(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2018 년 5 월 31 일 (31.05.2018)

WIPO | PCT

(10) 국제공개번호
WO 2018/097422 A1

(51) 국제특허분류:
H04L 29/06 (2006.01) *H04L 12/24* (2006.01)

(21) 국제출원번호: PCT/KR2017/004510

(22) 국제출원일: 2017 년 4 월 27 일 (27.04.2017)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2016-0157771 2016 년 11 월 24 일 (24.11.2016) KR
10-2016-0160786 2016 년 11 월 29 일 (29.11.2016) KR

(71) 출원인: **성균관대학교 산학협력단 (RESEARCH&BUSINESS FOUNDATION SUNGKYUNKWAN UNIVERSITY)** [KR/KR]; 16419 경기도 수원시 장안구 서부로 2066, Gyeonggi-do (KR).

(72) 발명자: **정재훈 (JEONG, Jaehoon)**; 46294 부산시 금정구 금강로 225, 204-1501, Busan (KR). **현상원 (HYUN, Sangwon)**; 07071 서울시 동작구 보라매로5길 51, 2105, Seoul (KR). **우상욱 (WOO, Sanguk)**; 13564 경기도 성남시 분당구 탄천로 59, 509-1103, Gyeonggi-do (KR). **여윤석 (YEO, Yunsuk)**; 01676 서울시 노원구 노원로 532, 907-1001, Seoul (KR).

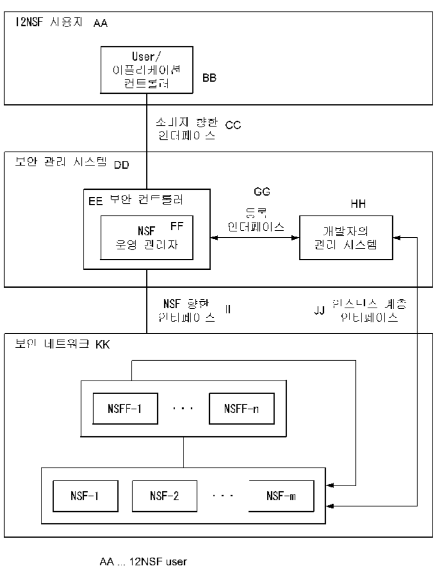
(74) 대리인: **특허법인 로얄 (ROYAL PATENT & LAW OFFICE)**; 08806 서울시 관악구 남부순환로 2072, 도원회관 빌딩 1층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: METHOD AND SYSTEM FOR TRAFFIC STEERING TRIGGERED BY NETWORK SECURITY FUNCTION, AND DEVICE THEREFOR

(54) 발명의 명칭: 네트워크 보안 기능에 의해 트리거되는 트래픽 스티어링을 위한 방법 및 시스템, 이를 위한 장치



AA ... 12NSF user
BB ... User/application controller
CC ... Consumer-directed interface
DD ... Security management system
EE ... Security controller
FF ... NSF operation manager
GG ... Registration interface
HH ... Management system of developer
II ... NSF-directed interface
JJ ... Instance layer interface
KK ... Security network

(57) Abstract: Disclosed are a method and a system for traffic steering triggered by a network security function (NSF), and a device therefor. Particularly, a system for supporting traffic steering triggered by an NSF can comprise an NSF forwarder (NSFF) for: performing a security check on a packet introduced to the system; determining whether an additional check by another NSF is necessary, on the basis of the result of the security check; attaching, to the packet, a packet forwarding header for summoning the additional check if the additional check is necessary; and transmitting the packet to a second NSF if a first NSF for transmitting, to the NSFF, the packet to which the packet forwarding header is attached and a second NSF having a security capability required for the additional check included in the packet forwarding header are discovered.

(57) 요약서: 네트워크 보안 기능(Network Security Function)에 의해 트리거되는 트래픽 스티어링(traffic steering)을 위한 방법 및 시스템, 이를 위한 장치가 개시된다. 구체적으로, 네트워크 보안 기능(NSF: Network Security Function)에 의해 트리거되는 트래픽 스티어링(traffic steering)을 지원하는 시스템에 있어서, 상기 시스템에 유입된 패킷에 대한 보안 검사를 수행하고, 상기 보안 검사의 결과에 기반하여 또 다른 NSF에 의한 추가적인 검사가 필요한지 여부를 판단하고, 상기 추가적인 검사가 필요하면, 상기 추가적인 검사를 호출하기 위한 패킷 전달 헤더(packet forwarding header)를 상기 패킷에 부착하고, 상기 패킷 전달 헤더가 부착된 패킷을 NSF 전달자(NSFF: NSF Forwarder)에게 전송하는 제1 NSF 및 상기 패킷 전달 헤더에 포함된 상기 추가적인 검사를 위해 요구되는 보안 능력을 가진 제2 NSF를 탐색한 경우, 상기 제2 NSF에게 상기 패킷을 전달하는 NSFF를 포함할 수 있다.

WO 2018/097422 A1

[다음 쪽 계속]

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 네트워크 보안 기능에 의해 트리거되는 트래픽 스티어링을 위한 방법 및 시스템, 이를 위한 장치

기술분야

[1] 본 발명은 보안 서비스를 제공하는 시스템에 관한 것으로서, 보다 상세하게 네트워크 보안 기능(NSF: Network Security Function)에 의해 트리거되는 트래픽 스티어링(traffic steering)을 위한 방법 및 시스템, 이를 위한 장치에 관한 것이다.

배경기술

[2] 오늘날 통신 사업자 및 인터넷 서비스 제공 업체와 같은 다양한 기업에서 운영 비용을 줄이고 보다 효율적이고 유연한 방법으로 자원을 활용하기 위해 네트워크 기능 가상화(NFV: Network Functions Virtualization) 기술을 널리 채택하고 있다. 또한, 제3자(third-party)의 서비스 공급 업체에 의해 제공되는 네트워크 기능 및 자원의 사용이 점차 대중화되고 있다. 기업들은 자신의 네트워크 시스템 및 정보 자산을 보호하기 위하여, 보안 기기(security appliance)를 직접 운영하는 대신에 third-party 보안 공급 업체에 의해 제공되는 보안 기능을 가입하여 사용하기 시작하였다.

[3] 이러한 운영 모델은 다양한 이점을 제공한다. 회사는 물리적인 보안 장비 구매에 비용을 지불하지 않아도 되기 때문에 자본 지출(capital outlay)을 줄일 수 있다. 또한, 다양한 공격 시그니처(attack signature)에 대한 최신(up-to-date) 데이터베이스를 항상 유지할 수 있다.

[4] 다만, 보안 기능(security function)은 다수의 솔루션 공급 업체(solution vendor)에 의해 개발되고, 다수의 네트워크 운영자에 의해 관리되기 때문에, NFV 기반 보안 기능(NFV-based security function)을 성공적으로 배포하기 위해서는 표준화가 요구된다.

발명의 상세한 설명

기술적 과제

[5] 본 발명의 목적은 네트워크 보안 기능(NSF: Network Security Function)에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 프레임워크를 제안한다.

[6] 본 발명에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

[7] 본 발명의 일 양상은, 네트워크 보안 기능(NSF: Network Security Function)에 의해 트리거되는 트래픽 스티어링(traffic steering)을 지원하는 시스템에 있어서,

상기 시스템에 유입된 패킷에 대한 보안 검사를 수행하고, 상기 보안 검사의 결과에 기반하여 또 다른 NSF에 의한 추가적인 검사가 필요한지 여부를 판단하고, 상기 추가적인 검사가 필요하면, 상기 추가적인 검사를 호출하기 위한 패킷 전달 헤더(packet forwarding header)를 상기 패킷에 부착하고, 상기 패킷 전달 헤더가 부착된 패킷을 NSF 전달자(NSFF: NSF Forwarder)에게 전송하는 제1 NSF 및 상기 패킷 전달 헤더에 포함된 상기 추가적인 검사를 위해 요구되는 보안 능력을 가진 제2 NSF를 탐색한 경우, 상기 제2 NSF에게 상기 패킷을 전달하는 NSFF를 포함할 수 있다.

[8] 바람직하게, 상기 패킷 전달 헤더는 상기 패킷의 보안 검사의 결과를 포함하는 동작 코드 필드, 상기 추가적인 검사를 위해 요구되는 보안 능력 정보를 포함하는 능력 정보 필드, 상기 능력 정보 필드의 개수를 나타내는 능력 정보의 수 필드를 포함할 수 있다.

[9] 바람직하게, 상기 시스템에 유입된 패킷은 상기 NSFF에 의해 수신되고, 상기 NSFF에 의해 상기 제1 NSF에게 전달될 수 있다.

[10] 바람직하게, 상기 패킷의 소스(source)의 신뢰 레벨(trust level)에 따라 상기 제1 NSF에 의해 상기 패킷은 안전한 패킷(secure packet), 위험한 패킷(dangerous packet) 및 의심스러운 패킷(suspicious packet)으로 분류될 수 있다.

[11] 바람직하게, 상기 패킷이 상기 안전한 패킷(secure packet)으로 분류된 경우 또 다른 NSF를 통해 추가의 보안 검사 없이 상기 패킷의 목적지(destination)으로 전달될 수 있다.

[12] 바람직하게, 상기 패킷이 상기 위험한 패킷(dangerous packet)으로 분류된 경우 상기 패킷은 드랍(drop)될 수 있다.

[13] 바람직하게, 상기 패킷이 상기 의심스러운 패킷(suspicious packet)으로 분류된 경우 상기 패킷은 상기 패킷 전달 헤더가 부착되어 상기 NSFF에게 전달될 수 있다.

[14] 바람직하게, 이용 가능한 모든 NSF에 대한 정보 리스트를 관리하는 NSF 운영 관리자(operation management)를 더 포함할 수 있다.

[15] 바람직하게, 상기 제2 NSF를 탐색하지 못한 경우, 상기 NSFF는 상기 추가적인 검사를 위해 요구되는 보안 능력을 포함하는 NSF 생성 요청 패킷을 상기 NSF 운영 관리자에게 전송하고, 상기 NSF 운영 관리자로부터 생성된 제3 NSF에 대한 정보를 수신하면 상기 제3 NSF에게 상기 패킷을 전달하고, 상기 NSF 운영 관리자는 상기 정보 리스트 내에서 각 NSF의 트래픽 로드 상태를 고려하여 상기 추가적인 검사를 위해 요구되는 보안 능력을 가지는 상기 제3 NSF를 선택하고, 상기 제3 NSF에 대한 정보를 상기 NSFF에게 전송할 수 있다.

[16] 바람직하게, 상기 정보 리스트 내에서 상기 추가적인 검사를 위해 요구되는 보안 능력을 가지는 NSF가 존재하지 않는 경우, 개발자 관리 시스템(developer's management system)에게 상기 추가적인 검사를 위해 요구되는 보안 능력을 가지는 NSF의 생성을 요청할 수 있다.

[17] 바람직하게, 상기 NSF 운영 관리자가 이용 가능한 모든 NSF의 트래픽 로드 상태를 모니터링하고, 특정 NSF에 대하여 과도한 트래픽이 발생됨을 감지하면, 개발자 관리 시스템(developer's management system)에게 상기 과도한 트래픽이 발생된 NSF와 동일한 보안 능력을 가지는 새로운 NSF의 생성을 요청할 수 있다.

[18] 바람직하게, 상기 NSF 운영 관리자가 이용 가능한 모든 NSF의 트래픽 로드 상태를 모니터링하고, 특정 NSF가 이용되지 않음을 감지하면, 개발자 관리 시스템(developer's management system)에게 상기 이용되지 않는 NSF의 제거를 요청할 수 있다.

[19] 본 발명의 다른 일 양상은, 네트워크 보안 기능(NSF: Network Security Function)이 트래픽 스티어링(traffic steering)을 수행하는 방법에 있어서, 상기 트래픽 스티어링(traffic steering)을 지원하는 시스템에 유입된 패킷에 대한 보안 검사를 수행하는 단계, 상기 보안 검사의 결과에 기반하여 또 다른 NSF에 의한 추가적인 검사가 필요한지 여부를 판단하는 단계, 상기 추가적인 검사가 필요하면, 상기 추가적인 검사를 호출하기 위한 패킷 전달 헤더(packet forwarding header)를 상기 패킷에 부착하는 단계 및 상기 패킷 전달 헤더가 부착된 패킷을 NSF 전달자(NSFF: NSF Forwarder)에게 전송하는 단계를 포함하고, 상기 패킷 전달 헤더는 상기 추가적인 검사를 위해 요구되는 보안 능력에 대한 정보를 포함할 수 있다.

[20] 바람직하게, 상기 패킷 전달 헤더는 상기 패킷의 보안 검사의 결과를 포함하는 동작 코드 필드, 상기 추가적인 검사를 위해 요구되는 보안 능력 정보를 포함하는 능력 정보 필드, 상기 능력 정보 필드의 개수를 나타내는 능력 정보의 수 필드를 포함할 수 있다.

[21] 바람직하게, 상기 패킷의 소스(source)의 신뢰 레벨(trust level)에 따라 상기 제1 NSF에 의해 상기 패킷이 안전한 패킷(secure packet), 위험한 패킷(dangerous packet) 및 의심스러운 패킷(suspicious packet)으로 분류될 수 있다.

발명의 효과

[22] 본 발명의 실시예에 따르면, NSF 간에 트래픽 스티어링을 가능하게 하고, 다양한 타입의 NSF를 통해 네트워크 트래픽의 복합적인 검사(composite inspection)를 가능하게 한다.

[23] 또한, 본 발명의 실시예에 따르면, 동적으로 생성된 NSF 인스턴스(instance)들을 통한 로드 밸런싱(load balancing)을 제공할 수 있다.

[24] 또한, 본 발명의 실시예에 따르면, 표준화된 인터페이스 및 데이터 모델을 이용함으로써, 다양한 네트워크 보안 기능(NSF)들을 제어 및 관리를 단순화 할 수 있다.

[25] 또한, 본 발명의 실시예에 따르면, NSF의 추상적인 뷰(abstract view)만을 사용자에게 제공함으로써, 사용자 친화적인(user-friendly) 보안 정책 설정(specification)을 가능하게 한다.

[26] 또한, 본 발명의 실시예에 따르면, NSF가 동적으로 활성화/비활성화(enabled/disabled)됨에 따라 다양한 네트워크 조건 및 보안 요구사항을 지원할 수 있다.

[27] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[28] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부 도면은 본 발명에 대한 실시예를 제공하고, 상세한 설명과 함께 본 발명의 기술적 특징을 설명한다.

[29] 도 1은 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템의 구성을 예시한다.

[30] 도 2는 기존의 서비스 기능 체인 아키텍처를 예시한다.

[31] 도 3은 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 NSF 능력에 대한 정보 모델을 예시하는 도면이다.

[32] 도 4는 본 발명의 일 실시예에 따른 패킷 필터링 능력을 가지는 NSF(들)을 위한 정보 모델(IM)을 예시한다.

[33] 도 5는 본 발명의 일 실시예에 따른 트래픽 스티어링을 개념적으로 설명하기 위한 도면이다.

[34] 도 6은 본 발명의 일 실시예에 따른 패킷 전달 헤더(Packet Forwarding Header)를 예시한다.

[35] 도 7은 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 트래픽의 흐름을 예시하는 도면이다.

[36] 도 8은 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 트래픽의 흐름을 예시하는 도면이다.

[37] 도 9는 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 로드 밸런싱 방법을 예시하는 도면이다.

[38] 도 10 내지 도 13은 본 발명의 일 실시예에 따른 NSF에 의해 트리거된 트래픽 스티어링 프레임워크를 활용하여 유입되는 VoIP/VoLTE 패킷에 수행되는 단계별 절차를 예시한다.

[39] 도 14는 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 방법을 예시한다.

[40] 도 15는 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 장치의 블록 구성도를 예시한다.

발명의 실시를 위한 형태

[41] 이하, 본 발명에 따른 바람직한 실시 형태를 첨부된 도면을 참조하여 상세하게 설명한다. 첨부된 도면과 함께 이하에 개시될 상세한 설명은 본 발명의 예시적인 실시형태를 설명하고자 하는 것이며, 본 발명이 실시될 수 있는 유일한 실시형태를 나타내고자 하는 것이 아니다. 이하의 상세한 설명은 본 발명의 완전한 이해를 제공하기 위해서 구체적 세부사항을 포함한다. 그러나, 당업자는 본 발명이 이러한 구체적 세부사항 없이도 실시될 수 있음을 안다.

[42] 몇몇 경우, 본 발명의 개념이 모호해지는 것을 피하기 위하여 공지의 구조 및 장치는 생략되거나, 각 구조 및 장치의 핵심기능을 중심으로 한 블록도 형식으로 도시될 수 있다.

[43] 이하의 설명에서 사용되는 특정 용어들은 본 발명의 이해를 돕기 위해서 제공된 것이며, 이러한 특정 용어의 사용은 본 발명의 기술적 사상을 벗어나지 않는 범위에서 다른 형태로 변경될 수 있다.

[44]

[45] 최근에는, NFV-based security function을 위한 기본 표준 인터페이스가 I2NSF(Interface to Network Security Functions) 워킹 그룹에 의해 개발되고 있다. 이는 인터넷 엔지니어링 태스크 포스(IETF: Internet Engineering Task Force)로 불리는 국제 인터넷 표준 기구의 일부이다.

[46] I2NSF의 목적은 다수의 보안 솔루션 벤더(security solution vendor)들에 의해 제공되는 이종의(heterogeneous) 네트워크 보안 기능(들)(NSF: network security function)을 위한 표준화된 인터페이스를 정의하기 위함이다.

[47] I2NSF 아키텍처(architecture)에서, NSF(들)의 관리에 대하여 상세히 고려할 필요 없이(NSF의 관리는 결국 보안 정책의 시행(enforce)을 요구한다), 사용자는 사용자의 네트워크 시스템 내 네트워크 자원을 보호하기 위한 보호 정책을 정의할 수 있다. 또한, 다수의 vendor들로부터 NSF(들)로의 표준화된 인터페이스는 이종의 NSF(들)에 대한 태스크(task)의 설정 및 관리를 단순화할 수 있다.

[48] 최근 들어 더 정교한(sophisticated) 네트워크 공격에 효과적으로 대처하기 위해서는 다양한 네트워크 보안 기능(들)(NSF: Network Security Functions)(또는 보안 기능(들)(security functions))이 협력하여(cooperatively) 네트워크 트래픽에 대한 복합적인 분석을 수행할 필요가 있다. 또한, 네트워크 트래픽의 특성과 의심되는 수준(suspiciousness level)에 따라 다양한 타입의 네트워크 트래픽이 서로 다른 NSF들의 세트를 통해 분석될 필요가 있다.

[49] NSF가 자체 분석 결과를 기반으로 다른 NSF를 호출함으로써 NSF가 추가 검사(inspection)를 트리거 할 수 있게 해주는 정보 모델(IM: Information Model)이 네트워크 보안 기능(들)로의 인터페이스(I2NSF: Interface to Network Security Functions) 프레임워크(framework) 내 NSF 향한 인터페이스(NFI: NSF-Facing Interface)를 위해 제안되었다.

[50] 그러나, I2NSF framework의 현재 설계는 다중 NSF를 통한

연속적인(consecutive) 검사를 가능하게 하기 위해 네트워크 트래픽 스티어링(network traffic steering)을 완전히 고려하지 않는 단점이 있다.

[51] 이에 따라, 본 발명에서는 NSF를 통한 traffic steering을 위한 추가 구성 요소를 I2NSF 프레임 워크(framework)에 통합하는 아키텍처를 제안한다.

[52] 특히, 본 발명에서는, NSF에 의해 트리거된(또는 NSF-트리거된)(NSF-triggered) traffic steering의 상위-레벨 정책(high-level policy)을 낮은 수준의 정책으로 해석(interpret)/변환하고 관리할 수 있도록, 보안 컨트롤러(security controller)의 기능을 확장하는 방법을 제안한다.

[53] 또한, 본 발명에 따르면, 사용 가능한 NSF 인스턴스(들)(instance) 및 NSF 인스턴스(들)의 정보(예를 들어, 네트워크 정보 및 작업로드(workload))를 추적하고, 주어진 보안 기능을 위해 사용할 NSF 인스턴스를 결정할 수 있다.

[54] 또한, 본 발명에 따르면, Security Controller에 의해 제공되어 전달되는 정보에 기반하여, 네트워크 보안 기능 전달자(NSFF: Network Security Function Forwarder)는 요구되는 NSF(들)을 통해 네트워크 traffic steering을 수행할 수 있다.

[55] 또한, 본 발명에 따르면, NSFF는 NSF로부터의 검사 결과를 해석하여 진보된 검사(advanced inspection)를 시행할 수 있다.

[56] 또한, 본 발명에 따르면, 보안 검사 결과 및 advanced inspection 요청을 특정하기 위한 추가적인 패킷 헤더(packet header) 포맷이 정의될 수 있다.

[57] 본 발명은 크게 다음과 같은 효과를 가진다.

[58] - 연속적인(consecutive) 검사를 위한 정책 설정: 본 발명에 따른 NSF-triggered traffic steering 아키텍처(architecture)는 NSF 트리거링(triggering)을 위한 정책 설정/관리를 허용한다. 트리거링 정책(triggering policy)에 기반하여, 관련된 네트워크 트래픽은 다양한 NSF(들)을 통해 복합적으로, 협업 방식으로 분석될 수 있다.

[59] - 연속적인 검사를 위한 network traffic steering: 본 발명에 따른 NSF-triggered traffic steering architecture에서는, 트리거링 정책에 기반하여 network traffic이 복수의 요구되는 NSF(들)을 통해 스티어링될 수 있다. 또한, NSF 향한 인터페이스(NFI: NSF facing interface)를 위한 I2NSF 정보 모델(IM)은 NSF가 자신의 검사 결과에 기반하여 추가의 검사를 위해 다른 NSF를 호출하도록 요구한다. 이러한 요구 사항을 만족하기 위하여, 본 발명에 따른 NSF-triggered traffic steering architecture에서는, 하나의 NSF로부터 또 다른 NSF로의 traffic 전달(forwarding)될 수 있다.

[60] - NSF 인스턴스(instance) 간의 로드 밸런싱(load balancing): 본 발명에 따른 NSF-triggered traffic steering architecture는 유연한 traffic steering 메커니즘을 활용(leveraging)함으로써 이용 가능한 NSF instance들에 유입되는 traffic의 load balancing을 제공한다. 이러한 목적을 위해, NSF에게 보안 기능에 대한 과도한 요청이 있을 때, NSF의 동적 인스턴스화(instantiation)를 수행(즉, 해당 보안

기능을 수행할 수 있는 새로운 NSF를 생성)할 수 있다.

[61]

[62] 본 문서에서 사용될 수 있는 용어(terminology)들은 다음과 같이 정의된다.

[63] - 네트워크 보안 기능(NSF: Network Security Function): 수신된 패킷(packet)의 특정 취급을 담당하는 기능을 담당하는 장치를 의미한다. NSF는 다양한 프로토콜 스택(stack)의 다양한 계층(예를 들어, 네트워크 계층 또는 다른 OSI(Open System Interconnection) 계층 등)에서 동작할 수 있다.

[64] 예를 들어, 네트워크 보안 서비스 기능 타입의 일례로서, 방화벽(firewall), 침입 방지 시스템(IPS: Intrusion Prevention System)/침입 탐지 시스템(IDS: Intrusion Detection System), 강한 패킷 검사(DPI: Deep Packet Inspection), 애플리케이션 가시성 및 제어(AVC: Application Visibility and Control), 네트워크 바이러스 및 악성 코드 스캐닝, 샌드박스(sandbox), 데이터 손실 방지(DLP: Data Loss Prevention), 분산 서비스 거부(DDoS: Distribute Denial of Service), 전송 계층 보안(TLS: Transport Layer Security) 프록시, 안티스푸핑(Anti-Spoofing) 등이 포함될 수 있다. 본 발명에 따른 NSF는 상술한 예시 중 어느 하나로 구현될 수 있으며, 다양한 타입의 NSF가 이용될 수 있다. 또한, 동일한 타입의 NSF가 다수로 구현될 수도 있다. 또한, 본 발명에 따른 NSF는 상술한 예시 중 어느 하나 이상이 결합되어 구현될 수도 있다.

[65] - 진보된 검사/동작(Advanced Inspection/Action): NFI(NSF-facing interface)를 위한 I2NSF 정보 모델(IM)과 같이, Advanced Inspection/Action은 NSF가 자신의 검사 결과에 기반하여 또 다른 NSF에게 추가적인 검사를 위한 호출을 의미한다.

[66] - 네트워크 보안 기능 프로파일(NSF Profile): NSF Profile은 NSF의 보안 검사 능력을 나타낸다. 각 NSF는 자신이 제공하는 보안 서비스의 타입, 자신의 자원 능력 등을 특정하기 위하여 자신의 NSF Profile을 가질 수 있다.

[67] - 네트워크 보안 기능 운영 관리자(NSF Operation Manager): NSF Operation Manager는 지속적으로 NSF instance의 정보 및 상태를 관리하고, advanced inspection 요청을 지원하기 위하여 NSF 네트워크 액세스 정보(network access information)을 제공하는 장치를 의미한다. 예를 들어, NSF instance의 정보는 지원되는 전송 프로토콜(transport protocol), IP(Internet Protocol) 주소, NSF instance을 위한 위치를 포함할 수 있다. 또한, NSF Operation Manager는 개발자의 관리 시스템(Developer's Management System)과의 협의 그리고 전체 NSF instance들에 대한 load balancing에 의해 NSF instance의 풀(pool)의 동적인 관리를 담당한다.

[68] - 패킷 전달 헤더/인캡슐레이션(Packet Forwarding Header/Encapsulation): Packet Forwarding Header는 추가 검사를 위해 하나의 NSF로부터 또 다른 NSF로의 packet을 전달하기 위하여 사용된다. 전자의 NSF(즉, 소스 NSF)는 후자의 NSF(즉, 타겟 NSF)의 NSF 프로파일로 Packet Forwarding Header을 구성(construct)하고, NSFF에게 해당 packet을 전달한다. 요구되는 필드는 동작

코드(action code), 메타데이터(metadata)의 수, 메타데이터(metadata)를 포함할 수 있다. 이때, metadata는 NSF profile의 일부 또는 전체를 포함할 수 있으며, 후술하는 Packet Forwarding Header에서 Spec info 필드로 지칭될 수 있다.

[69] - 네트워크 보안 기능 전달자(NSFF: Network Security Function Forwarder)(또는 보안 기능 전달자(SFF: Security Function Forwarder)): traffic이 NSF로부터 전달될 때, NSFF는 packet forwarding encapsulation 내에서 전달된 정보에 따라 하나 이상의 연결된 NSF에게 traffic을 전달하는 장치를 의미한다. 따라서, NSFF는 traffic을 또 다른 NSFF(동일한 또는 다른 타입의 오버레이(overlay))에게 전달하고, overlay 검사를 종료할 수 있다.

[70]

[71] 이하, 본 발명에서 제안하는 NSF-triggered traffic steering architecture 및 traffic steering의 기본 동작에 대하여 살펴본다. 또한, architecture의 각 구성 요소에 대하여 상세히 살펴본다.

[72] 도 1은 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템의 구성을 예시한다.

[73] 도 1을 참조하면, 본 발명에 따른 NSF-triggered traffic steering architecture는 I2NSF 사용자(user)(또는 사용자 장치), 네트워크 운영자 관리 보안 컨트롤러(Network Operator Management Security Controller, 간단히 보안 컨트롤러(Security Controller)로 지칭될 수 있음), 벤더의 관리 시스템(VMS: Vendor's Management System), NSF(또는 NSF 장치) 및 NSF 전달자(NSFF: NSF Forwarder)(또는 NSFF 장치)로 구성될 수 있다. 또한, Network Operator Management Security Controller는 NSF 운영 관리자(NSF Operation Manager)(또는 NSF Operation Manager 장치)를 포함할 수 있다.

[74] 도 1에 따른 architecture는 전송중인 packet의 복합 검사(composite inspection)를 지원한다. Packet Forwarding Header에 저장된 각 NSF의 검사 결과에 따라, traffic packet은 상세한 분석을 위해 또 다른 NSF로 스티어링될 수 있다.

[75] 기존의 I2NSF 프레임 워크의 구성 요소인 I2NSF 사용자(I2NSF User)(또는 I2NSF 클라이언트)로부터 상위-레벨(high-level) 진보된 검사에 대한 정책 및 설정을 반영할 수 있다.

[76] 또한, 본 발명에서 제안되는 architecture는 load balancing, 자동으로 추가적인(supplementary) NSF instance 생성 및 사용되지 않는 NSF instance 제거 기능을 제공할 수 있다.

[77] 이러한 설계 목적을 달성하기 위해 기존의 I2NSF 프레임 워크에 여러 구성 요소를 통합할 수 있다.

[78] 이하, 각 구성 요소에 대하여 살펴본다.

[79] - I2NSF User: I2NSF user는 네트워크 운영자의 기반시설(infrastructure)을 통해 네트워크 서비스를 수신하는 기업 네트워크(enterprise network)의 관리자(administrator)(또는 관리자 장치)를 나타낸다.

[80] I2NSF user는 또한 다양한 악의적인(malicious) 공격으로부터 enterprise network 트래픽(traffic)을 보호하기 위하여 네트워크 보안 서비스(network security service)를 이용할 필요가 있다. security service를 요청하기 위하여, I2NSF user는 자신이 원하는 security service의 상위-레벨(high-level) 보안 정책(security policy)을 특정(specify)하고, Security Controller에게 high-level security policy을 알릴 수 있다.

[81] high-level security policy를 준비하는 과정에서, I2NSF user는 각 NSF(들)를 위한 security service 또는 보안 정책 규칙 설정(security policy rule configuration)을 실현하기 위하여 요구되는 NSF(들)의 타입에 대하여 고려하지 않을 수 있다.

[82] 또한, I2NSF user는 Security Controller에 의해 기본적인(underlying) NSF(들) 내에서 발생되는 보안 이벤트(들)(security event)를 통지 받을 수 있다. 이들의 security event(들)을 분석함으로써, I2NSF user는 새로운 공격을 식별하고, 새로운 공격에 대처하기 위한 high-level security policy를 업데이트(또는 생성)할 수 있다.

[83] - Network Operator Management Security Controller(Security Controller): Security Controller는 네트워크 운영자에 의해 관리된다.

[84] Security Controller의 주요한 역할 중 하나는 I2NSF user로부터의 high-level 보안 정책(또는 정책 규칙)을 특정 NSF(들)을 위한 하위-레벨(low-level) 보안 정책 규칙으로 변환(translate)하는 것이다. Security Controller가 high-level 보안 정책을 I2NSF user로부터 수신한 후, Security Controller는 우선 I2NSF user에 의해 요구되는 정책을 시행하기 위하여 요구되는 NSF(들)의 타입을 결정할 수 있다. 그리고, Security Controller는 요구되는 각 NSF(들)을 위한 low-level 보안 정책을 생성할 수 있다. 결국, Security Controller는 생성된 low-level 보안 정책을 각 NSF(들)에게 설정할 수 있다.

[85] 또한, Security Controller는 시스템 내 구동 중인 NSF(들)을 모니터링하고, 각 NSF(들)에 대한 다양한 정보(예를 들어, 네트워크 액세스(access) 정보 및 작업로드(workload) 상태 등)를 유지할 수 있다. 또한, Security Controller는 Vendor's Management System의 도움을 받아 NSF 인스턴스의 동적인 수명시간(life-cycle) 관리를 통해 NSF 인스턴스(instance)의 풀(pool)을 동적으로 관리할 수 있다.

[86] - NSF 운영 관리자(NSF Operation Manager)

[87] NSF Operation Manager는 다음 3 가지의 동작을 담당한다.

[88] i) IP(Internet Protocol) 주소, 지원되는 전송 프로토콜(transport protocol), NSF profile, 로드 상태와 같이 사용 가능한 모든 NSF instance의 정보를 유지

[89] ii) 주어진 NSF profile과 관련된 진보된 검사(advanced inspection) 수행을 돕기 위하여 NSFF로부터 수신된 사용 가능한 NSF instance의 쿼리(query)에 대한 응답

[90] iii) 자원 낭비를 피하기 위한 기존 NSF instance의 제거 또는 서비스 혼잡을 피하기 위한 추가의(supplementary) NSF instance의 인스턴스화(instantiation)를 위하여 개발자의 관리 시스템(Developer’s Management System)으로의 요청

[91] 도 1에서 예시된 바와 같이, NSF Operation Manager는 Security Controller의 하위 모듈에 해당한다.

[92] 보다 구체적으로 살펴보면, 새로운 NSF instance가 등록될 때마다, Developer's Management System은 등록된 NSF instance의 정보를 NSF Operation Manager로 전달할 수 있다. 이에 따라, NSF Operation Manager는 사용 가능한 모든 NSF instance의 정보 리스트를 유지할 수 있다.

[93] 또한, NSF Operation Manger는 NSFF로부터 advanced inspection을 위한 NSF profile(즉, 보안 능력 정보)을 포함하는 요청 packet(예를 들어, NSF 생성 요청 패킷)을 수신할 수 있다. NSF Operation Manger가 NSFF로부터 특정 NSF profile의 query를 수신하면, NSF Operation Manger는 해당 NSF profile을 적용 가능한 모든 이용 가능한 NSF instance를 검색할 수 있다. 그리고, NSF의 위치 및 트래픽 로드 상태와 같은 선택 기준을 이용하여 최적(best)의 instance를 찾을 수 있다. 그리고, 검색 결과(즉, 최적의 instance)를 NSFF에게 반환할 수 있다.

[94] 또한, 각 NSF instance는 주기적으로 자신의 로드 상태를 NSF Operation Manger에게 보고할 수 있다. 이러한 보고에 기초하여, NSF Operation Manger는 NSF instance의 정보를 업데이트할 수 있다. 또한, NSF instance의 추가적인 인스턴스화(instantiation)(즉, 추가의 NSF instance 생생) 또는 NSF instance의 제거(elimination/destruct)를 위해 Developer’s Management System에게 요청함으로써 NSF instance의 pool을 관리할 수 있다. 결과적으로, NSF Operation Manger는 혼잡 및 자원 낭비를 방지함으로써 효율적인 자원 활용을 가능하게 한다.

[95] - 개발자의 관리 시스템(Developer’s Management System)

[96] Developer’s Management System은 벤더의 관리 시스템(Vendor's Management System)으로 지칭될 수도 있다. Developer’s Management System은 네트워크 운영자에게 NSF(들)을 제공하는 제3자(third-party) 보안 벤더에 의해 관리될 수 있다. 다양한 보안 벤더의 다수의 Developer’s Management System(들)이 존재할 수 있다.

[97] 본 발명에 따르면, 다음과 같이 추가 기능을 위해 Developer’s Management System이 확장될 수 있다.

[98] 상술한 바와 같이, NSF Operation Manager의 요청에 기반하여, Developer’s Management System는 새로운 NSF 인스턴스(들)을 생성하거나 또는 더 이상 사용되지 않는 기존의 NSF 인스턴스(들)을 제거(eliminate/destruct)할 수 있다.

[99] 다시 말해, NSF Operation Manager는 NSF의 기존 instance가 혼잡하면 추가적인 NSF instance를 생성하기 위해 Developer’s Management System에게 요청할 수 있다. 반면에 특정 NSF에 대한 instance의 수가 너무 많으면, NSF Operation Manager는 Developer’s Management System에게 NSF instance들 중 일부를 제거하도록 요청할 수 있다.

[100] 이러한 요청에 대한 응답으로 Developer's Management System은 NSF instance를

생성 및/또는 제거할 수 있다. 그리고, 새로운 NSF instance를 생성하거나 기존 NSF instance를 제거한 후에 Developer's Management System은 변경 사항을 NSF Operation Manager에 통보할 수 있다.

[101] - NSF 및 NSF Forwarder(NSFF):

[102] NSF(예를 들어, firewall, DPI, 서비스 거부 공격 중재자(Dos(Denial of Service) attack mitigator) 등)는 Security Controller로부터 수신한 보안 정책 규칙에 따라 network traffic의 보안 검사를 수행한다.

[103] 특히, 본 발명에 따른 architecture 내 NSF는 자신의 보안 검사 결과에 기반하여 서로 다른 NSF 타입으로 진보된 보안 검사(advanced security inspection)(예를 들어, DPI 및 분산 서비스 거부 공격 중재자(DDoS(Distribute Denial of Service) attack mitigator)를 트리거(trigger)할 수 있다. 예를 들어, firewall은 DPI를 이용한 suspicious traffic의 추가적인 검사를 트리거할 수 있다.

[104] 이 경우, 그러한 진보되고 복합적인 검사(composite inspection)를 실현하기 위하여, NSFF는 현재 NSF로부터 다음의(successor) NSF로의 suspicious traffic의 전달을 수행할 수 있다.

[105] 도 1에서는 NSFF가 Security Controller 및 NSF와는 별도의 구성 요소로 도시하고 있으나, 본 발명이 이에 한정되는 것은 아니다. 즉, NSFF는 Security Controller 또는 NSF 중에 어느 것에도 포함(즉, 하나의 장치로 함께 구현)될 수 있는 논리적인 구성 요소이다.

[106] 다음으로, 도 1에 예시된 architecture의 인터페이스에 대하여 살펴본다.

[107] - 소비자를 향한 인터페이스(CFI: Consumer-Facing Interface): 도 1에서 볼 수 있듯이, CFI는 I2NSF user와 Security Controller 사이에 위치하고, CFI는 사용자의 I2NSF 시스템으로의 인터페이스이다. 이렇게 설계됨으로써, 하위(underlying) NSF(들)의 상세한 내용을 숨기고, 사용자에게 NSF(들)의 추상적인 시각(abstract view)만을 제공한다.

[108] 이 인터페이스의 주요한 목적은 사용자가 I2NSF 시스템에게 보안 서비스를 요청할 수 있도록 허용하기 위함이다. 또한, Security Controller가 하위(underlying) NSF(들)로부터 수신한 보안 경보(alert)를 이 CFI를 통해 사용자에게 전달하기 위함이다. 수신한 경보를 분석함으로써, 사용자는 새로운 공격을 식별하고, 새로운 공격에 대처하기 위한 high-level security policy를 업데이트(또는 생성)할 수 있다.

[109] - NSF를 향한 인터페이스(NFI: NSF-Facing Interface): NFI는 NSFF(들)과 Security Controller 사이 및/또는 NSF(들)과 Security Controller 사이에 위치한다.

[110] NFI의 주요한 목적은 NSF(들)로부터 보안 관리 기법을 분리(decouple)함으로써 다양한 보안 솔루션 벤더들의 NSF(들)을 제어하고 관리하기 위한 표준화된 인터페이스를 제공하기 위함이다. NFI는 NSF(들)의 상세한 내용(예를 들어, 벤더, 유형 인자(form factor) 등)과 독립된다. 따라서, security policy rule을 NSF에게 설정할 때, Security Controller는 벤더 특정한 차이 및/또는 NSF의 form

factor를 고려할 필요가 없다.

[111] 기본적으로, NFI 인터페이스를 통해, Security Controller는 I2NSF user에 의한 high-level security policy를 시행하기 위하여 플로우 기반(flow-based) security policy를 각 타겟 NSF에게 전달할 수 있다. 원격 유지(maintenance)의 목적으로, Security Controller는 NFI 인터페이스를 통해 NSF(들)에게 제어 명령을 트리거할 수 있다.

[112] 각 NSF는 또한 Security Controller에게 현재 상태(예를 들어, workload 레벨, 혼잡(congestion) 등)를 주기적으로 알리기 위하여 NFI 인터페이스를 사용할 수 있다. 또한, 보안 이벤트/경보가 NSF 상에 발생할 때마다, NSF는 NFI 인터페이스를 통해 Security Controller에게 이를 보고할 수 있다.

[113] 각 NSFF는 Security Controller로부터 NFI 인터페이스를 통해 시스템 내 구동 중인 NSF의 전달 정보(forwarding information)를 수신할 수 있다. 이때, NSFF가 주어진 traffic을 전달하기 위한 forwarding information를 가지고 있지 않은 경우, NSFF는 NFI 인터페이스를 통해 Security Controller에게 정보의 쿼리(query)를 전송할 수 있다.

[114] - 등록 인터페이스(RI: Registration Interface): 도 1에서 볼 수 있듯이, RI는 Security Controller와 Developer's Management System 사이에 위치한다. RI의 주요한 목적은 NSF instance의 동적인 life-cycle 관리 및 시스템 상에 새로운 NSF instance의 등록을 수행하기 위함이다.

[115] 새로운 NSF가 시스템 내 요구되면, Security Controller는 새로운 NSF 생성을 Developer's Management System에게 요청할 수 있다. 이때, Security Controller의 요청은 요청된 NSF instance의 프로파일(profile)을 포함하고, 이 profile은 NSF instance에 의해 제공되어야 하는 보안 능력(security capability) 및 서비스 능력(service capacity)을 특정할 수 있다.

[116] 이 요청이 수신되면, Developer's Management System은 요청된 NSF profile을 만족하는 새로운 NSF instance를 생성하고, Security Controller에게 이 새로운 NSF instance의 네트워크 액세스 정보(network access information)(예를 들어, IP(Internet Protocol) 주소, 포트 넘버(port number) 등)를 알릴 수 있다. 네트워크 액세스 정보는 시스템 내 새로운 NSF instance의 고유한 식별자로서 사용될 수 있다.

[117] 반면, Security Controller가 특정한 기존의 NSF instance가 더 이상 필요하지 않다고 결정하면, Security Controller는 Developer's Management System에게 해당 NSF instance를 제거(destruct)하라고 요청할 수 있다. 이 제거 요청(destruction request)는 제거될 NSF instance의 고유한 식별자를 포함할 수 있다.

[118]

[119] 이하, NSF에 의해 트리거된 트래픽 스티어링(NSF-Triggered Traffic Steering)에 대하여 살펴본다.

[120] 도 2는 기존의 서비스 기능 체인 아키텍처를 예시한다.

[121] 서비스 기능 체인/체이닝(SFC: Service Function Chain/Chaining)은 다수의 서비스 기능(예를 들어, NSF)을 통해 traffic을 steering함으로써 이를 가능하게 하는 기술에 해당한다.

[122] (1 단계) 트래픽(즉, packet)에 대한 SFC 설정 및 관리(SFC configuration & management)가 미리 정의된다.

[123] (2 단계) I2NSF 아키텍처 내 유입된 트래픽(즉, packet)은 미리 정의된 SFC 설정 및 관리(SFC configuration & management)를 이용하여 해당 트래픽을 최초로 분류한다. 즉, 해당 트래픽이 어떠한 NSF을 통해 검사되는지에 대한 서비스 기능 경로(SFP: Service Function Path)를 결정한다. 도 2에서는 해당 트래픽이 NSF1을 통해 검사되고, 이어 NSF2를 통해 검사되는 SFP가 결정되었다고 가정한다.

[124] (3 단계) 트래픽은 결정된 SFP에 통해 트래픽 스티어링된다. 즉, 트래픽은 결정된 SFP에 따라 서비스 기능 전달자(SFF: Service Function Forwarder)를 경유하여 NSF1에게 전달된다.

[125] (4 단계) NSF1에 의해 검사가 수행된 후, 해당 트래픽은 SFF를 경유하여 NSF2에게 전달된다. 이때, 해당 트래픽에 대하여 결정된 SFP도 함께 전달된다.

[126] 이와 같이, 트래픽이 I2NSF 아키텍처 내 유입되면, 미리 정해진 미리 정의된 SFC 설정 및 관리(SFC configuration & management)에 따라 해당 트래픽에 대한 SFP가 결정된다.

[127] 반면, 본 발명에 따른 I2NSF architecture 내에서는 트래픽의 검사 경로(즉, NSF의 경로)가 미리 정해지지 않고, 동적으로 결정된다.

[128]

[129] 도 3은 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 NSF 능력에 대한 정보 모델을 예시하는 도면이다.

[130] 본 발명에 따른 I2NSF architecture 내 NSF는 자신의 보안 검사 결과에 기반하여 서로 다른 NSF 타입으로 진보된 보안 검사(advanced security action)(즉, advanced security inspection)(예를 들어, DPI 및 DDoS attack mitigation)을 트리거할 수 있다. 예를 들어, firewall은 DPI를 이용하여 suspicious packet의 추가적인 검사를 트리거할 수 있다.

[131] 즉, 도 3과 같이, NSF는 자신의 보안 검사 결과에 기반하여 동적으로 전달자(FW: Forwarder)를 통해 DPI와 DDos Mitigator 중에 어떠한 진보된 보안 동작(advanced security action)이 다음에 수행되어야 할지를 결정할 수 있다.

[132]

[133] 이하, 표준화된 인터페이스를 위한 정보 모델(IM: Information Model) 및 데이터 모델(DM: Data Model)과, IM 및 DM을 정의함으로써 다양한 NSF(들)로의 표준화된 인터페이스를 셋업(set up)하는 절차에 대하여 살펴본다.

[134] 도 4는 본 발명의 일 실시예에 따른 패킷 필터링 능력을 가지는 NSF(들)을 위한 정보 모델(IM)을 예시한다.

[135] I2NSF에서는 다양한 보안 솔루션 벤더의 NSF(들)로의 표준화된 인터페이스를 셋업하기 위하여 정보 모델(IM) 및 데이터 모델(DM)이 정의될 수 있다.

[136] I2NSF 시스템 내에서, 다양한 NSF(들)은 security capability에 따라 하나 이상의 카테고리로 분류될 수 있다. IM은 NSF(들)의 각 카테고리 별로 정의될 수 있다. IM의 주요 목적은 동일한 카테고리 내 NSF(들)을 위한 security policy rule을 표현(represent)하기 위하여 종합적인(comprehensive) 모델을 정의하기 위함이다. 이러한 목적을 위해, 도 4의 예시와 같이, IM은 이벤트-조건-동작(ECA: Event-Condition-Action) 규칙의 개념에 기반하여 모든 요구되는 데이터 아이템을 정의하고, 계층적인 구조로 데이터 아이템을 특징에 따라 분류할 수 있다.

[137] 다음 단계로 IM 내 정의된 콘텐츠(content)가 실제 구현되고, 구현된 결과는 데이터 모델(DM)으로 지칭된다. 예를 들어, DM 구현을 위해 YANG(Yet Another Next Generation) 데이터 모델링 언어가 사용될 수 있다.

[138] DM이 구현된 후, 각 관련된 NSF는 구현된 DM으로 사전-설정(pre-configure)될 수 있다.

[139] Security Controller가 새로운 security policy rule을 가지는 NSF를 설정할 필요가 있을 때, Security Controller는 해당 DM 내 특정된 포맷에 따라 security policy rule을 표현할 수 있다.

[140] 예를 들어, I2NSF는 security policy rule을 인코딩하기 위하여 XML(extensible markup language)를 사용할 수 있으며, XML로 인코딩된(XML-encoded) security policy rule은 네트워크 설정 프로토콜(NETCONF: Network Configuration Protocol)을 이용하여 NSF(들)에게 전달될 수 있다.

[141] XML로 인코딩된 security policy rule이 수신된 후, NSF는 이미 사전-설정되어 있는 매칭되는 DM을 기반으로 수신된 security policy rule을 디코딩하고, 수신된 security policy rule로부터 content를 추출할 수 있다. 결국, NSF는 자신의 policy rule table 내 수신한 content를 등록할 수 있다.

[142] CFI 및 RI를 표준화하기 위하여, IM 및 DM의 동일한 개념 및 절차가 적용될 수 있다.

[143]

[144] 결국, 본 발명에 따른 I2NSF architecture에서는 앞서 도 2에서 예시된 기존의 SFC 접근 방식과 비교하여 1 단계 내지 3 단계가 생략(skip)될 수 있다. 다시 말해, 트래픽(즉, packet)에 대한 SFC 설정 및 관리(SFC configuration & management)를 미리 정의하는 1 단계, I2NSF 아키텍처 내 유입된 트래픽(즉, packet)은 미리 정의된 SFC 설정 및 관리(SFC configuration & management)를 이용하여 해당 트래픽을 최초로 분류하는 2 단계 및 결정된 SFP에 통해 트래픽이 스티어링되는 3 단계가 생략될 수 있다.

[145] 즉, SFC 아키텍처에 친화적인 접근 방식은 기존의 표준이며, 정적인 서비스 기능 경로를 적용하기 위해 적합하다. 반면, I2NSF framework에 친화적인 본 발명의 제안은 NSF 경로 설정 및 관리가 미리 정의되지 않는다. 따라서,

분류기(classifier) 및 초기 분류(initial classification)가 요구되지 않는 장점이 있다. 또한, 재분류(re-classification)가 요구되지 않는 장점이 있다.

[146]

[147] 도 5는 본 발명의 일 실시예에 따른 트래픽 스티어링을 개념적으로 설명하기 위한 도면이다.

[148] 상술한 바와 같이, 본 발명에 따른 I2NSF architecture 내 NSF는 자신의 보안 검사 결과에 기반하여 서로 다른 NSF 타입으로 진보된 보안 동작(advanced security action)(예를 들어, DPI 및 DDoS attack mitigation)을 트리거할 수 있다. 도 5의 경우, I2NSF architecture 내 유입된 트래픽은 NSF1에 의해 검사되고, NSF1은 자신의 보안 검사 결과에 기반하여 NSF2의 보안 검사를 트리거할 수 있으며, NSF2는 자신의 보안 검사 결과에 기반하여 NSF3의 보안 검사를 트리거할 수 있으며, NSF3은 자신의 보안 검사 결과에 기반하여 NSF4의 보안 검사를 트리거할 수 있다.

[149] advanced security action을 트리거링할 때, 현재 NSF는 suspicious packet에 메타데이터(metadata)를 추가할 수 있으며, metadata는 advanced security action을 위해 요구되는 security capability를 기술한다. 그리고, 현재 NSF는 다음 NSF에게 전달하기 위하여 패킷을 NSFF에게 전달한다.

[150] NSFF는 하나의 NSF instance로부터 또 다른 NSF instance에게 packet을 전달하는 기능(즉, 트래픽 스티어링)을 수행한다.

[151] traffic forwarding/steering 작업을 위해, NSFF(또는 NSF Operation Manager)는 시스템 내 이용 가능한 NSF instance의 forwarding information 테이블(table)을 유지할 수 있다. 전달할 패킷을 수신한 후에, NSFF는 먼저 패킷에 추가된 metadata 내에서 특정된 요구된(required) security capability와 매칭되는 NSF instance를 위한 table을 탐색할 수 있다.

[152] NSFF는 packet을 전달하기 위한 다음 NSF instance가 어떤 NSF instance인지 Security Controller(또는 NSF operation manager)와 협의할 수 있다. 즉, NSFF가 어떠한 매칭되는 항목(entry)를 찾지 못하면, NSFF는 required security capability와 함께 NSF instance의 query를 Security Controller에게 전송할 수 있다.

[153] Security Controller(또는 NSF operation manager)는 또한 시스템 내 현재 구동 중인 모든 NSF instance(들)의 정보의 table(즉, NSF 정보 테이블)을 유지할 수 있다.

[154] 여기서, NSF instance의 정보는 NSF profile, 전달 정보(즉, IP 주소, VxLAN 등), NSF의 능력, NSF의 로드 상태 중 하나 이상을 포함할 수 있다.

[155] Security Controller(또는 NSF operation manager)가 NSFF로부터 query를 수신할 때, Security Controller(또는 NSF operation manager)는 문의된 security capability와 매칭되는 NSF instance를 위한 table을 탐색할 수 있다.

[156] Security Controller(또는 NSF operation manager)는 NSFF에게 선택된 NSF instance의 전달 정보를 제공할 수 있다. 다시 말해, Security Controller(또는 NSF

operation manager)가 매칭되는 NSF instance를 찾으면, Security Controller(또는 NSF operation manager)는 찾은 NSF instance의 forwarding information을 NSFF에게 응답한다.

[157] 그렇지 않으면, 시스템 내 required security capability를 가지는 기존의 NSF instance가 존재하지 않은 경우를 의미한다.

[158] 이 경우, Security Controller(또는 NSF operation manager)는 developer's management system에게 동적 인스턴스화(instantiation)(즉, NSF 생성) 또는 제거(elimination)을 요청한다. 다시 말해, Security Controller(또는 NSF operation manager)는 Developer's Management System에게 RI를 통해 required security capability로 새로운 NSF instance를 생성하도록 요청할 수 있다.

[159] Developer's Management System은 제3자(third party) 도메인(예를 들어, NSF 벤더(vendor)의 클라우드) 내 존재할 수 있다.

[160] Developer's Management System은 Security Controller의 요청에 기반하여 NSF instance를 생성할 수 있다. 이후에, Security Controller는 NSFF에게 생성된 NSF instance의 forwarding information를 알린다.

[161] 또한, Security Controller(또는 NSF operation manager)는 NSF instance의 현재 상태(즉, 로드가 가중되는지 혹은 사용되지 않는지)에 기반하여 Developer's Management System에게 NSF 인스턴스화(instantiation) 또는 제거(elimination)을 요청할 수 있다.

[162] 이 경우, Developer's Management System은 기존의 NSF instance가 혼잡될 때 추가의 NSF instance를 생성할 수 있으며, 또한, 사용되지 않은 하나 이상의 NSF instance를 제거할 수 있다.

[163] 결국, NSFF는 자신의 forwarding information table로부터의 또는 Security Controller로부터 수신한 forwarding information을 이용하여 타겟 NSF instance에게 패킷을 전달할 수 있다.

[164]

[165] 이하, 패킷 전달 헤더(Packet Forwarding Header)에 대하여 상세히 살펴본다.

[166] 도 6은 본 발명의 일 실시예에 따른 패킷 전달 헤더(Packet Forwarding Header)를 예시한다.

[167] Packet Forwarding Header는 NSFF에게 검사 결과와 필요한 검사를 전달하기 위해 사용되므로 도 6과 같이 필드의 길이가 가변적일 수 있다.

[168] Packet Forwarding Header는 고정된(fixed) 동작(Action) 또는 동작 코드(Action Code) 필드와 능력 정보의 수(SpecInfo Num) 필드, 그리고 가변적인(variable) 능력 정보(SpecInfo) 필드(들)을 포함할 수 있다.

[169] Action Code 필드는 packet에 대한 보안 검사 결과를 포함할 수 있다.

[170] packet의 보안 검사 결과 이상이 없어 목적지(destination)으로 전달하는 것을 허용하는 경우 "허용(allow)", packet의 보안 검사 결과 이상이 발견되어 packet을 목적지(destination)으로 전달하는 것을 허용하지 않는 경우 "거부(deny)",

packet의 보안 검사 결과 또 다른 NSF에 의해 추가 보안 검사가 요구되는 경우 "진보된(advanced)" 및 packet의 보안 검사 결과 목적지(destination)으로 전달하는 것을 허용하되 또 다른 NSF에 의해 추가 보안 검사가 요구되는 경우 "미러(mirror)" 중 하나의 값을 포함할 수 있다.

[171] SpecInfo Num 필드는 Packet Forwarding Header에 몇 개의 SpecInfo 필드(즉, 메타데이터)가 포함되는지 나타낸다.

[172] 각 SpecInfo 필드는 다음의 보안 검사를 위해 요구되는 보안 능력에 대한 정보를 포함할 수 있다. 즉, NSF profile의 일부를 포함할 수 있다. 복수의 SpecInfo 필드를 포함하는 Packet Forwarding Header가 패킷에 부착된 경우, NSFF를 통해 각 SpecInfo 필드 내 NSF의 서비스 프로파일에 매칭되는 복수의 NSF에게 패킷이 전달되어 추가 검사가 수행될 수 있다.

[173] 예를 들어, SepcInfo 필드는 NSF의 서비스 프로파일인 "SYN 플러드 완화(syn-flood-mitigate)", "UDP 플러드 완화(udp-flood-mitigate)" 등을 포함할 수 있다.

[174] SYN 플러드는 공격자가 합법적인 트래픽에 대해 시스템이 응답하지 않도록 충분한 서버 자원을 사용하기 위해 SYN 요청을 대상 시스템에 전송하는 DoS 공격의 하나의 형태이다. UDP 플러드 공격은 세션없는/연결없는 컴퓨터 네트워킹 프로토콜인 UDP(User Datagram Protocol)를 사용하는 DoS 공격의 하나의 형태이다.

[175]

[176] 이하, 네트워크 보안 기능 전달자(NSFF: Network Security Function Forwarder)(또는 보안 기능 전달자(SFF: Security Function Forwarder))에 대하여 보다 상세히 살펴본다.

[177] NSFF는 다음과 같은 두 가지 기능을 담당한다.

[178] - NSF 향한 인터페이스(NFI)를 위한 I2NSF 정보 모델에서 설명된 바와 같이, 초기에 유입된(incoming) traffic/packet을 Network Security 서브-모듈(Sub-Module)(즉, NSF)로 전달

[179] - Packet Forwarding Header에 지정된 NSF profile을 사용하여 일치하는 NSF로 traffic/packet을 전달

[180] NSFF는 게이트웨이 기능을 사용하여 유입되는(incoming) traffic/packet을 먼저 수신한다.

[181] 그리고, NSFF는 traffic/packet을 Network Security Sub-Module(즉, NSF)에게 전달하기 위하여 외부 인캡슐레이션(outer encapsulation)을 traffic/packet에 부착한다.

[182] 예를 들어, Network Security Sub-Module(즉, NSF)은 packet header 검사를 수행하는 방화벽에 해당될 수 있다.

[183] 이 Network Security Sub-Module은 outer encapsulation와 원본 패킷(origin packet) 사이에 Packet Forwarding Header를 부착한다.

[184] 그리고, packet이 진보된 검사를 위해 컨텐츠 보안 서브-모듈(Content Security Sub-Module) 또는 완화 서브-모듈(Mitigate Sub-Module)에게 전달될 수 있도록, Packet Forwarding Header 내 NSF profile을 특정한다.

[185] Network Security Sub-Module로부터 특정 NSF profile의 Packet Forwarding Header가 부착된 packet을 수신하면, NSFF는 NSF profile에 해당되는(즉, 매칭되는) 네트워크 보안 서비스를 제공하는 이용 가능한 NSF instance를 탐색한다. 그리고, NSFF는 찾은 NSF instance에게 packet을 전달한다.

[186] NSF가 packet이 또 다른 타입의 NSF를 통한 추가적인 검사가 요구된다고 결정하면, NSF는 진보된 NSF의 NSF profile로 특정된(즉, 포함하는) packet forwarding header를 구성(construct)하고, 헤더를 packet에 부착한다. 그리고, packet을 NSFF에게 전송한다.

[187] packet을 수신하면, NSFF는 packet forwarding header 내 특정된 NSF profile을 체크한다. 그리고, NSFF는 NSF Operation Manager와 협의함으로써 NSF profile와 매칭되는 NSF instance를 찾고, 해당 NSF instance에게 packet을 전달한다.

[188]

[189] 본 발명에 따른 NSF-triggered Traffic Steering Framework를 이용한 2가지의 실시예를 살펴본다.

[190] (1) 패킷 소스의 신뢰 레벨에 따른 서로 다른 NSF의 시행(Enforcing Different NSFs Depending on a Packet Source's Trust Level)

[191] 도 7은 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 트래픽의 흐름을 예시하는 도면이다.

[192] 본 발명에 따른 architecture에서, architecture로 유입된(incoming) 모든 packet은 최초로 NSFF에 도착한다.

[193] 현재 보안 정책이 모든 유입된(incoming) packet이 기본적으로 firewall에 의해 검사되도록 강제한다고 가정한다. 따라서, NSFF는 수신한 packet을 firewall instance에게 전달한다.

[194] firewall은 traffic의 소스(source)를 식별하고, source의 신뢰 레벨(trust level)을 평가할 수 있다.

[195] 예를 들어, 방화벽 필터(firewall filter)는 먼저 네트워크 패킷(network packet)을 안전한 패킷(secure packet), 위험한 패킷(dangerous packet) 및 의심스러운 패킷(suspicious packet)으로 분류할 수 있다. 상술한 바와 같이, source의 신뢰 레벨(trust level)을 평가함으로써 안전한 패킷(secure packet), 위험한 패킷(dangerous packet) 및 의심스러운 패킷(suspicious packet)으로 분류할 수 있다.

[196] 도 7(a)와 같이 만약, traffic이 신뢰되는 source로부터 수신된 경우(또는 안전한 패킷(secure packet)으로 분류된 경우), traffic은 추가의 세부적인 검사 없이 단순히 목적지(destination)에게 전달될 수 있다.

[197] 반면, 도 7(a)와 같이 traffic이 신뢰되지 않은 source로부터 수신된 경우(또는

의심스러운 패킷(suspicious packet)으로 분류된 경우), firewall은 DPI에 해당하는 NSF profile을 포함하는 packet forwarding header를 packet에 부착하고, NSFF에게 packet forwarding header가 부착된 packet을 반환할 수 있다.

[198] firewall로부터 packet forwarding header가 부착된 packet을 수신하면, NSFF는 해당 packet을 DPI instance에게 전달할 수 있다.

[199] DPI instance는 수신한 packet의 페이로드(payload)에 대하여 상세한 검사를 수행할 수 있다.

[200] 그리고, DPI instance에 의해 packet의 페이로드(payload)에 대하여 상세한 검사를 수행한 결과, 안전한 패킷(secure packet)으로 판정된 경우, 해당 packet은 NSFF를 경유하여 목적지(destination)로 전달될 수 있다.

[201] 이와 같이, suspicious packet만을 침입 탐지 시스템(intrusion detection system) 내 DPI 모듈로 검사할 수 있다.

[202] 이때, dangerous packet은 firewall filter에 의해 단순히 드랍(drop)(즉, 삭제)될 수도 있다. 이 방법은 이미 안전하거나 위험한 것으로 분류 된 패킷에 대한 불필요한 분석 작업을 방지함으로써 intrusion detection system의 성능을 향상시키는 데 도움이 될 수 있다.

[203] 도 7(a)에서는 추가적인 검사를 위한 NSF로서 DPI를 예시하고 있으나 이는 하나의 예시에 불과하며 본 발명이 이에 한정되는 것은 아니고 다른 NSF가 이용될 수도 있다.

[204] 한편, 의심스러운 패킷(suspicious packet)으로 분류할 때 소스의 신뢰도의 레벨의 고려하여 의심스러운 정도가 복수로 구분될 수도 있으며, 의심스러운 정도의 레벨에 따라 NSF에 의한 추가적인 검사의 정도/횟수가 정해질 수 있다. 이에 대하여 도 8을 참조하여 보다 상세히 살펴본다.

[205] 도 8은 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 트래픽의 흐름을 예시하는 도면이다.

[206] 도 8(a)를 참조하여 트래픽의 흐름을 살펴본다.

[207] (1 단계) I2NSF 시스템으로 유입된(incoming) 모든 packet은 최초로 NSFF에 도착한다.

[208] (2 단계) packet은 firewall instance에 의해 신뢰 레벨(trust level)이 평가될 수 있다.

[209] 2 단계에 대하여 보다 구체적으로 살펴보면, NSFF는 수신한 packet을 firewall instance에게 전달한다.

[210] firewall은 traffic의 소스(source)를 식별하고, source의 신뢰 레벨(trust level)을 평가할 수 있다.

[211] 예를 들어, 방화벽 필터(firewall filter)는 먼저 네트워크 패킷(network packet)을 안전한 패킷(secure packet), 위험한 패킷(dangerous packet) 및 의심스러운 패킷(suspicious packet)으로 분류할 수 있다. 상술한 바와 같이, source의 신뢰 레벨(trust level)을 평가함으로써 안전한 패킷(secure packet), 위험한

패킷(dangerous packet) 및 의심스러운 패킷(suspicious packet)으로 분류할 수 있다.

[212] 이때, 의심스러운 패킷(suspicious packet)으로 분류할 때 소스의 신뢰도의 레벨의 고려하여 의심스러운 정도가 복수로 구분될 수도 있다. 따라서, 의심스러운 정도의 레벨에 따라 NSF에 의한 추가적인 검사의 정도/횟수가 정해질 수 있다. 예를 들어, packet의 의심스러운 정도의 레벨이 2가지의 레벨로 구분되고, 그 의심스러운 정도의 정도가 클수록 레벨이 크게 정해진다고 가정한다. 이 경우, Firewall instance에 의한 packet의 분류 결과 packet의 의심스러운 정도의 레벨이 1 레벨인 경우, IDS/IPS에 의한 추가 검사가 진행될 수 있다.

[213] 해당 packet이 의심스러운 패킷(suspicious packet)으로 분류되고 그 레벨이 1인 경우, firewall은 IDS/IPS에 해당하는 NSF profile을 포함하는 packet forwarding header를 packet에 부착하고, NSFF에게 packet forwarding header가 부착된 packet을 반환할 수 있다.

[214] (3 단계) 다음으로, packet은 IDS/IPS에 의해 상세하게 검사될 수 있다.

[215] 3 단계에 대하여 보다 구체적으로 살펴보면, firewall로부터 packet forwarding header가 부착된 packet을 수신하면, NSFF는 해당 packet을 IDS/IPS instance에게 전달할 수 있다.

[216] IDS/IPS instance는 수신한 packet에 대하여 상세한 검사를 수행할 수 있다.

[217] 만약, IDS/IPS instance에 의해 packet에 대하여 상세한 검사를 수행한 결과, 안전한 패킷(secure packet) 판정된 경우, IDS/IPS instance는 packet을 NSFF에게 반환할 수 있다.

[218] 반면, IDS/IPS instance에 의해 packet에 대하여 상세한 검사를 수행한 결과, 안전한 패킷(secure packet)이 아니라고 판정된 경우, IDS/IPS instance는 packet을 드랍(drop)할 수 있다.

[219] (4 단계) IDS/IPS instance로부터 packet을 수신한 NSFF는 목적지(destination)로 packet을 전달할 수 있다.

[220] 도 8(b)를 참조하여 트래픽의 흐름을 살펴본다.

[221] (1 단계) I2NSF 시스템으로 유입된(incoming) 모든 packet은 최초로 NSFF에 도착한다.

[222] (2 단계) packet은 firewall instance에 의해 신뢰 레벨(trust level)이 평가될 수 있다.

[223] 2 단계에 대하여 보다 구체적으로 살펴보면, NSFF는 수신한 packet을 firewall instance에게 전달한다.

[224] firewall은 traffic의 소스(source)를 식별하고, source의 신뢰 레벨(trust level)을 평가할 수 있다.

[225] 예를 들어, 방화벽 필터(firewall filter)는 먼저 네트워크 패킷(network packet)을 안전한 패킷(secure packet), 위험한 패킷(dangerous packet) 및 의심스러운

패킷(suspicious packet)으로 분류할 수 있다. 상술한 바와 같이, source의 신뢰 레벨(trust level)을 평가함으로써 안전한 패킷(secure packet), 위험한 패킷(dangerous packet) 및 의심스러운 패킷(suspicious packet)으로 분류할 수 있다.

[226] 이때, 의심스러운 패킷(suspicious packet)으로 분류할 때 소스의 신뢰도의 레벨의 고려하여 의심스러운 정도가 복수로 구분될 수도 있다. 따라서, 의심스러운 정도의 레벨에 따라 NSF에 의한 추가적인 검사의 정도/횟수가 정해질 수 있다. 예를 들어, packet의 의심스러운 정도의 레벨이 2가지의 레벨로 구분되고, 그 의심스러운 정도의 정도가 클수록 레벨이 크게 정해진다고 가정한다. 이 경우, Firewall instance에 의한 packet의 분류 결과 의심스러운 정도의 레벨이 2 레벨인 경우, IDS/IPS, Anti-Spoofing, DPI에 의한 추가 검사가 진행될 수 있다.

[227] 해당 packet이 의심스러운 패킷(suspicious packet)으로 분류되고 그 레벨이 2인 경우, firewall은 IDS/IPS에 해당하는 NSF profile을 포함하는 packet forwarding header를 packet에 부착하고, NSFF에게 packet forwarding header가 부착된 packet을 반환할 수 있다.

[228] (3 단계) 다음으로, packet은 IDS/IPS에 의해 상세하게 검사될 수 있다.

[229] 3 단계에 대하여 보다 구체적으로 살펴보면, firewall로부터 packet forwarding header가 부착된 packet을 수신하면, NSFF는 해당 packet을 IDS/IPS instance에게 전달할 수 있다.

[230] IDS/IPS instance는 수신한 packet에 대하여 상세한 검사를 수행할 수 있다.

[231] 만약, IDS/IPS instance에 의해 packet에 대하여 상세한 검사를 수행한 결과, 안전한 패킷(secure packet)으로 판정된 경우, IDS/IPS instance는 패킷이 전달될 다음 NSF를 기술하기 위해 Anti-Spoofing에 해당하는 NSF profile을 포함하는 packet forwarding header를 packet에 부착하고, NSFF에게 packet forwarding header가 부착된 packet을 반환할 수 있다.

[232] 반면, IDS/IPS instance에 의해 packet에 대하여 상세한 검사가 수행된 결과, 안전한 패킷(secure packet)이 아니라고 판정된 경우, IDS/IPS instance는 packet을 드랍(drop)할 수 있다.

[233] (4 단계) 다음으로, packet은 Anti-Spoofing에 의해 상세하게 검사될 수 있다.

[234] 4 단계에 대하여 보다 구체적으로 살펴보면, IDS/IPS로부터 packet forwarding header가 부착된 packet을 수신하면, NSFF는 해당 packet을 Anti-Spoofing instance에게 전달할 수 있다.

[235] Anti-Spoofing instance는 수신한 packet에 대하여 상세한 검사를 수행할 수 있다.

[236] 만약, Anti-Spoofing instance에 의해 packet에 대하여 상세한 검사가 수행된 결과, 안전한 패킷(secure packet)으로 판정된 경우, Anti-Spoofing instance는 DPI에 해당하는 NSF profile을 포함하는 packet forwarding header를 packet에 부착하고, NSFF에게 packet forwarding header가 부착된 packet을 반환할 수 있다.

[237] 반면, Anti-Spoofing instance에 의해 packet에 대하여 상세한 검사를 수행한 결과, 안전한 패킷(secure packet)이 아니라고 판정된 경우, Anti-Spoofing instance는 packet을 드랍(drop)할 수 있다.

[238] (5 단계) 다음으로, packet은 DPI에 의해 상세하게 검사될 수 있다.

[239] 5 단계에 대하여 보다 구체적으로 살펴보면, Anti-Spoofing으로부터 packet forwarding header가 부착된 packet을 수신하면, NSFF는 해당 packet을 DPI instance에게 전달할 수 있다.

[240] DPI instance는 수신한 packet에 대하여 상세한 검사를 수행할 수 있다.

[241] 만약, DPI instance에 의해 packet에 대하여 상세한 검사가 수행된 결과, 안전한 패킷(secure packet) 판정된 경우, DPI instance는 packet을 NSFF에게 반환할 수 있다.

[242] 반면, DPI instance에 의해 packet에 대하여 상세한 검사를 수행한 결과, 안전한 패킷(secure packet)이 아니라고 판정된 경우, DPI instance는 packet을 드랍(drop)할 수 있다.

[243] (6 단계) DPI instance로부터 packet을 수신한 NSFF는 목적지(destination)에게 packet을 전달할 수 있다.

[244] (2) 동적 NSF 인스턴스화를 이용한 효과적인 로드 밸런싱(Effective Load Balancing with Dynamic NSF Instantiation)

[245] 도 9는 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 로드 밸런싱 방법을 예시하는 도면이다.

[246] 대규모의 네트워크 도메인(domain)에서, 일반적으로 다양한 보안 서비스를 제공하는 다수의 NSF instance가 존재한다. 이때, 특정 NSF instance가 자신의 능력을 벗어나 과도한 traffic 양을 겪을 수 있다. 이 경우, traffic의 일부를 또 다른 이용 가능한 동일 NSF의 instance에게 할당하는 것이 요구된다.

[247] 만약, 동일 NSF의 이용 가능한 추가의 instance가 없다면, 새로운 NSF instance를 생성하고, 새로운 instance에게 다음의 traffic이 향하도록 할 필요가 있다. 이렇게 함으로써, 서비스 혼잡을 방지하고, 더욱 효율적인 자원 활용을 달성할 수 있다.

[248] 이 프로세스는 공통적으로 load balancing으로 지칭될 수 있다.

[249] 본 발명에 따른 architecture에서, NSF Operation Manager는 이용 가능한 NSF instance의 트래픽 로드 상태를 주기적으로 모니터링할 수 있다.

[250] 또한, 본 발명에 따르면, Developer’s Management System을 통해 새로운 NSF instance가 동적으로 생성될 수 있다.

[251] 이러한 동적 NSF instance 생성이 traffic steering 메커니즘과 결합됨으로서 결국 load balancing 서비스를 제공할 수 있다.

[252] 이하, firewall instance에서 혼잡이 발생될 때, load balancing의 상세한 프로세스를 살펴본다.

[253] (1 단계) NSF Operation Manager는 현재 가용한 firewall instance가 너무 많은

요청을 수신하였음을 감지한다. 즉, firewall instance에 과도한 트래픽이 발생하였음을 감지한다.

[254] (2 단계) 현재, 추가로 이용 가능한 firewall instance가 없다고 가정한다.

[255] 추가로 이용 가능한 firewall instance가 없으므로, NSF Operation Manager가 Developer's Management System에게 동일한 보안 서비스를 제공할 수 있는 새로운 firewall instance의 생성을 요청한다.

[256] (3 단계) Developer's Management System은 새로운 firewall instance를 생성하고, 새로운 firewall instance의 정보를 NSF Operation Manager에게 등록한다.

[257] NSF Operation Manager는 새로운 firewall instance를 반영하여 NSF 정보 테이블(NSF information table)을 업데이트하고, NSF 및 NSFF에게 이러한 업데이트를 알린다.

[258] (4 단계) 새로운 전달 정보(forwarding information)에 따라, NSFF는 다음의 traffic을 새로운 firewall instance에게 전달한다. 결과적으로, 기존의 firewall instance의 부담을 효과적으로 완화시킬 수 있다.

[259]

[260] 이하, 본 발명에 따른 NSF-triggered Traffic Steering Framework를 활용한 예를 살펴본다.

[261] 이하, 2가지의 시나리오에 대하여 살펴본다.

[262] - 시간-종속적인 웹 액세스 필터링(Time-dependent Web Access Filtering)

[263] 이 시나리오에서, I2NSF 기반 기업(corporate) 네트워크 시스템을 가정하고, 기업(corporate) 관리자가 근무 시간 동안에 직원들이 소셜 네트워킹 사이트에 액세스하는 것을 방지하는 것을 원한다고 가정한다.

[264] 이 시나리오에서, 기업 네트워크 관리자는 I2NSF user에 해당한다. 그리고, I2NSF user는 먼저 근무 시간 동안 직원들의 소셜 네트워킹 사이트로의 액세스를 제한(block)하는 high-level security policy를 명시(특정)한다.

[265] 예를 들어, "오전 9시부터 오후 6시까지 직원들에 의한 소셜 네트워킹 사이트로의 모든 액세스를 차단"와 같이 high-level security policy가 특정될 수 있다.

[266] 관리자는 CFI를 통해 Security Controller에게 high-level security policy를 전달한다.

[267] high-level security policy가 수신될 때, Security Controller는 high-level security policy를 low-level security policy rule으로 변환한다. Security Controller는 먼저 기업 네트워크 시스템의 IP 주소 매핑의 데이터베이스를 액세스하여, 직원들에 의해 사용될 IP 주소들을 찾는다(figure out). 이 정보에 기반하여, Security Controller는 직원들의 IP 주소로부터 소셜 네트워킹 사이트로의 액세스를 제한하는 firewall rule을 생성한다. firewall rule은 또한 근무 시간에 대한 정보를 포함한다.

[268] Security Controller는 NFI를 통해 생성된 security policy rule를 firewall에

설정한다.

[269] 그리고, 직원이 근무 시간 동안에 그의 컴퓨터를 이용하여 소셜 네트워킹 사이트로 액세스를 시도하면, 액세스 요청 패킷(access request packet)은 firewall에게 전달된다.

[270] firewall은 패킷 헤더(packet header)를 검사하고, 해당 packet이 소셜 네트워킹 사이트로 전달될지 여부를 판단한다. 예를 들어, 소스/목적지 IP 주소를 이용하여 소셜 네트워킹 사이트로 전달될지 여부를 판단할 수 있다.

[271] 그리고, 현재 시간을 체크하여 근무 시간 내인지 여부를 판단한다. packet이 2가지의 조건에 만족하면, firewall은 소셜 네트워킹 사이트로의 액세스를 제한하기 위하여 해당 packet을 드랍(drop)한다.

[272]

[273] - suspicious VoIP(Voice over Internet Protocol)/VoLTE(Voice over Long Term Evolution) 패킷에 대한 선택적인 보안 검사

[274] 이 시나리오는 자신의 고객의 VoIP/VoLTE 호(call)를 위한 보안 서비스를 제공하길 원하는 이동 통신 서비스 제공자에 관한 것이다.

[275] 이 시나리오에서, 이동 통신 서비스 네트워크의 관리자가 자신의 고객의 VoIP/VoLTE 호(call)에 보안 서비스를 제공하길 원한다. 이 시나리오의 관리자는 I2NSF user에 해당한다. 그리고, I2NSF user는 도착하는(incoming) VoIP/VoLTE packet에 적용하길 원하는 high-level security policy rule을 명시(특정)한다.

[276] 예를 들어, "밤에 특이한(unusual) 국가로부터 개시된 VoIP/VoLTE call의 패킷에 대하여 보안 검사를 수행하여, 악의적인지(malicious) 여부를 판단하고, 검출된 malicious call는 관리자에게 보고한다"와 같이 high-level security policy가 특정될 수 있다. 관리자는 Security Controller에게 high-level security policy rule을 전송한다.

[277] 관리자로부터 high-level security policy rule을 수신할 때, Security Controller는 level security policy rule 내 국가 명칭을 해당 IP 주소 범위로 변환한다. 그리고, Security Controller는 call packet의 소스 주소(source address) 및 목적지 주소(destination address)를 체크함으로써 VoIP/VoLTE call이 의심스러운지 여부를 결정하기 위하여 firewall rule을 생성하고, 생성된 rule을 firewall instance에 설정한다.

[278] 또한, Security Controller는 malicious call에 해당하는 VoIP/VoLTE packet의 다양한 필드를 체크하기 위한 DPI rule을 생성하고, 그러한 rule을 DPI instance에 전송한다.

[279] 도 10 내지 도 13은 본 발명의 일 실시예에 따른 NSF에 의해 트리거된 트래픽 스티어링 프레임워크를 활용하여 유입되는 VoIP/VoLTE 패킷에 수행되는 단계별 절차를 예시한다.

[280] 도 10과 같이, VoIP/VoLTE packet이 모바일 서비스 제공자의 네트워크에 도착한 후, VoIP/VoLTE packet은 firewall에 전달되거나 또는 복사(mirror)된다.

Security Controller에 의해 설정된 rule에 기반하여, firewall은 이 트래픽이 unusual call 패턴에 해당하는지 여부를 결정한다.

[281] 이 트래픽이 unusual하고, suspicious하다면, firewall은 VoIP/VoLTE packet의 다양한 필드에 대한 더욱 상세한 보안 검사를 위한 DPI를 트리거한다.

[282] 예를 들어, NSFF 1은 패킷에 Packet Forwarding Header를 부착할 수 있다. Packet Forwarding Header는 T 필드(앞서 도 6에서 Action Code 필드), N 필드(SpecInfo Num 필드), Spec 필드(SpecInfo 0...n 필드)를 포함할 수 있다. 그리고, NSFF 1은 Packet Forwarding Header 내 T 필드의 값을 "진보된(advanced)" 및 "미러(mirror)" 중 하나로 셋팅할 수 있으며, Spec 필드는 추가로 검사되어야 할 NSF의 profile로 셋팅될 수 있다. 만약, T 필드가 "진보된(advanced)"으로 셋팅되고, Spec 필드가 DPI profile로 셋팅된 경우, 해당 트래픽 패킷은 NSFF를 경유하여 DPI로 전달될 수 있다.

[283] 만약, T 필드가 "미러(mirror)"로 셋팅되고, Spec 필드가 DPI profile로 셋팅된 경우, 도 11과 같이 유입된 패킷은 인트라넷(intranet)으로 전달되고, 미러링(복사)를 통해 복사된 패킷은 NSFF를 경유하여 DPI로 전달될 수 있다.

[284] 도 12와 같이, security policy rule table 내 VoIP/VoLTE packet의 rule에 기반하여, DPI는 수신한 VoIP/VoLTE packet의 다양한 필드를 체크하고, 이 call이 악의적(malicious)인지 여부를 결정한다. 그리고, DPI가 판단한 결과, malicious traffic packet 으로 결정한 경우, 해당 traffic packet을 드랍(drop)할 수 있다.

[285] 그리고, 도 13과 같이 call이 malicious하다면, DPI는 NFI 및 CFI를 통해 검출된 malicious 동작을 I2NSF user에게 통지할 수 있다. 즉, DPI는 NFI를 통해 malicious 동작을 NSF Operation Manager에게 통지하고, NSF Operation Manager는 CFI를 통해 malicious 동작을 I2NSF user에게 통지할 수 있다.

[286]

[287] 도 14는 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 방법을 예시한다.

[288] 도 14를 참조하면, NSF는 트래픽 스티어링(traffic steering)을 지원하는 시스템에 유입된 패킷에 대한 보안 검사를 수행한다(S1401).

[289] 이때, 시스템에 유입된 패킷은 NSFF에 의해 수신되고, NSFF에 의해 NSF에게 전달될 수 있다.

[290] 보안 검사의 결과에 기반하여, NSF는 또 다른 NSF에 의한 추가적인 검사가 필요한지 여부를 판단한다(S1402).

[291] NSF는 패킷의 소스(source)의 신뢰 레벨(trust level)에 따라 패킷을 안전한 패킷(secure packet), 위험한 패킷(dangerous packet) 및 의심스러운 패킷(suspicious packet)으로 분류할 수 있다.

[292] 패킷이 상기 안전한 패킷(secure packet)으로 분류된 경우 또 다른 NSF를 통해 추가의 보안 검사 없이 패킷의 목적지(destination)으로 전달될 수 있다. 또는 패킷이 상기 위험한 패킷(dangerous packet)으로 분류된 경우 패킷은 드랍(drop)될

수 있다. 또는 패킷이 상기 의심스러운 패킷(suspicious packet)으로 분류된 경우 패킷은 패킷 전달 헤더가 부착되어 NSFF에게 전달될 수 있다.

[293] 추가적인 검사가 필요하면, NSF는 추가적인 검사를 호출하기 위한 패킷 전달 헤더(packet forwarding header)를 패킷에 부착한다(S1403).

[294] 이때, 패킷 전달 헤더는 상기 추가적인 검사를 위해 요구되는 보안 능력에 대한 정보를 포함할 수 있다.

[295] 보다 구체적으로, 패킷 전달 헤더는 패킷의 보안 검사의 결과를 포함하는 동작 코드 필드, 추가적인 검사를 위해 요구되는 보안 능력 정보를 포함하는 능력 정보 필드, 능력 정보 필드의 개수를 나타내는 능력 정보의 수 필드를 포함할 수 있다.

[296] NSF는 패킷 전달 헤더가 부착된 패킷을 NSFF에게 전송한다(S1404).

[297]

[298] 도 15는 본 발명의 일 실시예에 따른 NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 장치의 블록 구성도를 예시한다.

[299] 도 15를 참조하면, NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 장치(1500)는 프로세서(processor, 1501), 메모리(memory, 1502) 및 통신 모듈(communication module, 1503)을 포함한다.

[300] NSF에 의해 트리거되는(NSF-triggered) 트래픽 스티어링(traffic steering) 시스템 내 장치(1500)는 앞서 설명한 NSF, NSFF, Security Controller, NSF Operation Manager, Developer's Management System, I2NSF user에 해당될 수 있다.

[301] 프로세서(1501)는 앞서 도 1 내지 도 14에서 제안된 기능, 과정 및/또는 방법을 구현한다. 메모리(1502)는 프로세서(1501)와 연결되어, 프로세서(1501)를 구동하기 위한 다양한 정보를 저장한다. 통신 모듈(1503)은 프로세서(1501)와 연결되어, 유/무선 신호를 송신 및/또는 수신한다.

[302] 메모리(1502)는 프로세서(1501) 내부 또는 외부에 있을 수 있고, 잘 알려진 다양한 수단으로 프로세서(1501)와 연결될 수 있다.

[303] 이상에서 설명된 실시예들은 본 발명의 구성요소들과 특징들이 소정 형태로 결합된 것들이다. 각 구성요소 또는 특징은 별도의 명시적 언급이 없는 한 선택적인 것으로 고려되어야 한다. 각 구성요소 또는 특징은 다른 구성요소나 특징과 결합되지 않은 형태로 실시될 수 있다. 또한, 일부 구성요소들 및/또는 특징들을 결합하여 본 발명의 실시예를 구성하는 것도 가능하다. 본 발명의 실시예들에서 설명되는 동작들의 순서는 변경될 수 있다. 어느 실시예의 일부 구성이나 특징은 다른 실시예에 포함될 수 있고, 또는 다른 실시예의 대응하는 구성 또는 특징과 교체될 수 있다. 특허청구범위에서 명시적인 인용 관계가 있지 않은 청구항들을 결합하여 실시예를 구성하거나 출원 후의 보정에 의해 새로운 청구항으로 포함시킬 수 있음은 자명하다.

[304] 본 발명에 따른 실시예는 다양한 수단, 예를 들어, 하드웨어, 펌웨어(firmware), 소프트웨어 또는 그것들의 결합 등에 의해 구현될 수 있다. 하드웨어에 의한

구현의 경우, 본 발명의 일 실시예는 하나 또는 그 이상의 ASICs(application specific integrated circuits), DSPs(digital signal processors), DSPDs(digital signal processing devices), PLDs(programmable logic devices), FPGAs(field programmable gate arrays), 프로세서, 콘트롤러, 마이크로 콘트롤러, 마이크로 프로세서 등에 의해 구현될 수 있다.

[305] 펌웨어나 소프트웨어에 의한 구현의 경우, 본 발명의 일 실시예는 이상에서 설명된 기능 또는 동작들을 수행하는 모듈, 절차, 함수 등의 형태로 구현될 수 있다. 소프트웨어 코드는 메모리에 저장되어 프로세서에 의해 구동될 수 있다. 상기 메모리는 상기 프로세서 내부 또는 외부에 위치하여, 이미 공지된 다양한 수단에 의해 상기 프로세서와 데이터를 주고 받을 수 있다.

[306] 본 발명은 본 발명의 필수적 특징을 벗어나지 않는 범위에서 다른 특정한 형태로 구체화될 수 있음은 당업자에게 자명하다. 따라서, 상술한 상세한 설명은 모든 면에서 제한적으로 해석되어서는 아니 되고 예시적인 것으로 고려되어야 한다. 본 발명의 범위는 첨부된 청구항의 합리적 해석에 의해 결정되어야 하고, 본 발명의 등가적 범위 내에서의 모든 변경은 본 발명의 범위에 포함된다.

산업상 이용가능성

[307] 본 발명은 보안 서비스를 제공하는 다양한 시스템에 적용될 수 있다.

청구범위

[청구항 1] 네트워크 보안 기능(NSF: Network Security Function)에 의해 트리거되는 트래픽 스티어링(traffic steering)을 지원하는 시스템에 있어서,
상기 시스템에 유입된 패킷에 대한 보안 검사를 수행하고, 상기 보안 검사의 결과에 기반하여 또 다른 NSF에 의한 추가적인 검사가 필요한지 여부를 판단하고, 상기 추가적인 검사가 필요하면, 상기 추가적인 검사를 호출하기 위한 패킷 전달 헤더(packet forwarding header)를 상기 패킷에 부착하고, 상기 패킷 전달 헤더가 부착된 패킷을 NSF 전달자(NSFF: NSF Forwarder)에게 전송하는 제1 NSF; 및
상기 패킷 전달 헤더에 포함된 상기 추가적인 검사를 위해 요구되는 보안 능력을 가진 제2 NSF를 탐색한 경우, 상기 제2 NSF에게 상기 패킷을 전달하는 NSFF를 포함하는 트래픽 스티어링 시스템.

[청구항 2] 제1항에 있어서,
상기 패킷 전달 헤더는 상기 패킷의 보안 검사의 결과를 포함하는 동작 코드 필드, 상기 추가적인 검사를 위해 요구되는 보안 능력 정보를 포함하는 능력 정보 필드, 상기 능력 정보 필드의 개수를 나타내는 능력 정보의 수 필드를 포함하는 트래픽 스티어링 시스템.

[청구항 3] 제1항에 있어서,
상기 시스템에 유입된 패킷은 상기 NSFF에 의해 수신되고, 상기 NSFF에 의해 상기 제1 NSF에게 전달되는 트래픽 스티어링 시스템.

[청구항 4] 제1항에 있어서,
상기 패킷의 소스(source)의 신뢰 레벨(trust level)에 따라 상기 제1 NSF에 의해 상기 패킷은 안전한 패킷(secure packet), 위험한 패킷(dangerous packet) 및 의심스러운 패킷(suspicious packet)으로 분류되는 트래픽 스티어링 시스템.

[청구항 5] 제4항에 있어서,
상기 패킷이 상기 안전한 패킷(secure packet)으로 분류된 경우 또 다른 NSF를 통해 추가의 보안 검사 없이 상기 패킷의 목적지(destination)으로 전달되는 트래픽 스티어링 시스템.

[청구항 6] 제4항에 있어서,
상기 패킷이 상기 위험한 패킷(dangerous packet)으로 분류된 경우 상기 패킷은 드랍(drop)되는 트래픽 스티어링 시스템.

[청구항 7] 제4항에 있어서,
상기 패킷이 상기 의심스러운 패킷(suspicious packet)으로 분류된 경우 상기 패킷은 상기 패킷 전달 헤더가 부착되어 상기 NSFF에게 전달되는 트래픽 스티어링 시스템.

[청구항 8] 제1항에 있어서,

이용 가능한 모든 NSF에 대한 정보 리스트를 관리하는 NSF 운영 관리자(operation management)를 더 포함하는 트래픽 스티어링 시스템.

[청구항 9] 제8항에 있어서,
상기 제2 NSF를 탐색하지 못한 경우, 상기 NSFF는 상기 추가적인 검사를 위해 요구되는 보안 능력을 포함하는 NSF 생성 요청 패킷을 상기 NSF 운영 관리자에게 전송하고, 상기 NSF 운영 관리자로부터 생성된 제3 NSF에 대한 정보를 수신하면 상기 제3 NSF에게 상기 패킷을 전달하고,
상기 NSF 운영 관리자는 상기 정보 리스트 내에서 각 NSF의 트래픽 로드 상태를 고려하여 상기 추가적인 검사를 위해 요구되는 보안 능력을 가지는 상기 제3 NSF를 선택하고, 상기 제3 NSF에 대한 정보를 상기 NSFF에게 전송하는 트래픽 스티어링 시스템.

[청구항 10] 제9항에 있어서,
상기 정보 리스트 내에서 상기 추가적인 검사를 위해 요구되는 보안 능력을 가지는 NSF가 존재하지 않는 경우,
개발자 관리 시스템(developer's management system)에게 상기 추가적인 검사를 위해 요구되는 보안 능력을 가지는 NSF의 생성을 요청하는 트래픽 스티어링 시스템.

[청구항 11] 제8항에 있어서,
상기 NSF 운영 관리자가 이용 가능한 모든 NSF의 트래픽 로드 상태를 모니터링하고,
특정 NSF에 대하여 과도한 트래픽이 발생됨을 감지하면, 개발자 관리 시스템(developer's management system)에게 상기 과도한 트래픽이 발생된 NSF와 동일한 보안 능력을 가지는 새로운 NSF의 생성을 요청하는 트래픽 스티어링 시스템.

[청구항 12] 제8항에 있어서,
상기 NSF 운영 관리자가 이용 가능한 모든 NSF의 트래픽 로드 상태를 모니터링하고,
특정 NSF가 이용되지 않음을 감지하면, 개발자 관리 시스템(developer's management system)에게 상기 이용되지 않는 NSF의 제거를 요청하는 트래픽 스티어링 시스템.

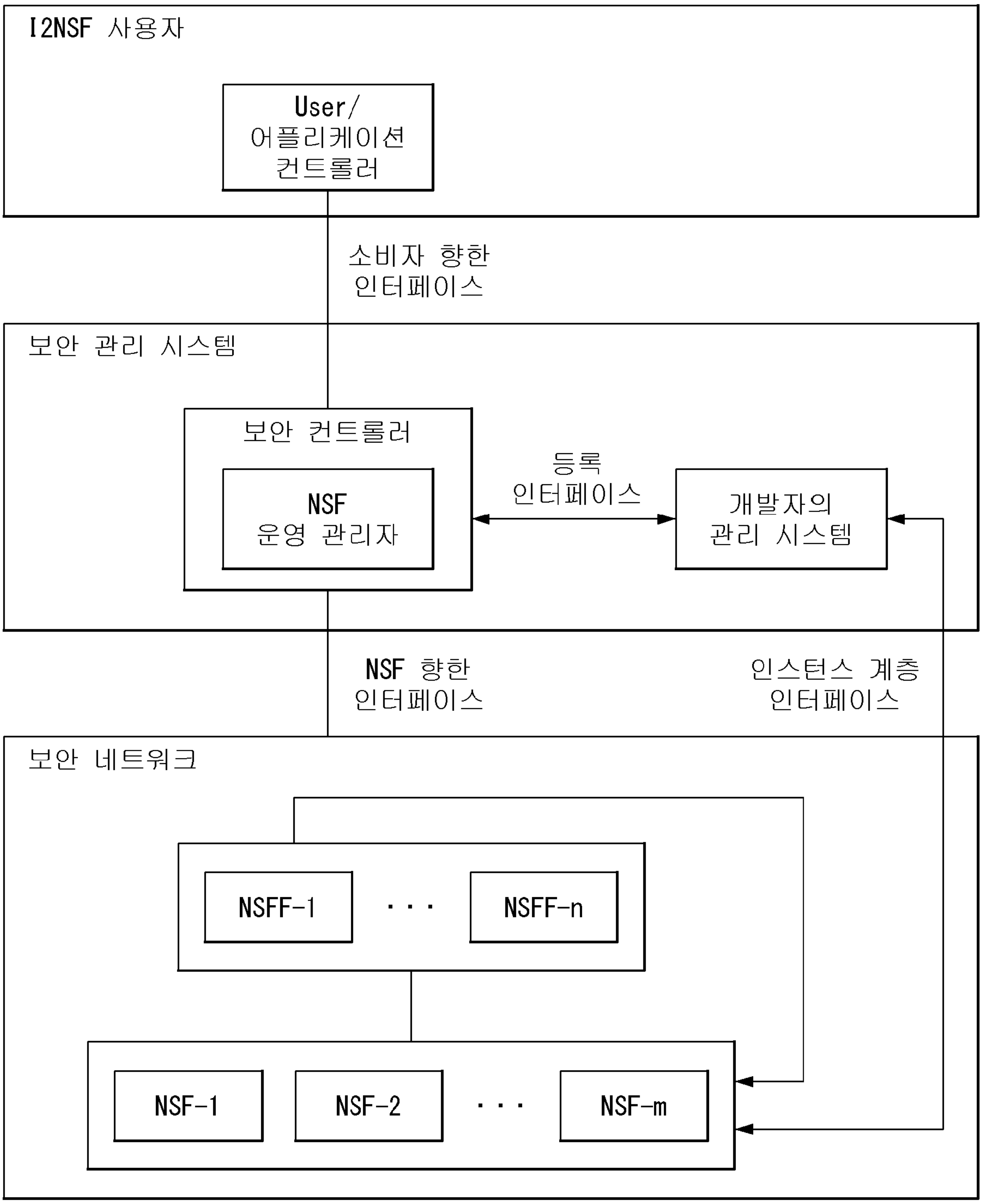
[청구항 13] 네트워크 보안 기능(NSF: Network Security Function)이 트래픽 스티어링(traffic steering)을 수행하는 방법에 있어서,
상기 트래픽 스티어링(traffic steering)을 지원하는 시스템에 유입된 패킷에 대한 보안 검사를 수행하는 단계;
상기 보안 검사의 결과에 기반하여 또 다른 NSF에 의한 추가적인 검사가 필요한지 여부를 판단하는 단계;
상기 추가적인 검사가 필요하면, 상기 추가적인 검사를 호출하기 위한 패킷 전달 헤더(packet forwarding header)를 상기 패킷에 부착하는 단계; 및

상기 패킷 전달 헤더가 부착된 패킷을 NSF 전달자(NSFF: NSF Forwarder)에게 전송하는 단계를 포함하고,
상기 패킷 전달 헤더는 상기 추가적인 검사를 위해 요구되는 보안 능력에 대한 정보를 포함하는 트래픽 스티어링 방법.

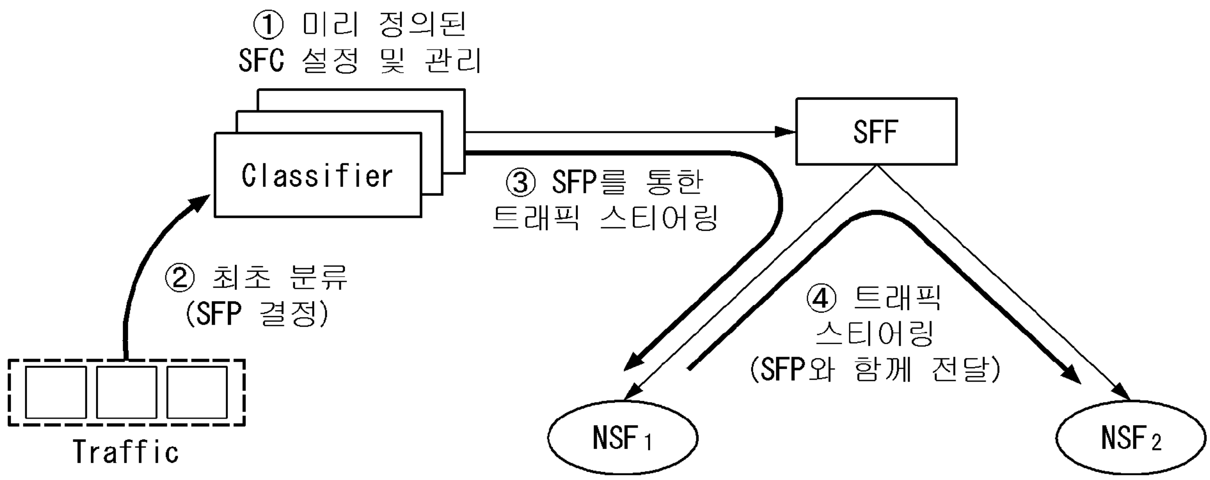
[청구항 14] 제13항에 있어서,
상기 패킷 전달 헤더는 상기 패킷의 보안 검사의 결과를 포함하는 동작 코드 필드, 상기 추가적인 검사를 위해 요구되는 보안 능력 정보를 포함하는 능력 정보 필드, 상기 능력 정보 필드의 개수를 나타내는 능력 정보의 수 필드를 포함하는 트래픽 스티어링 방법.

[청구항 15] 제13항에 있어서,
상기 패킷의 소스(source)의 신뢰 레벨(trust level)에 따라 상기 제1 NSF에 의해 상기 패킷이 안전한 패킷(secure packet), 위험한 패킷(dangerous packet) 및 의심스러운 패킷(suspicious packet)으로 분류되는 트래픽 스티어링 방법.

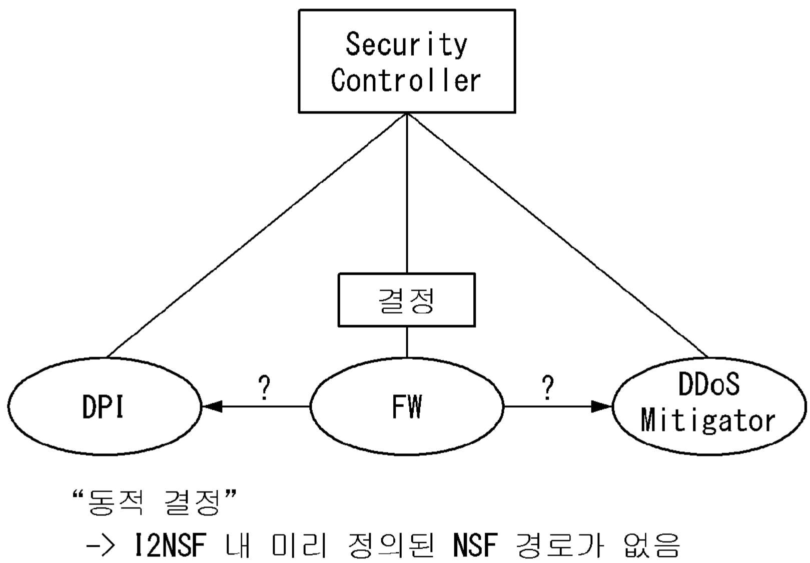
[도1]


I2NSF 사용자
User/
어플리케이션
컨트롤러
소비자 향한
인터페이스
보안 관리 시스템
보안 컨트롤러
NSF
운영 관리자
등록
인터페이스
개발자의
관리 시스템
NSF 향한
인터페이스
인스턴스 계층
인터페이스
보안 네트워크
NSFF-1
NSFF-n
NSF-1
NSF-2
NSF-m

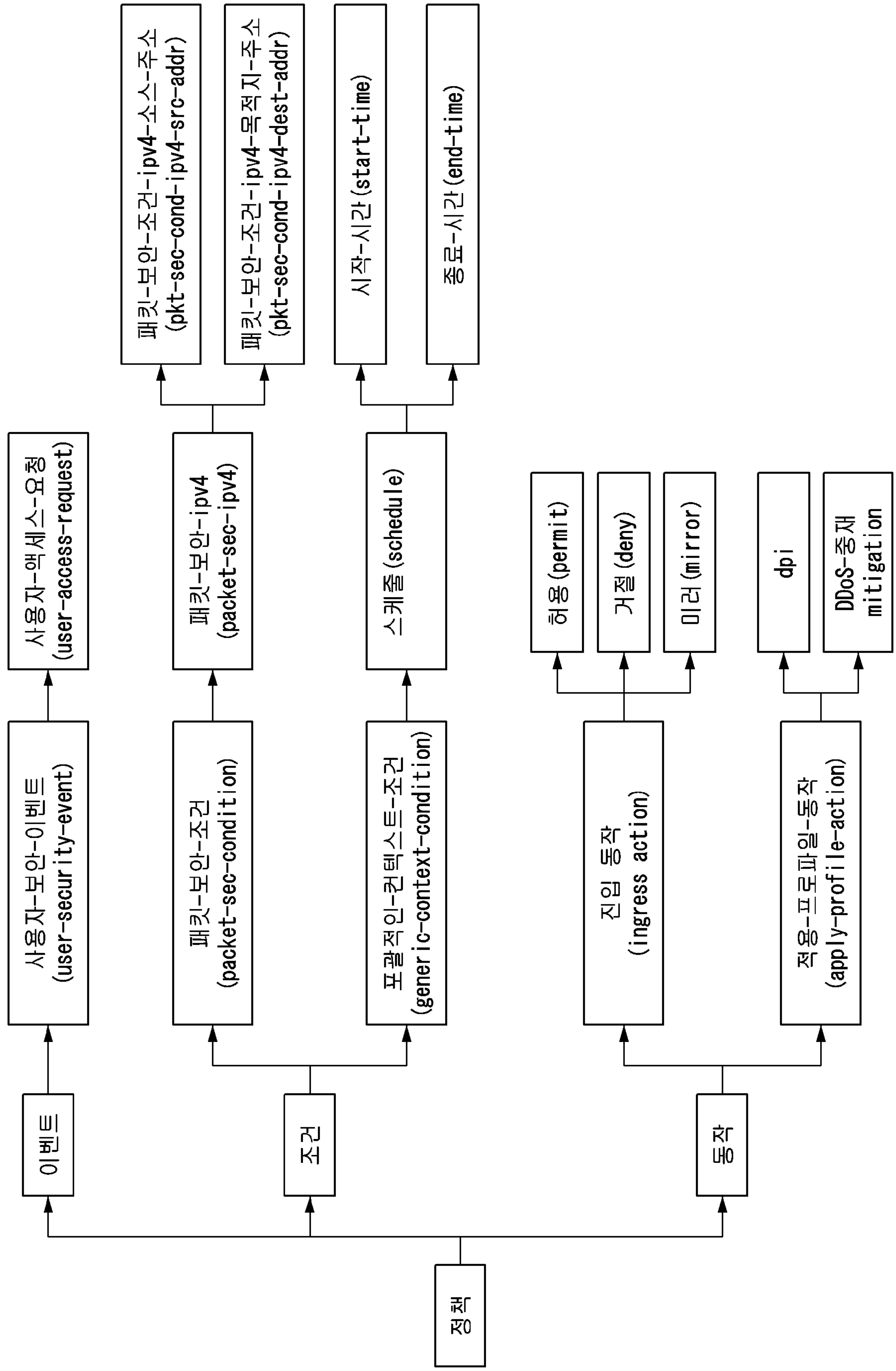
[도2]


① 미리 정의된
SFC 설정 및 관리
Classifier
SFF
③ SFP를 통한
트래픽 스티어링
② 최초 분류
(SFP 결정)
④ 트래픽
스티어링
(SFP와 함께 전달)
Traffic
NSF 1
NSF 2

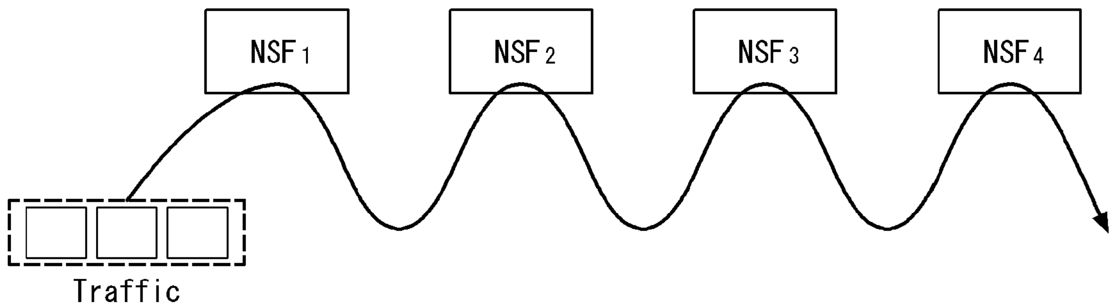
[도3]


Security
Controller
결정
DPI
?
FW
?
DDoS
Mitigator
"동적 결정"
-> I2NSF 내 미리 정의된 NSF 경로가 없음

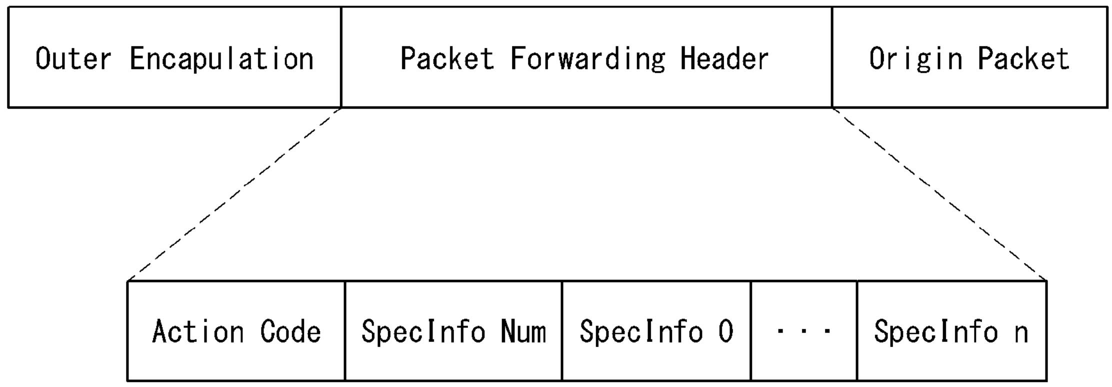
[도4]


정책
이벤트
조건
동작
사용자-보안-이벤트 (user-security-event)
사용자-액세스-요청 (user-access-request)
패킷-보안-조건 (packet-sec-condition)
패킷-보안-ipv4 (packet-sec-ipv4)
패킷-보안-조건-ipv4-소스-주소 (pkt-sec-cond-ipv4-src-addr)
패킷-보안-조건-ipv4-목적지-주소 (pkt-sec-cond-ipv4-dest-addr)
포괄적인-컨텍스트-조건 (generic-context-condition)
스케줄 (schedule)
시작-시간 (start-time)
종료-시간 (end-time)
진입 동작 (ingress action)
허용 (permit)
거절 (deny)
미러 (mirror)
적용-프로파일-동작 (apply-profile-action)
dpi
DDoS-중재 mitigation

[도5]

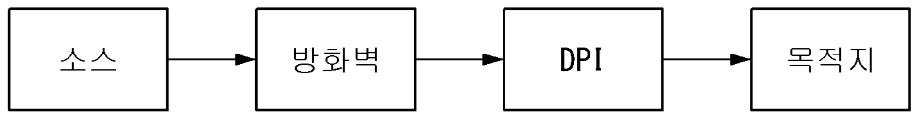


[도6]



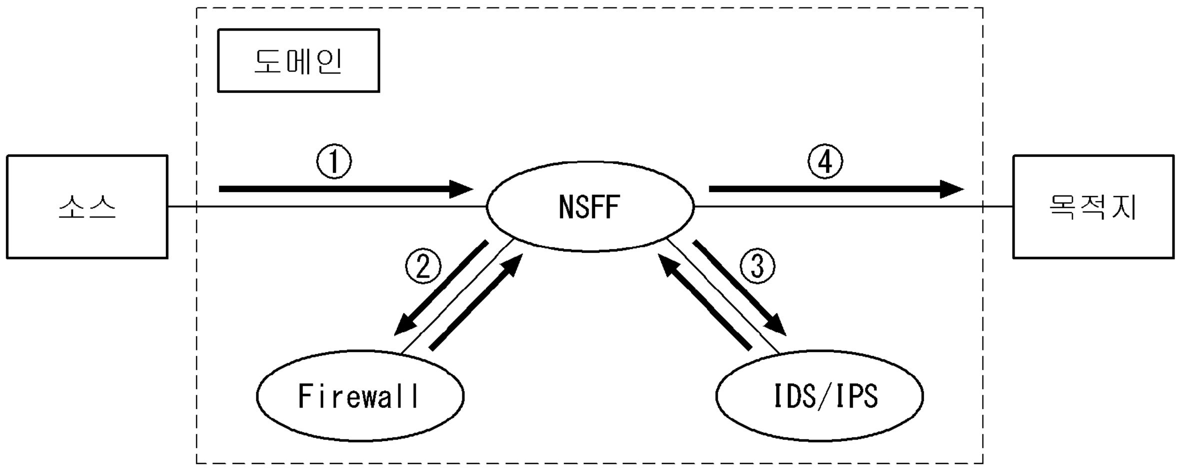
[도7]

(a) 신뢰된 소스의 트래픽 흐름

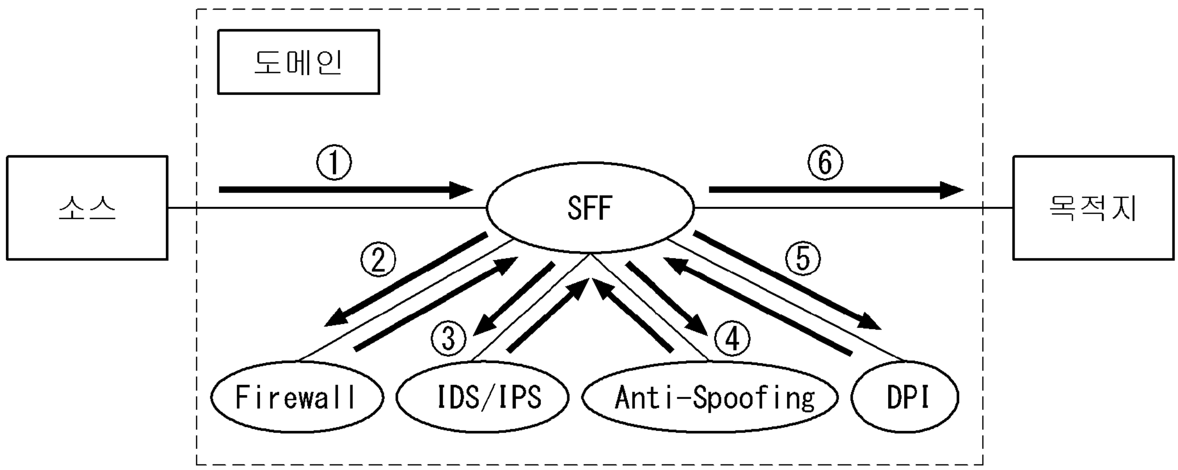


(b) 신뢰되지 않은 소스의 트래픽 흐름

[도8]

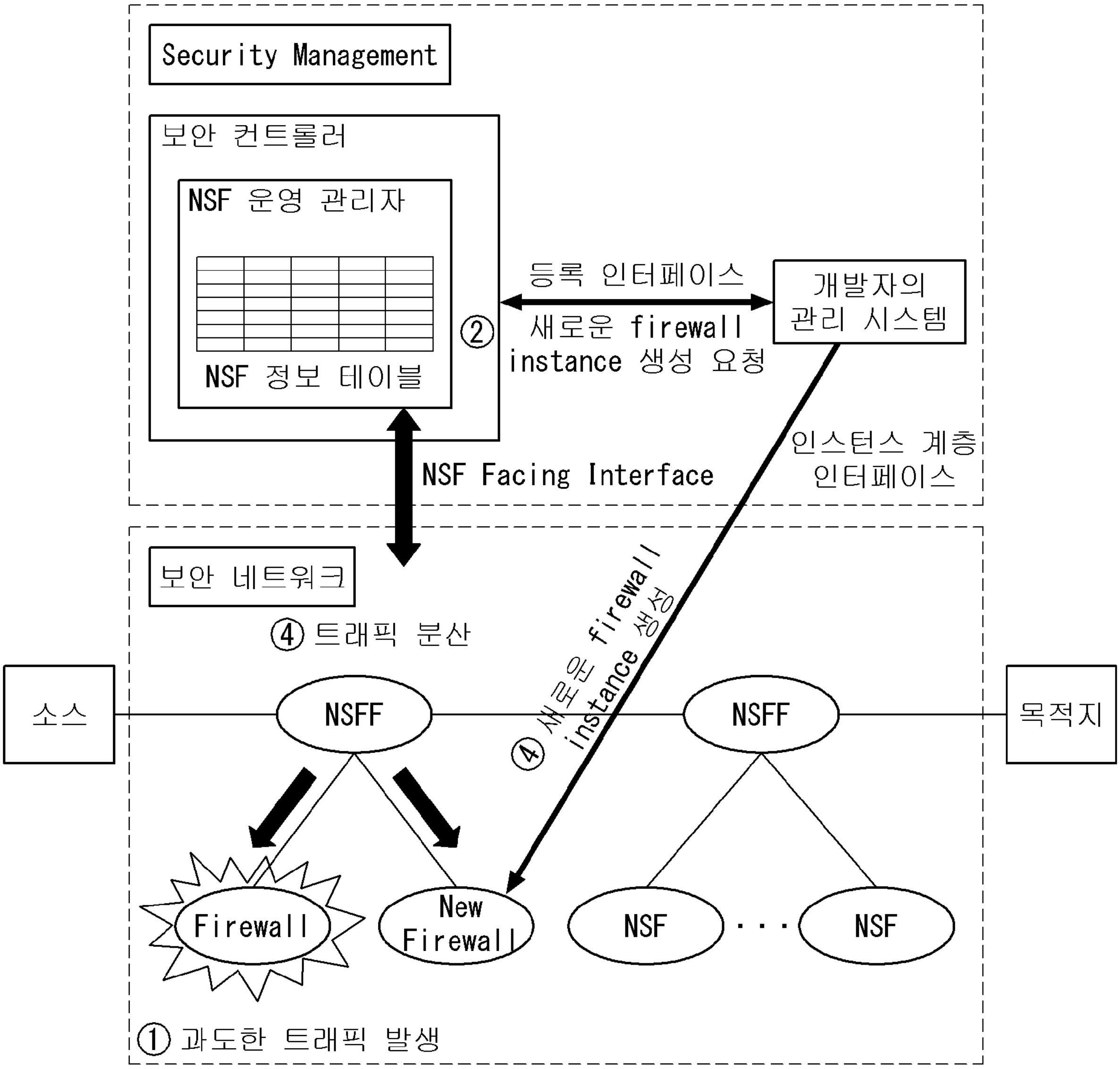

도메인
①
④
소스
NSFF
목적지
②
③
Firewall
IDS/IPS

(a)

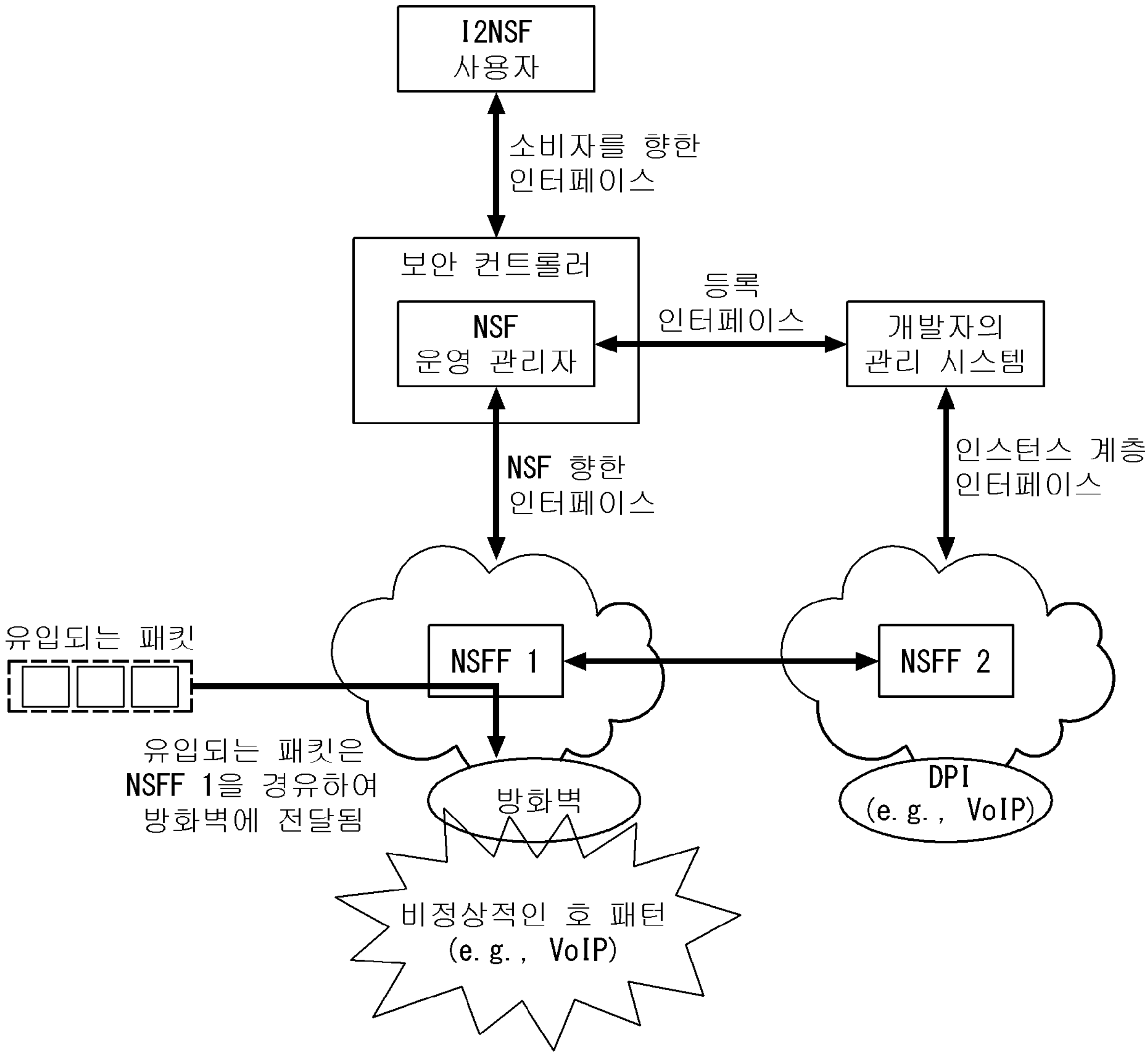

도메인
①
⑥
소스
SFF
목적지
②
⑤
③
④
Firewall
IDS/IPS
Anti-Spoofing
DPI

(b)

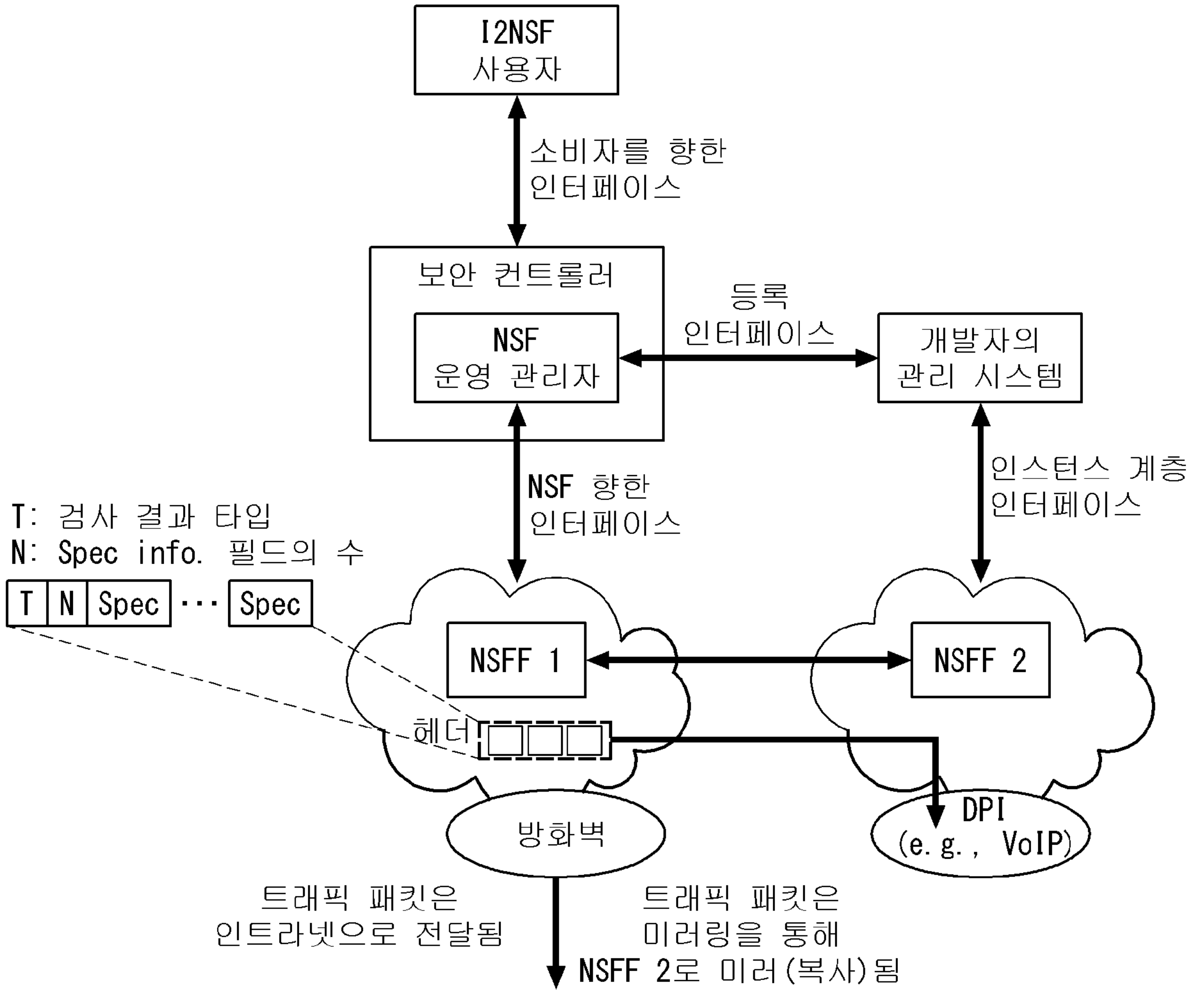
[도9]


Security Management
보안 컨트롤러
NSF 운영 관리자
NSF 정보 테이블
②
등록 인터페이스
새로운 firewall instance 생성 요청
개발자의 관리 시스템
인스턴스 계층 인터페이스
NSF Facing Interface
보안 네트워크
④ 트래픽 분산
④ 새로운 firewall instance 생성
소스
NSFF
NSFF
목적지
Firewall
New Firewall
NSF
NSF
① 과도한 트래픽 발생

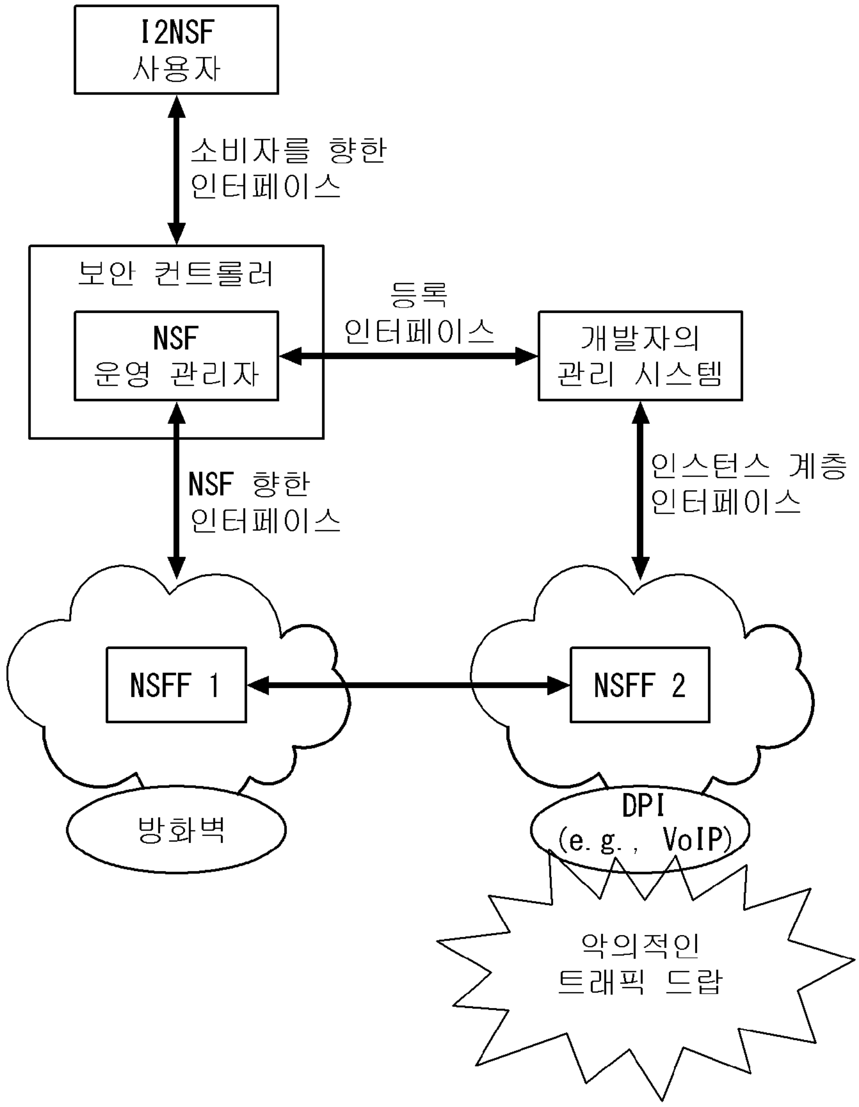
[도10]


I2NSF
사용자
소비자를 향한
인터페이스
보안 컨트롤러
NSF
운영 관리자
등록
인터페이스
개발자의
관리 시스템
NSF 향한
인터페이스
인스턴스 계층
인터페이스
유입되는 패킷
NSFF 1
NSFF 2
유입되는 패킷은
NSFF 1을 경유하여
방화벽에 전달됨
방화벽
DPI
(e.g., VoIP)
비정상적인 호 패턴
(e.g., VoIP)

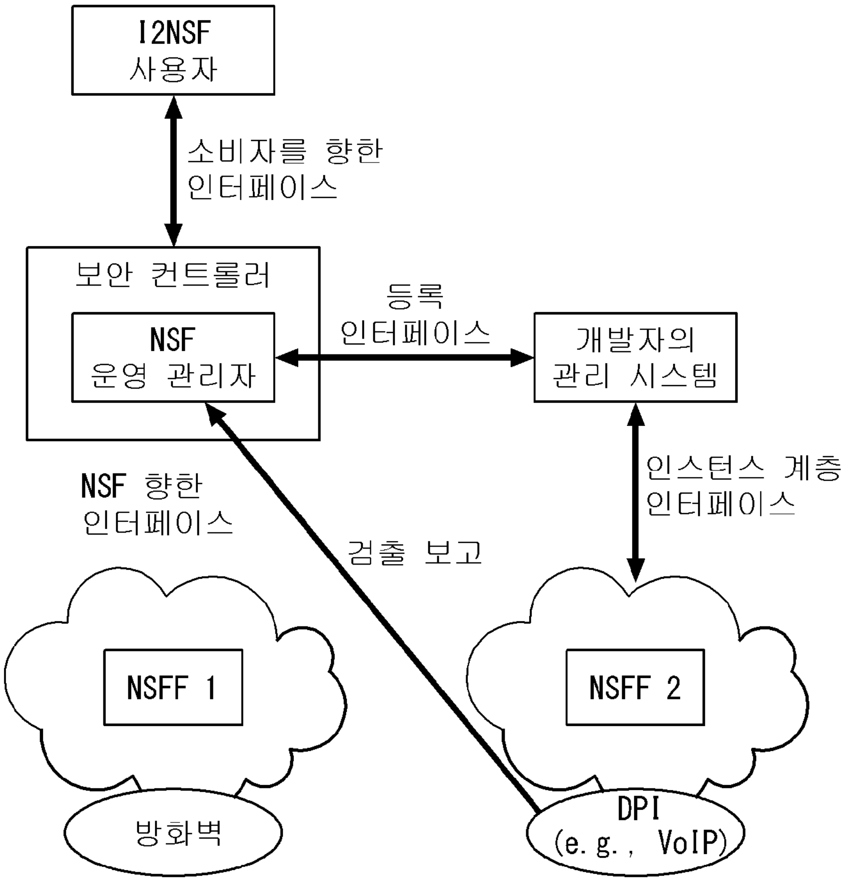
[도11]


I2NSF
사용자
소비자를 향한
인터페이스
보안 컨트롤러
NSF
운영 관리자
등록
인터페이스
개발자의
관리 시스템
NSF 향한
인터페이스
인스턴스 계층
인터페이스
T: 검사 결과 타입
N: Spec info. 필드의 수
T N Spec ··· Spec
NSFF 1
NSFF 2
헤더
방화벽
DPI
(e.g., VoIP)
트래픽 패킷은
인트라넷으로 전달됨
트래픽 패킷은
미러링을 통해
NSFF 2로 미러(복사)됨

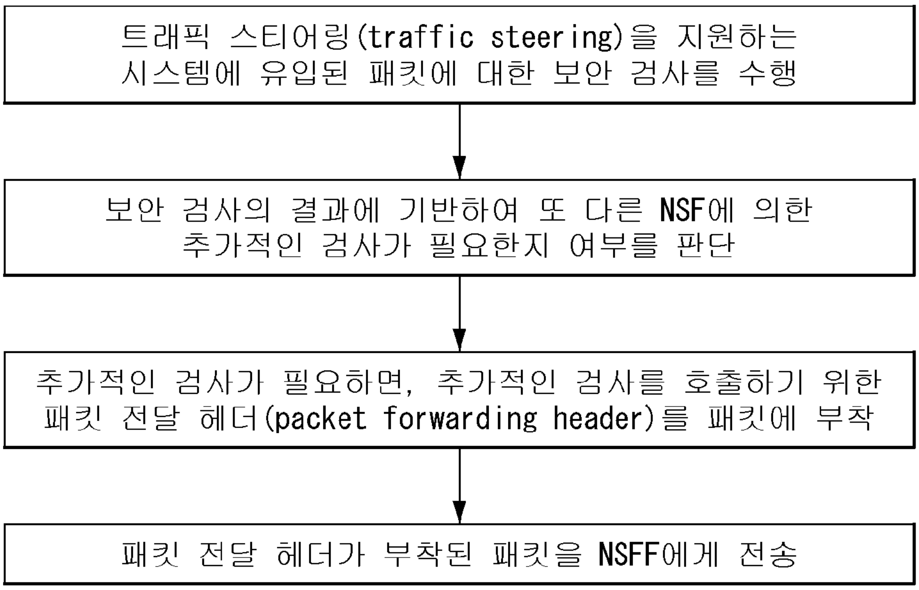
[도12]


I2NSF
사용자
소비자를 향한
인터페이스
보안 컨트롤러
NSF
운영 관리자
등록
인터페이스
개발자의
관리 시스템
NSF 향한
인터페이스
인스턴스 계층
인터페이스
NSFF 1
NSFF 2
방화벽
DPI
(e.g., VoIP)
악의적인
트래픽 드랍

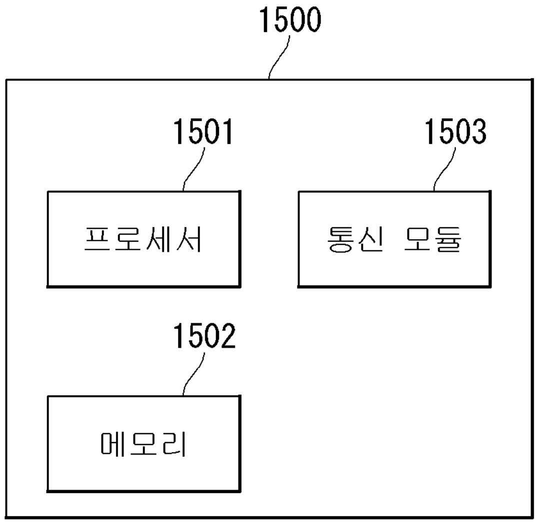
[도13]


I2NSF
사용자
소비자를 향한
인터페이스
보안 컨트롤러
NSF
운영 관리자
등록
인터페이스
개발자의
관리 시스템
NSF 향한
인터페이스
검출 보고
인스턴스 계층
인터페이스
NSFF 1
NSFF 2
방화벽
DPI
(e.g., VoIP)

[도14]


트래픽 스티어링(traffic steering)을 지원하는
시스템에 유입된 패킷에 대한 보안 검사를 수행
보안 검사의 결과에 기반하여 또 다른 NSF에 의한
추가적인 검사가 필요한지 여부를 판단
추가적인 검사가 필요하면, 추가적인 검사를 호출하기 위한
패킷 전달 헤더(packet forwarding header)를 패킷에 부착
패킷 전달 헤더가 부착된 패킷을 NSFF에게 전송

[도15]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2017/004510

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i, H04L 12/24(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L 29/06; H04L 12/24; H04L 29/08; H04L 12/26; H04L 12/28; H04L 12/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS (KIPO internal) & Keywords: network security, packet, header, traffic, trigger, security inspection, additional inspection, trust level

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2010-0132079 A (TIPPINGPOINT TECHNOLOGIES, INC.) 16 December 2010 See paragraphs [0021]-[0035], [0054]-[0061]; claim 14; and figures 1-2.	1-15
Y	KR 10-2009-0031380 A (QUALCOMM INCORPORATED) 25 March 2009 See paragraph [0133]; claim 79; and figure 6.	1-15
Y	HYUN, S. et al., NSF-triggered Traffic Steering in I2NSF Framework draft-hyun-i2nsf-nsf-triggered-steering-01, Network Working Group, 13 November 2016, pages 1-14. See page 7, lines 17-43; page 10, lines 8-10.	8-12
A	KR 10-1445765 B1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 06 October 2014 See paragraphs [0011]-[0023]; and figure 1.	1-15
A	US 2015-0215285 A1 (FLEURY, Damon E. et al.) 30 July 2015 See paragraphs [0016]-[0033]; and figures 1-4.	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 AUGUST 2017 (04.08.2017)	**07 AUGUST 2017 (07.08.2017)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. +82-42-481-8578	Telephone No.

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2010-0132079 A	16/12/2010	AR 42020 A1	08/06/2005
		AU 2003-290674 A1	03/06/2004
		AU 2003-290674 A8	03/06/2004
		CN 100472479 C	25/03/2009
		CN 1720459 A	11/01/2006
		CN 1720459 C	17/12/2008
		CN 1748205 A	15/03/2006
		EP 1558937 A2	03/08/2005
		EP 1558937 A4	28/01/2009
		EP 1558937 B1	24/08/2011
		EP 1590740 A2	02/11/2005
		JP 2006-506853 A	23/02/2006
		JP 2010-268483 A	25/11/2010
		KR 10-1045362 B1	30/06/2011
		KR 10-1111433 B1	17/02/2012
		KR 10-2005-0086441 A	30/08/2005
		US 2004-0093513 A1	13/05/2004
		US 2004-0151382 A1	05/08/2004
		US 2005-0028013 A1	03/02/2005
		US 2005-0044422 A1	24/02/2005
		US 7134143 B2	07/11/2006
		US 7451489 B2	11/11/2008
		US 7454499 B2	18/11/2008
		US 7454792 B2	18/11/2008
		WO 2004-045126 A2	27/05/2004
		WO 2004-045126 A3	02/12/2004
		WO 2004-070575 A2	19/08/2004
		WO 2004-070575 A3	23/06/2005
KR 10-2009-0031380 A	25/03/2009	AU 2008-279217 A1	29/01/2009
		AU 2008-279217 B2	30/06/2011
		AU 2008-279219 A1	29/01/2009
		AU 2008-279219 B2	08/09/2011
		BR PI712412 A2	14/08/2012
		CA 2646906 A1	13/12/2007
		CL 2007-001656 A1	11/01/2008
		CN 101433055 A	13/05/2009
		CN 101779422 A	14/07/2010
		CN 101855870 A	06/10/2010
		EP 2036302 A2	18/03/2009
		EP 2181529 A1	05/05/2010
		EP 2181530 A1	05/05/2010
		IL 203004 A	31/10/2010
		IL 203005 A	31/10/2010
		JP 2009-540694 A	19/11/2009
		JP 2010-534975 A	11/11/2010
		JP 2010-534976 A	11/11/2010
		KR 10-1028977 B1	12/04/2011
		KR 10-2010-0047273 A	07/05/2010

Patent document cited in search report	Publication date	Patent family member	Publication date
		KR 10-2010-0047274 A	07/05/2010
		RU 2008-148124 A	10/06/2010
		RU 2420903 C2	10/06/2011
		TW 200814641 A	16/03/2008
		TW 200920037 A	01/05/2009
		TW 200920054 A	01/05/2009
		US 2007-0286126 A1	13/12/2007
		US 2008-0069048 A1	20/03/2008
		US 2008-0075045 A1	27/03/2008
		US 7978677 B2	12/07/2011
		US 8565216 B2	22/10/2013
		US 8565217 B2	22/10/2013
		WO 2007-143721 A2	13/12/2007
		WO 2007-143721 A3	16/10/2008
		WO 2009-015196 A1	29/01/2009
		WO 2009-015198 A1	29/01/2009
KR 10-1445765 B1	06/10/2014	NONE	
US 2015-0215285 A1	30/07/2015	CN 104488229 A	01/04/2015
		EP 2880819 A1	10/06/2015
		EP 2880819 A4	09/03/2016
		JP 2015-528263 A	24/09/2015
		KR 10-2015-0037940 A	08/04/2015
		TW 201406106 A	01/02/2014
		TW I528761 B	01/04/2016
		US 9544273 B2	10/01/2017
		WO 2014-021863 A1	06/02/2014

국제조사보고서

국제출원번호 **PCT/KR2017/004510**

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 29/06(2006.01)i, H04L 12/24(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 29/06; H04L 12/24; H04L 29/08; H04L 12/26; H04L 12/28; H04L 12/22

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 네트워크 보안, 패킷, 헤더, 트래픽, 트리거, 보안 검사, 추가 검사, 신뢰 레벨

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2010-0132079 A (팁핑포인트 테크놀러지스 인코포레이티드) 2010.12.16 단락 [0021]-[0035], [0054]-[0061]; 청구항 14; 및 도면 1-2 참조.	1-15
Y	KR 10-2009-0031380 A (퀄컴 인코포레이티드) 2009.03.25 단락 [0133]; 청구항 79; 및 도면 6 참조.	1-15
Y	S. HYUN et al., NSF-triggered Traffic Steering in I2NSF Framework draft-hyun-i2nsf-nsf-triggered-steering-01, Network Working Group, 2016.11.13, 페이지 1-14. 페이지 7, 라인 17-43; 페이지 10, 라인 8-10 참조.	8-12
A	KR 10-1445765 B1 (한국전자통신연구원) 2014.10.06 단락 [0011]-[0023]; 및 도면 1 참조.	1-15
A	US 2015-0215285 A1 (DAMON E. FLEURY 등) 2015.07.30 단락 [0016]-[0033]; 및 도면 1-4 참조.	1-15

☐ 추가 문헌이 C(계속)에 기재되어 있습니다. ☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2017년 08월 04일 (04.08.2017)	2017년 08월 07일 (07.08.2017)

ISA/KR의 명칭 및 우편주소	심사관
대한민국 특허청 (35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)	김성우
팩스 번호 +82-42-481-8578	전화번호 +82-42-481-3348

국제조사보고서

대응특허에 관한 정보

국제출원번호

PCT/KR2017/004510

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2010-0132079 A	2010/12/16	AR 42020 A1	2005/06/08
		AU 2003-290674 A1	2004/06/03
		AU 2003-290674 A8	2004/06/03
		CN 100472479 C	2009/03/25
		CN 1720459 A	2006/01/11
		CN 1720459 C	2008/12/17
		CN 1748205 A	2006/03/15
		EP 1558937 A2	2005/08/03
		EP 1558937 A4	2009/01/28
		EP 1558937 B1	2011/08/24
		EP 1590740 A2	2005/11/02
		JP 2006-506853 A	2006/02/23
		JP 2010-268483 A	2010/11/25
		KR 10-1045362 B1	2011/06/30
		KR 10-1111433 B1	2012/02/17
		KR 10-2005-0086441 A	2005/08/30
		US 2004-0093513 A1	2004/05/13
		US 2004-0151382 A1	2004/08/05
		US 2005-0028013 A1	2005/02/03
		US 2005-0044422 A1	2005/02/24
		US 7134143 B2	2006/11/07
		US 7451489 B2	2008/11/11
		US 7454499 B2	2008/11/18
		US 7454792 B2	2008/11/18
		WO 2004-045126 A2	2004/05/27
		WO 2004-045126 A3	2004/12/02
		WO 2004-070575 A2	2004/08/19
		WO 2004-070575 A3	2005/06/23
KR 10-2009-0031380 A	2009/03/25	AU 2008-279217 A1	2009/01/29
		AU 2008-279217 B2	2011/06/30
		AU 2008-279219 A1	2009/01/29
		AU 2008-279219 B2	2011/09/08
		BR PI712412 A2	2012/08/14
		CA 2646906 A1	2007/12/13
		CL 2007-001656 A1	2008/01/11
		CN 101433055 A	2009/05/13
		CN 101779422 A	2010/07/14
		CN 101855870 A	2010/10/06
		EP 2036302 A2	2009/03/18
		EP 2181529 A1	2010/05/05
		EP 2181530 A1	2010/05/05
		IL 203004 A	2010/10/31
		IL 203005 A	2010/10/31
		JP 2009-540694 A	2009/11/19
		JP 2010-534975 A	2010/11/11
		JP 2010-534976 A	2010/11/11
		KR 10-1028977 B1	2011/04/12
		KR 10-2010-0047273 A	2010/05/07

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2017/004510

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
		KR 10-2010-0047274 A	2010/05/07
		RU 2008-148124 A	2010/06/10
		RU 2420903 C2	2011/06/10
		TW 200814641 A	2008/03/16
		TW 200920037 A	2009/05/01
		TW 200920054 A	2009/05/01
		US 2007-0286126 A1	2007/12/13
		US 2008-0069048 A1	2008/03/20
		US 2008-0075045 A1	2008/03/27
		US 7978677 B2	2011/07/12
		US 8565216 B2	2013/10/22
		US 8565217 B2	2013/10/22
		WO 2007-143721 A2	2007/12/13
		WO 2007-143721 A3	2008/10/16
		WO 2009-015196 A1	2009/01/29
		WO 2009-015198 A1	2009/01/29
KR 10-1445765 B1	2014/10/06	없음	
US 2015-0215285 A1	2015/07/30	CN 104488229 A	2015/04/01
		EP 2880819 A1	2015/06/10
		EP 2880819 A4	2016/03/09
		JP 2015-528263 A	2015/09/24
		KR 10-2015-0037940 A	2015/04/08
		TW 201406106 A	2014/02/01
		TW I528761 B	2016/04/01
		US 9544273 B2	2017/01/10
		WO 2014-021863 A1	2014/02/06