]Global HRD Inc · [4]HHOME & INTERMEDIA

E-mail : doan0105@naver.com, paperblue21@hanmail.net, jesuissarah@naver.com, alex@im.co.kr, hkjung@pcu.ac.kr

요 약

IDC(Internet Data Center)는 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. 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

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. 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

router, linux, firewall,traffic shaping, IDS, IPS, OpenWRT, VPN

Ⅰ. 서 론

전통적인 웹서버, 스트리밍, 인트라넷 그리고 최근의 빅데이타, 클라우드 등 많은 서비스가 서버 기반에 운영되고 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. 본 논문에서는 이를 해결하기 위해 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.

Ⅱ. 트래픽 쉐이핑과 IPS

Snort의 기능은 막강하다. 유사한 솔루션 중 snort가 제일 오래되고 다양한 플러그인이 가능하기 때문에 IDS, IPS 보안솔루션과 접목하여 지능

* corresponding author

형 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.

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.

2.1 실시간 트래픽 쉐이핑 및 IPS 계산

실시간 트래픽 쉐이핑 계산은 선행연구에서 CPU 부하량 계산과 패킷DROP율 계산 그리고 다중큐잉에서 큐잉당 트래픽 계산에서 제시한 방법을 적용하며 여기서는 구체적인 설명을 생략한다[1,2]. 여기에 IPS 룰셋에서 다음과 같이 확장 적용하여 의심패킷에 대해서는 별도의 제한된 큐잉에 보내고 모니터링 하면서 공격확인이 되면 차단시키는 방법을 적용한다. 해당되는 패킷 생성방법은 다음과 같다.

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 IPS 룰셋을 설정하고/ nping으로 패킷을 룰셋에 걸리도록 발생시키고/ tail 명령으로 로그데이타를 모니터링하면/ snort룰셋에 정한대로 alert 메시지를 확인할 수 있다. 공격이 확실하면 DROP이나 REJECT 할 수 있지만 우선은 alert 로그만 남기고 다음 의심패킷관리에서 처리하도록 한다.

2.2성능 분석

본 연구의 성능은 Table. 1과 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 운용전략에 맞추어 오탐율을 조정할 수 있다는 것이다.

Table. 1 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

III. 결 론

본 논문에서는 실시간 트래픽쉐이핑과 IPS를 접목한 데이터센터용 소형 통합 VPN 라우터를 만들었다. 향후 연구과제로 의심패킷을 관리하는 알고리즘을 업그레이드하고 인공지능 분석기법까지 도입시킨다면 오탐율을 더욱 낮출 수 있고 점점 더 지능화 되고 있는 침입공격에 대해서도 대응 할 수 있는 방법이 될 것이다.

Acknowledgements

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. U. Yang, I. S. Kang, B. O. Go, 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. Jun 2017.

[2] S. E. Yang, B. O. Hog, J. K. Choi, 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.