# 서비스 인식 보안 서비스 기능 체이닝 구성 연구

조현준, 김경백

전남대학교 정보보안협동과정

# A Study of Service Aware Security Service Function Chaining Composition

Hyeonjun Jo, Kyungbaek Kim

Interdisciplinary program of Information Security, Chonnam National University

요 약

네트워킹에 필요한 모든 유형의 자원을 추상화 하는 NFV 기술을 이용하여 복잡해지는 네트워크 환경에서 네트워크 관리의 용이성, 관리 비용 감소 등 네트워크 환경에서의 효율성을 얻고 있다. 하지만 최근 취약점이 존재하는 클라우드 기반 애플리케이션 서비스 요청이 증가하고 있으며, NFV 기술을 효과적으로 이용하기 위해 보안이 고려된 서비스 요청 방법에 대한 연구가 필요하다. 이 논문은 NFV에서 지원되는 보안 기능을 사용하여, 서비스 기능 체이닝 으로 구성된 네트워크 서비스 에서 각각 다른 서비스 요청 시 보안 인식된 서비스 기능 체이닝 구성 방법에 대해 제안한다.

## I. 서론

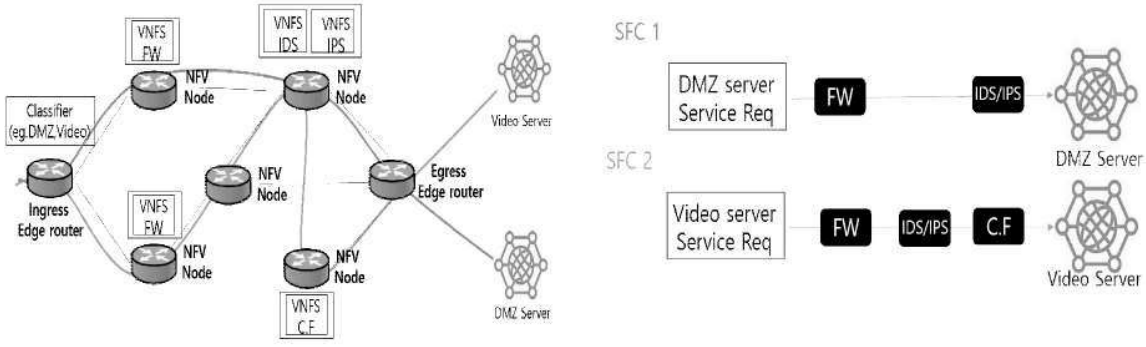
5G 융복합 사업에 대한 수요와 스마트화를 시도하는 기업이 점차 증가함에 따라 다양한 네트워크 인프라 및 서비스는 빠르게 성장 할 뿐만 아니라 정부의 비대면 산업을 육성함에 따라 네트워크상 사용자가 요구하는 서비스는 급격히 증가하고 있다. 또한, 새로운 서비스를 도입하기 위해 네트워크 유연성을 높이고 시간 및 비용을 줄일 수 있는 NFV 기술을 사용하여 기존 하드웨어에서 제공된 기술(IDS, IPS, FW 등)을 가상화하여 소프트웨어로 구현하여 이들을 상황 변화에 따라 유연하게 제공되고 있다

NFV는 VNF 체인을 통해 실행되는 서비스에 대하여 무결성, 기밀성이 보장되어야 한다. 하지만 NFV는 스니핑, 분산 서비스 거부 등 사이버 공격의 취약점에 노출되어 있으며, 제공되는 장점을 충분히 사용하려면 각기 다른 VNF의 간의 보안을 고려하여 서비스 체인을 구성해야 한다.

서비스 기능 체이닝(SFC)은 트래픽 유형에 따라 네트워크 기능을 선택적으로 조합하고 실행하여 트래픽별로 맞춤형 서비스를 제공할 수 있다[1]. 이러한 서비스 기능 체이닝 기술 특징을 사용할 경우 복잡해지는 네트워크 환경에서의 서비스 다변화에 대한 문제를 해결할 수 있다. 이 논문은 서비스 기능 체이닝이 지원되는 네트워크에서, 서비스의 보안 요구사항을 고려하여 사용자의 서비스 요청을 보안 인식된 서비스 요청으로 동적으로 수정하는 방법을 제안한다.

## II. 보안 요구사항

VNF 지원 서비스들을 위한 보안 기능을 서비스 기능 체이닝에 추가하기 위해서 NFVI에서 존재하는 취약점에 대한 대응할 수 있는 보안 기능에 대하여 설명하고, DMZ 구간에 위치하는 웹, 이메일, FTP 서버들에 대하여 서비스 보안 인식된 서비스 요청 모범 사례 방법을 설




(a) (b)

그림 1 (a) : SFC in NFVI, (b) : Service request Flow(SFC 1,2)

명한다.

2.1 위협 및 대응 보안 기능

[2]의 저자는 NFVI에서 발생 할 수 있는 보안 위협을 제시하였으며 특히 피해 대상이 VNF인 DDoS 공격, 악성코드 삽입 등을 분석하였다. 보안 장비(SE)는 침입 차단·탐지 시스템, 방화벽 등이 될 수 있으며 요청 서비스에 따라 보안 서비스를 제공할 수 있다. 표1에서는 네트워크 보안 시스템의 종류를 정리하였다.

표 1. 네트워크 보안 시스템의 종류

| 특징 | 보안 장비 |
|---|---|
| 외부 사용자들이 내부 네트워크에 함부로 접근하지 못하도록 정해진 보안 규칙 집합을 기반으로 트래픽을 허용 및 차단 | 방화벽(Firewall) |
| 기존의 방화벽이 탐지할 수 없는 악의적인 네트워크 트래픽을 탐지하는 시스템 | 침입 탐지·차단 시스템 (IDS) |
| 인터넷과 같은 공중 데이터 통신망을 이용해 개인이 구축한 통신망과 같이 이를 직접 운용할 수 있는 기술 | 가상사설망(VPN) |
| 네트워크 기반 기기를 위해 부적절하고, 비생산적인 웹 콘텐츠와 불법적인 악성 웹 콘텐츠를 차단하고 관리 | 콘텐츠 필터링 |

2.2 보안 인식 서비스 요청 모범 사례

기존 네트워크 환경에서 보안 장비를 이용하여 요청하는 서비스에 대한 보안 인식된 서비스 요청 모범 사례에 대하여 설명한다. 비디오, 웹·이메일·FTP 서버를 이용한 서비스 체인 구성 시 필요한 보안 서비스들은 다음과 같이 정리할 수 있다.

(1) 웹·이메일·FTP 서버

웹·이메일·FTP 서버와 같이 외부에서 접근되어야 할 필요가 있는 서버들은 DMZ 구간에 설치된다. 외부 사용자가 DMZ 구간에 위치하는 서버들에게 요청 순서는, 외부 네트워크에서 DMZ로 가기 위해서 방화벽, 침입 탐지·방지 시스템을 거쳐 통신 해야한다.

(2) 비디오 서버

개인영상정보등 민감 콘텐츠 영상을 다루는 특성상 웹 서버 시스템 보다 높은 보안(악의적인 공격 및 해킹 대응)을 구성해야 하며, 방화벽, 침입 탐지·방지 시스템, 콘텐츠 필터링을 거쳐 통신해야 한다[3].

## III. 보안 인식 서비스 요청 방법

NFV에서 지원되는 보안 기능을 사용하여 보안 인식된 서비스 요청을 구성하기 위해 먼저 하드웨어에서 제공되었던 보안 기능(NAT, 방화벽 등)을 NFVI에서 가상 네트워크 보안 기능(VNSF)으로 배치 후 보안 인식된 서비스 요청 구성에 대해 제안한다.

3.1 NFVI 모델

NFVI를 모델링하기 위해 다음과 같이 그래프($G_s=(N_s,L_s)$)로 표시 할 수 있다. 이때 $N_s$는 NFVI 노드($n_s$)들의 집합이며 $L_s$는 링크($l_s$)들의 집합을 의미한다. $A(n_s)$는 노드($n_s$)의 제한된 자

원(CPU, 스토리지 및 메모리)의 가용 용량을 의미하며 링크$bw(l_s)$는 링크$(l_s)$에서 사용 가능한 대역폭을 의미한다.

그림 1의 (a)에서의 NFVI 노드 7개와 9개의 엣지를 포함하는 소규모 NFVI Topology를 구성하였다. 이와 같이 구성된 네트워크를 이용하여 해당 트래픽이 인입되었을 때 해당 트래픽별 보안 요구 사항을 충족시키기 위해 가상 네트워크 보안 기능(VNSF) 서비스가 존재하는 NFVI 노드를 경유하게 된다.

3.2 VNF 배치

VNF 배치는 VNF의 요구 사항(CPU 코어 수, 메모리 등)을 해당 자원을 제공 할 수 있는 물리 노드에 매핑하는 것을 의미한다.

이 논문에서의 NFV 환경에서의 FW, IDS/IPS, 콘텐츠 필터링(C.F) 배치하기 위해 다음과 같은 사항을 고려하였다.

⑴ VNF 타입

일반적으로 IDS/IPS는 탐색 엔진 및 검사 영역이 동일한 특성을 가지고 있으며, 탐지와 차단 영역에서 역할이 나누어 진다. 이와 같이 유형이 비슷한 타입을 묶어 동일 NFVI에 IDS/IPS를 배치 하였다.

⑵ VNF CPU 부하

DMZ에 위치한 서버, 비디오 서버와 통신을 하기 위해서는 모든 트래픽은 초기 방화벽을 거쳐 트래픽별 가상 네트워크 보안 기능(VNFS)을 이용하여 서비스 기능 체이닝을 구성한다. 만약 하나의 NFVI에서 방화벽 기능을 수행하게 된다면 CPU의 부하는 높아질 것이며 결과적으로 NFV 이점을 얻을 수 없게 될 것이다. 따라서 2개의 NFVI에 방화벽을 배치하였다.

3.3 서비스 인식 보안 서비스 기능 체이닝

가상 네트워크 보안 기능(VNSF)을 추가하여 사용자가 각 서버에 서비스 요청 시 2.2 절에서 언급한 보안 인식 서비스 요청 사례를 접목하여 그림1의 (b)와같이 서비스 기능 체이닝을 구성한다. 결과적으로 NFV 상의 지원 보안 기능을 적절하게 이용하면서 각기다른 서비스들 간의 종단간 보안 인식된 서비스 요청을 수행할 수 있게 된다.

## IV. 결론 및 향후 연구

NFV기술이 주는 장점을 온전히 이용하려면 취약점이 존재하는 클라우드 기반 애플리케이션에 대하여 적절한 보안 조치가 필요하다. 이에 본 논문에서는 보안 모범 사례를 참고하여 사용자 요청 서비스별 서비스 기능 체이닝에 가상 네트워크 보안 기능(VNFS)을 추가하는 보안 인식된 서비스 요청 방법을 제안하였다.

향후, 가상 네트워크 보안 기능(VNSF) 최적의 배치 문제 해결 방법과 동적으로 서비스 기능 체이닝 경로를 제공하기 위해 효율적인 알고리즘 연구도 진행할 계획이다.

## ACKNOWLEGEMENTS

"이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임"(IITP-2019-0-01343)

## [참고문헌]

[1] Bhamare, Deval, et al. "A survey on service function chaining." Journal of Network and Computer Applications 75 (2016): 138-155.

[2] S. Lal, T. Taleb and A. Dutta, "NFV: Security Threats and Best Practices," in IEEE Communications Magazine, vol. 55, no. 8, pp. 211-217, Aug. 2017.

[3] KISA, "정보보호시스템 구축을 위한 실무 가이드", 2018