P4 기반 방화벽에 대한 연구

김수연, 박태준*
전남대학교(학부생), *전남대학교(교수)
rlatndus6205@jnu.ac.kr, *taejune.park@jnu.ac.kr

A Study on Firewall using P4

Sooyeon Kim, Taejune Park*
Chonnam National Univ., *Chonnam National Univ.

요 약

네트워크 사용량이 증가함에 따라 네트워크 보안 위협 또한 증가하고 있다. 네트워크 방화벽은 네트워크를 보호하는 첫 번째 방어 수단이라는 의미에서 중요하다. 기존의 하드웨어 기반 방화벽과 SDN(Software Defined Network) 기반 방화벽은 각각의 한계점이 있다. 이러한 한계점을 극복하기 위해 하드웨어를 프로그래밍할 수 있는 언어인 P4를 기반으로 하는 방화벽이 등장했다. 이러한 P4 기반 방화벽은 소프트웨어의 성능 문제와 하드웨어의 벤더 종속성을 해결했다. 본 논문에서는 P4 기반 방화벽의 등장 배경과 P4의 특징을 살펴보고, P4 기반 방화벽 애플리케이션의 연구 동향을 분석한다. 또한, 이를 바탕으로 P4 기반 방화벽이 향후 어떤 방향으로 연구되어야 하는지 방향성을 제시한다.

Ⅰ. 서 론

1-1. 등장 배경

1) 네트워크 사용량의 증가

현재 사회는 의료, 교육, 산업, 금융 등 다양한 분야에 네트워크를 사용하고 있다. 특히 디지털 기술의 발전과 코로나19의 영향으로 네트워크를 사용해 다양한 원격 환경에서 네트워크를 사용하는 경우가 급증하고 있다. 이로 인해 네트워크는 현대 사회의 핵심 인프라로서의 역할을 다하고 있다. 그러나 이러한 네트워크 사용량의 증가는 동시에 다양한 네트워크 보안 위협을 수반한다.

2) 네트워크 보안 위협의 증가와 방화벽의 중요성

네트워크 사용량의 증가와 병행하게, 네트워크 보안 위협 또한 더욱 복잡해지고 규모가 증가하고 있다. 해킹, 개인정보 유출, 랜섬웨어, DDoS 등의 공격은 네트워크 보안에 심각한 위협을 가하며, 네트워크 환경에 악영향을 끼치고 있다. 네트워크가 현대 사회의 핵심 인프라로서의 역할을 수행하고 있는 상황에서 이러한 공격들이 네트워크 보안에 악영향을 끼치지 않도록 네트워크를 안전하게 관리하는 것은 중요한 과제이다. 네트워크 방화벽인 네트워크에 위협을 가하는 다양한 공격들로부터 네트워크를 보호하는 첫 번째 방어선 역할을 한다. 본 논문에서는 P4를 사용해 네트워크 방화벽을 구현한 다양한 연구를 살펴보고자 한다.

3) 보안 위협을 완화할 솔루션들 등장

네트워크 보안 위협의 증가에 따라 공격을 완화하고 네트워크 환경을 보다 안전하게 만들기 위한 다양한 솔루션들이 개발되고 있다. 방화벽 부분에서도 연구가 꾸준히 진행되고, 이를 바탕으로 훨씬 발전되고 세밀화된 방화벽 솔루션들이 등장했다. 허나, 기존의 하드웨어 기반 방화벽은 업데이트를 위해 하드웨어 장비를 수정하기 위해서는 하드웨어 공급업체가 방화벽을 재설정해야 한다. 즉, 네트워크 변경은 각 하드웨어 장비를 직접 손봐야하는 번거로움이 있으며 이는 시간과 비용 효율성이 떨어진다 [1]. 이를 해결하기 위해 SDN(Software Defined Netwrok) 기반의 방화벽이 등장했다. SDN은 중앙 집중식 컨트롤러를 통해 네트워크를 중앙 집중식으로 관리한다. SDN 기반 방화벽은 중앙 집중식 컨트롤러에서 보안 정책을 설정한 후 이러한 정책에 따라 패킷 필터링을 수행한다. SDN은 동적으로 변화하는 네트워크 환경에 대응하기 위해 설계되었기 때문에, SDN 기반 방화벽도 이러한 네트워크 환경에 대응하기 위한 기능을 제공해야 한다. 허나, 이러한 기능들의 사용은 애매한 흐름 경로, 충돌 발생 시 우선순위 처리, 성능 문제, 동시 업데이트 무시 등의 문제가 존재한다 [2].

1-2. P4 기반 방화벽 등장

기존 하드웨어 솔루션과 SDN 기반의 솔루션들의 이러한 문제점을 해결하기 위해 P4 기반 방화벽이 등장했다. P4는 하드웨어를 프로그래밍 가능하도록 함으로써 소프트웨어의 성능 문제와 하드웨어의 벤더 종속성을 해결했다. 이렇게 P4를 사용해 프로그래밍 가능하도록 만든 스위치를 사용하면 네트워크 방화벽은 네트워크 구조와 기능을 유연하게 변경할 수 있고 이를 통해 네트워크 보안성을 강화할 수 있다.

본 논문에서는 기존 하드웨어 기반 방화벽과 SDN 기반 방화벽의 한계에 언급한 후 P4 기반 방화벽의 필요성에 대해 설명한다. 이후, 본론에서 방화벽의 중요성을 설명한 후 방화벽에서 P4를 사용해야 하는 이유에 대해 알아보고 다양한 P4 기반 방화벽 애플리케이션의 연구 현황에 대해 살펴본다. 마지막으로는 P4 기반 방화벽이 향후 어떤 방향으로 연구되어야 하는지 방향성을 제시하고자 한다.

Ⅱ. 본론

2-1. Background

1) 방화벽

방화벽은 네트워크 내부로 들어오는 침입자나 악성 공격을 차단하고 내부에서 외부로 정보가 유출되는 것을 방지하는 보안 시스템이다. 방화벽은 기본적으로 네트워크를 통과하는 트래픽을 검사하고 사전에 정의한 보안 규칙에 기반하여 허용되지 않은 트래픽을 차단하는 패킷 필터링을 수행한다. 이를 통해 방화벽은 침입자나 악성 공격으로부터 네트워크를 보호하는 문지기와 같은 역할을 수행한다. 또한, 방화벽은

다양한 연구를 거쳐 패킷 필터링 외에도 다양한 역할을 수행하거나 특정한 기술을 집중적으로 수행하도록 발전했다 [3,4,5]. 이러한 연구를 통해 방화벽은 네트워크의 일정 부분에서만 사용되는 것이 아니라 IT 사회의 전반적인 부분에서 사용되는 방향으로 발전하고 있다.

2) P4 (Programming Protocol-Independent Packet Processors)

P4 [6,7]는네트워크 장비를 위한 오픈 소스, Domain-specific 프로그래밍 언어이다. P4는 스위치, 라우터와 같이 데이터 평면에서 동작하는 장비들이 어떻게 패킷을 처리하는지에 대해 정의할 수 있고 프로토콜과는 독립적으로 즉, 프로토콜의 종류에 구애받지 않고 패킷 처리 동작 방식을 프로그래밍할 수 있는 언어이다. 이를 가능하게 한 것은 match-action 테이블의 개념인데, P4는 match-action 테이블을 직접 프로그래밍할 수 있다. 이는 IP, TCP와 같이 형식적인 프로토콜뿐만 아니라 프로그래머가 자신이 필요한 헤더를 직접 작성하고 그 헤더에 맞는 match-action 테이블도 직접 구현 가능하다는 뜻이다. 이러한 특징은 P4를 통해 프로그래밍 되는 데이터 평면이 벤더 종속성으로부터 자유로워질 수 있게 만들어준다. 또한, P4는 스테이지와 파이프라인 측면에서 병렬성도 지원함으로써 성능을 높이고 있다 [6]. 이러한 유연성과 성능 향상 기능을 가지고 있는 P4는 방화벽, IDS 및 IPS, 로드 밸런서, 네트워크 모니터링 도구와 같은 다양한 보안 구성 요소에서 널리 활용되고 있다.

2-2. P4 기반 방화벽 애플리케이션

1) P4 기반 방화벽 애플리케이션의 장점

P4 언어의 가장 큰 특성 중 하나는 프로토콜 독립성으로부터 나오는 유연성이다. P4 기반 방화벽 또한 이러한 특성을 가지고 있고 이는 현재까지의 방화벽 솔루션들이 가지지 못한 몇 가지 장점을 제공한다. 첫 번째 장점은 빠른 적응력이다. 새로운 취약점이 발견될 경우 기존의 방화벽들이 새로운 업데이트를 적용하기까지 걸리는 시간이 필요한데 P4를 사용할 경우 프로그래머가 필요한 보안 규칙을 직접 프로그래밍하고 배포함으로써 걸리는 시간을 단축할 수 있다. 이는 제로데이 공격과 같이 빠른 대응이 필요한 상황에서 중요한 장점이 된다. 또 다른 장점으로는 맞춤형 보안 정책 구현이 있다. P4를 사용하면 네트워크에서의 특정 요구 사항에 맞춰 세밀하게 조정된 보안 정책을 구현할 수 있다. 이는 표준화된 기존 보안 솔루션으로는 해결하기 어려운 특정한 네트워크 환경에 맞는 보안 정책을 구현할 수 있게 해준다. 마지막으로 이러한 P4 방화벽은 네트워크의 확장성을 고려하여 설계될 수 있으며, 이는 미래에 새로운 네트워크 환경이 등장하더라도 새로운 네트워크에 빠르게 적응할 수 있다는 것을 의미한다.

2) P4 기반 방화벽 애플리케이션

P4 Guard [8]는 P4 언어를 사용해서 프로그래밍 가능한 데이터 평면에 소프트웨어 방화벽을 구현한다. 제어 평면과 데이터 평면으로 구성되며, 컨트롤러는 방화벽 서비스를 동적으로 제공하고 통계 정보를 기반으로 네트워크를 모니터링한다. P4 데이터 평면에 구현된 소프트웨어 방화벽은 미리 정의된 방화벽 정책에 따라 패킷을 parse하고 deparse하기 위해 데이터 평면에 match-action 테이블을 정의했다.

CoFilter[9]는 P4를 사용해 프로그래밍 가능한 데이터 평면에서 stateful 패킷 필터를 구현한다. CoFilter는 프로그래밍 가능한 데이터 평면을 사용해 고성능, 저비용의 장점을 갖고 있을 뿐만 아니라, P4의 프로그래밍 가능하다는 특징을 사용해 유연성 또한 달성했다. 이를 통해 효율적으로 상태 패킷 필터링을 수행함으로써 네트워크 연결의 보안을 강화할 수 있다.

이렇게 P4 기반 방화벽 애플리케이션에 대한 연구가 진행되고 있음에도 아직 P4 기반 방화벽에는 여러 문제점이 남아있다 [10,11]. 이 뿐만 아니라 Neupane et al.이 작성한 Next generation firewall for network security [12]에서는 사이버 공격이 점점 더 증가하고 있고 이러한 공격을 막기 위해서 DPI를 사용하는 새로운 방화벽이 등장해야 한다고 말하고 있다. 현재 P4 기반 DNS 패킷 DPI 시스템 [13]도 존재하지만 DNS 패킷에만 국한된다는 한계점이 존재한다.

Ⅲ. 결론

현재 네트워크가 더욱 복잡해지면서 네트워크 방화벽의 중요성이 점점 커지고 있다. 동시에, 새로운 P4 프로그래밍 언어가 주목받기 시작하면서 이 둘을 결합한 P4 기반 방화벽 또한 중요해지고 있다. 미래 세대는 현재의 P4 방화벽이 가지고 있는 문제점을 해결하고 next generation firewall에서 언급한 보안 이슈를 해결하고 DPI를 완벽하게 수행할 수 있는 P4 방화벽을 목표로 꾸준히 연구를 진행해야 한다.

ACKNOWLEDGMENT

본 연구는 한국인터넷진흥원(KISA)-정보보안 특성화대학 지원사업 및 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2022R1C1C1006967).

참 고 문 헌

[1] Suh, Michelle, et al. "Building firewall over the software-defined network controller." *16th International Conference on Advanced Communication Technology*. IEEE, 2014.

[2] Dixit, Vaibhav Hemant, et al. "Challenges and Preparedness of SDN-based Firewalls." *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*. 2018.

[3] Kim, Dong-Yong, and Hyoung-Kee Choi. "Efficient design for secure multipath TCP against eavesdropper in initial handshake." *2016 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2016.

[4] Trabelsi, Zouheir, et al. "Improved session table architecture for denial of stateful firewall attacks." *IEEE Access 6* (2018): 35528-35543.

[5] Aziz, Mohd Zafran Abdul, et al. "Performance analysis of application layer firewall." *2012 IEEE Symposium on Wireless Technology and Applications (ISWTA)*. IEEE, 2012.

[6] Bosshart, Pat, et al. "P4: Programming protocol-independent packet processors." *ACM SIGCOMM Computer Communication Review* 44.3 (2014): 87-95.

[7] P4, “P4 Open Source Programming Language”, (https://p4.org/)

[8] Datta, Rakesh, et al. "P4guard: Designing p4 based firewall." *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018.

[9] Cao, Jiamin, et al. "CoFilter: High-Performance Switch-Accelerated Stateful Packet Filter for Bare-Metal Servers." *IEEE Transactions on Parallel and Distributed Systems* 33.9 (2021): 2249-2262.

[10] Hauser, Frederik, et al. "A survey on data plane programming with p4: Fundamentals, advances, and applied research." *Journal of Network and Computer Applications* 212 (2023): 103561.

[11] Kfoury, Elie F., Jorge Crichigno, and Elias Bou-Harb. "An exhaustive survey on p4 programmable data plane switches: Taxonomy, applications, challenges, and future trends." *IEEE access* 9 (2021): 87094-87155.

[12] Neupane, Kishan, Rami Haddad, and Lei Chen. "Next generation firewall for network security: a survey." *SoutheastCon 2018*. IEEE, 2018.

[13] AlSabeh, Ali, et al. "P4ddpi: Securing p4-programmable data plane networks via dns deep packet inspection." *NDSS Symposium 2022*. 2022.