SDN기반의 I2NSF 프레임워크를 이용한 NSF 모니터링과 로드 밸런싱

홍동진, 정재훈

성균관대학교 전자전기컴퓨터공학과

{dong.jin, pauljeong}@skku.edu

NSF Monitoring and Load Balancing using I2NSF based on SDN

Dongjin Hong, Jaehoon (Paul) Jeong

Department of Computer Science and Engineering, Sungkyunkwan Univ.

요 약

본 논문은 I2NSF(Interface to Network Security Functions) 프레임워크에서 NSF(Network Security Functions)들을 모니터링하고 로드 밸런싱 하는 방법에 대해 소개한다. 방화벽이나 안티바이러스와 같은 동일한 기능을 하는 NSF가 있음에도 불구하고 패킷을 분산하여 처리하지 못하는 것은 비효율적이다. 본 논문에서는 기존의 프레임워크를 토대로 NSF 와 Security Controller가 통신하기 위한 메시지 형식을 IETF(Internet Engineering Task Force) I2NSF Working Group에서 제안한 IM(Information Model)을 토대로 모니터링과 로드 밸런싱을 추가한 향상된 프레임워크를 소개한다. NSF 모니터링과 로드 밸런싱을 추가한 프레임워크는 NSF들에게 패킷을 분배함으로써 프레임워크의 처리율을 향상시킬 수 있다.

Ⅰ. 서 론

최근 네트워크를 소프트웨어를 통해 동적으로 관리할 수 있는 SDN(Software-Defined Networking)[1] 기술과 네트워크 리소스를 가상화하여 사용 할 수 있는 NFV(Network Functions Virtualization)[2] 기술은 서로 시너지효과를 만들며 연구 및 개발 활동이 활발하게 이루어지고 있다. 특히, IETF(Internet Engineering Task Force) I2NSF(Interface to Network Security Functions) Working Group[3]은 SDN 및 NFV를 기본 인프라로 이용하는 네트워크 환경에서 네트워크 보안 서비스(Network Security Service)를 제공하기 위한 표준 인터페이스를 정의하고 구현하는 것을 목표로 한다. 기존에 구현된 SDN기반의 I2NSF 프레임워크는 정책 생성과 생성된 정책을 기반으로 Firewall, IDS, IPS, Anti-DDoS, Anti-Virus 등과 같은 네트워크 보안함수(Network Security Functions, NSF)에 규칙을 만들어 적용하여 보안 서비스를 제공한다[4]. 하지만 기존에 구현된 프레임워크는 방화벽이나 안티바이러스와 같이 동일한 기능을 하는 NSF가 있음에도 불구하고 패킷을 분산하여 처리하는 것이 불가능하기 때문에 비효율적일 수 있다. 따라서 본 논문에서는 정책과 규칙 생성 및 적용이 가능한 기존 프레임워크와 더불어 IETF I2NSF WG에서 제안한 NSF를 모니터링하기 위한 IM(Information Model)[5]을 사용하여 NSF 모니터링과 로드 밸런싱이 가능한 향상된 프레임워크를 제안하려한다. 본 논문에서는 모니터링으로 인한 오버헤드는 고려하지 않는다.

NSF를 주기적으로 그리고 포괄적으로 모니터링 하는 것은 보안 서비스를 제공하는 프레임워크를 효율적으로 사용하기 위한 관점에서 중요한 역할을 한다. 본 논문에서는 I2NSF 프레임워크 환경에서 NSF가 생성하는 모니터링 정보 중 네트워크 트래픽 상태와 리소스 사용에 대한 정보를 보안 제어기(Security Controller, SC)가 지속적으로 모니터링 한다면 네트워크 트래픽을 NSF들에게 패킷을 분산시킴으로써 부하를 줄일 수 있으며 이는 프레임워크의 처리율을 향상시킬 것으로 예상된다.

Ⅱ. 본 론

1. 기존에 구현된 I2NSF 프레임워크

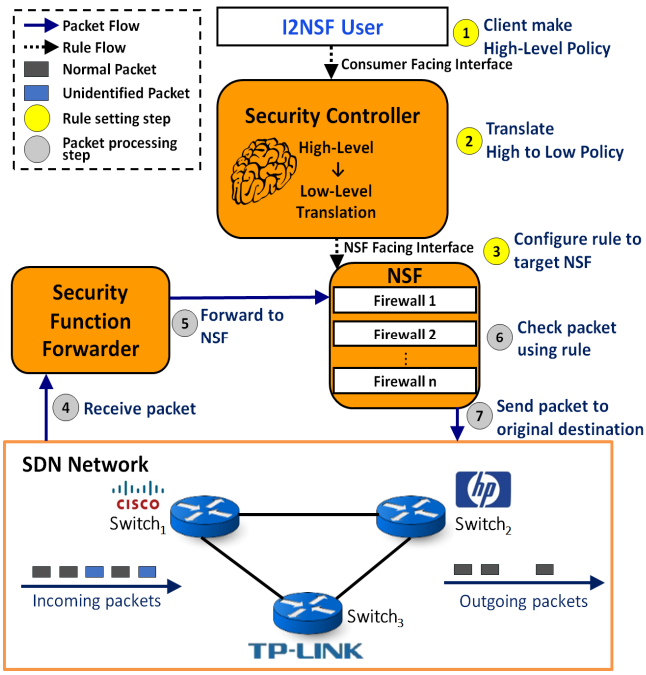

그림 1. I2NSF 프레임워크 기반의 보안 서비스 제공 구성도

그림 1은 기존에 구현된 I2NSF 프레임워크 기반의 보안 서비스 제공 구도를 보여준다. 프레임워크 기반의 보안 서비스는 크게 정책 및 규칙 생성과 적용, SDN Network로부터 수신된 패킷의 처리로 구분할 수 있다.

첫 번째, I2NSF 클라이언트가 RESTCONF[6] 프로토콜과 YANG[7] 데이터 모델링 언어 사용하여 관리자가 이용하는 I2NSF User 응용프로그램과 SC를 통신하게 하는 Consumer Facing Interface를 통해 SC로 내린

상위 수준의 정책을 SC가 하위 수준의 정책으로 번역한 뒤 NETCONF[8] 프로토콜과 YANG를 사용하여 SC와 NSF를 통신하게 하는 NSF Facing Interface를 통해 규칙이 생성되고 특정 NSF들에 규칙을 적용한다.

두 번째, 기존에 구현된 프레임워크는 SDN 네트워크에 의해 스위치로부터 확인되지 않은 패킷을 전달 받아 보안 함수 전달자 (Security Function Forwarder, SFF)를 시작으로 NSF를 거쳐 최종적으로 목적지로 향하게 하는 I2NSF 프레임워크를 경유하게 되고 이 때 패킷은 NSF에 의해 조사, 필터링 등의 조치를 취하도록 구현되어져있다.

2. NSF 모니터링과 로드 밸런싱이 가능한 향상된 프레임워크

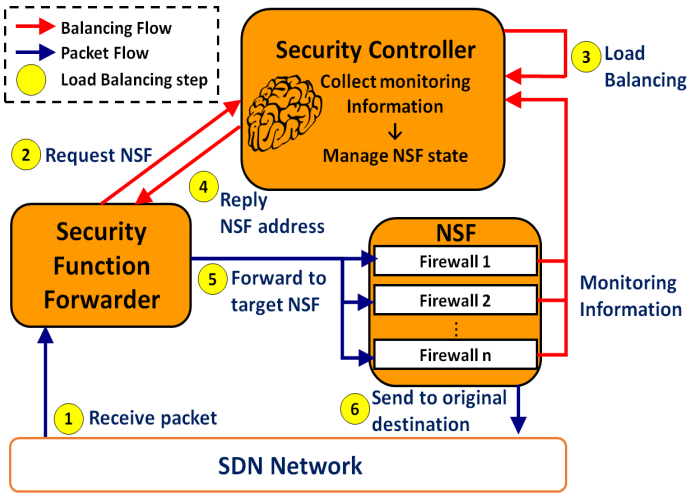

그림 2. I2NSF 프레임워크 기반 NSF 모니터링 및 로드 밸런싱 구성도

그림 2는 본 논문이 제안하는 기존 프레임워크 기반의 NSF 모니터링 및 로드 밸런싱이 가능한 향상된 프레임워크를 전반적으로 보여준다.

기존의 프레임워크처럼 SFF는 SDN 네트워크로 부터 패킷을 전달받고 SC에게 수신된 패킷을 어떤 NSF로 전달해야 할지 소켓 통신을 통해 요청한다. SC는 NETCONF/YANG을 이용한 통신으로 프레임워크 내부에 등록된 NSF들로부터 모니터링 정보(시스템 상태, CPU 사용률, 메모리 사용률, 디스크 사용률, 남은 디스크 공간 등)를 수신하여 NSF들의 상태를 판단하고 해당 패킷을 처리할 특정 NSF의 IP주소를 SFF에게 알려준다. SFF는 NSF의 IP주소를 가지고 패킷을 전달함으로서 로드 밸런싱이 일어난다. 이후 과정은 기존 I2NSF 프레임워크 기반의 보안서비스에서의 순서와 같다.

그림 3은 본 논문이 제안하는 인터넷 표준화 기구에서 제안한 것과 유사한 구조의 NSF에 의해 주기적으로 생산되고 수집되고 SC와 통신할 때 전송해야 할 정보의 형식이며 아래는 형식에 대한 설명이다[5].

Version	Type	Time	NSF_name	Vender_info	Severity

그림 3. NSF Monitoring Information Model 기반의 메시지 형식

- Version : 데이터 형식의 버전을 나타낸다. 값으로는 01부터 시작하는 2자리 10진수이다.
- Type : 이벤트, 경고, 알람, 카운터, 로그 등의 값을 사용한다. 본 논문에서 제안한 향상된 프레임워크를 위해 시스템 상태, CPU 사용률, 메모리 사용률, 디스크 사용률, 남은 디스크 공간, 그리고 트래픽 정보를 제공하는 Resource Utilization Logs를 사용해야한다.
- Time : 메시지가 생성된 시간을 나타낸다.
- NSF_name : 메시지를 생성하는 NSF의 이름 또는 IP 주소를 나타낸다.
- Vender_info : NSF 공급업체의 이름을 나타낸다.
- Severity : 메시지가 가지는 심각한 정도를 나타내며 0에서 7까지 총 8개의 단계로 구성된다. 숫자가 작을수록 심각도가 더 높다.

Ⅲ. 결 론

본 논문에서는 기존에 구현된 I2NSF 프레임워크는 동일한 기능을 하는 NSF가 있음에도 불구하고 분산처리를 하지 못하는 것은 비효율적이기 때문에 기존 프레임워크를 통한 보안서비스와 인터넷 표준화기구에서 제안한 모니터링 IM을 적용하여 부하 분산이 가능한 향상된 프레임워크에 대해 연구하였다. 본 논문의 향상된 프레임워크가 처리 효율 및 프레임워크 내부의 트래픽 흐름을 향상시키며 표준화를 위해 기여할 수 있다고 믿는다. 향후 연구로 Mininet[9]에서 제안된 프레임워크를 개발하고 SFF 내부에서 주소 값을 관리하는 Cache를 설계하려 한다.

ACKNOWLEDGMENT

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발)

참 고 문 헌

[1] ONF, “Software-Defined Networking: The New Norm for Networks,” ONF White Paper, 2012.

[2] ETSI-NFV, “Network Functions Virtualization (NFV); Architectural Framework”, ETSI GS NFV 002 V1.1.1, October 2013.

[3] IETF I2NSF Working Group, “Interface to Network Security Functions(I2NSF),” https://datatracker.ietf.org/wg/i2nsf/charter/

[4] K. Jinyoung, M. D. Firoozjaei, J. P. Jeong, H. Kim, and J. S. Park, “SDN-based Security Services using Interface to Network Security Functions,” Proceedings of the 7th International Conference on ICT Convergence (ICTC), pp. 526 - 529, Oct. 2015.

[5] L. Xia, D. Zhang, Y. Wu, R. Kumar, A. Lohiya, and H.Birkholz, “An Information Model for the Monitoring of Network Security Functions(NSF),” IETF draft-zhang-i2nsf-info-model-monitoring, Mar, 2017.

[6] A. Bierman, M. Bjorklund, and K. Watsen, "RESTCONF Protocol", IETF RFC 8040, Jan, 2017.

[7] M. Bjorklund, "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)," IETF RFC 6020, Oct. 2010.

[8] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, “Network Configuration Protocol (NETCONF),” IETF RFC 6421, Jun, 2011.

[9] Mininet, “An instant virtual network on your laptop” http://mininet.org.