(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2018 년 9 월 20 일 (20.09.2018)

WIPO | PCT

(10) 국제공개번호
WO 2018/169291 A1

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

(21) 국제출원번호: PCT/KR2018/002954

(22) 국제출원일: 2018 년 3 월 13 일 (13.03.2018)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2017-0031424 2017 년 3 월 13 일 (13.03.2017) KR

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

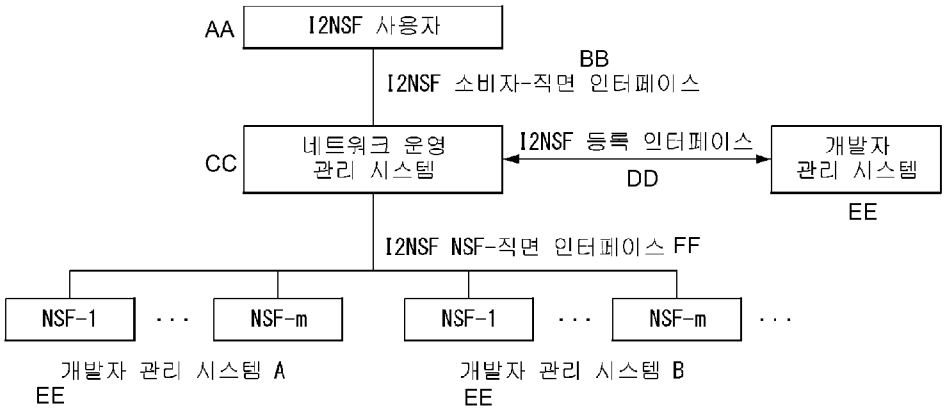
(72) 발명자: 정재훈 (JEONG, Jaehoon); 46294 부산시 금정구 금강로 225, 204-1501, Busan (KR). 현상원 (HYUN, Sangwon); 07071 서울시 동작구 보라매로5길 51, 2105, Seoul (KR). 우상욱 (WOO, Sang Uk); 13564 경기도 성남시 분당구 탄천로 59, 509-1103, Gyeonggi-do (KR). 여윤석 (YEO, Yunsuk); 01676 서울시 노원구 노원로 532, 907-1001, Seoul (KR).

(74) 대리인: 특허법인 로얄 (ROYAL PATENT & LAW OFFICE); 06648 서울시 서초구 반포대로 104 서일빌딩 4 층, 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, JO, 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,

(54) **Title:** REGISTRATION INTERFACE INFORMATION MODEL WITH RESPECT TO NETWORK SECURITY FUNCTION

(54) **발명의 명칭:** 네트워크 보안 기능에 대한 등록 인터페이스 정보 모델



AA ... I2NSF user
BB ... I2NSF user-contact interface
CC ... Network operation management system
DD ... I2NSF registration interface
EE ... Developer management system
FF ... I2NSF NSF-contact interface

(57) **Abstract:** Disclosed is a security management system for managing a network security function (NSF) by means of a registration interface. More particularly, a method performed by means of a security controller can comprise the steps of: transmitting an instantiation request message with respect to an NSF required in a security management system to a developer management system; and receiving from the developer management system a registration message indicating registration of an NSF instance with respect to the required NSF as a response to the request message.

(57) **요약서:** 본 발명에서는 등록 인터페이스(Registration Interface)를 통해 네트워크 보안 기능(NSF: Network Secure Function)을 관리하는 보안 관리 시스템이 개시된다. 구체적으로, 보안 제어기(Security Controller)에 의해 수행되는 방법은, 상기 보안 관리 시스템에서 필요한 NSF에 대한 인스턴스화(instantiation) 요청 메시지를 개발자 관리 시스템(Developer's Management System)으로 전송하는 단계; 및 상기 요청 메시지에 대한 응답으로 상기 필요한 NSF에 대한 NSF 인스턴스의 등록을 지시하는 등록 메시지를 상기 개발자 관리 시스템으로부터 수신하는 단계를 포함할 수 있다.

WO 2018/169291 A1

[다음 쪽 계속]

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).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 네트워크 보안 기능에 대한 등록 인터페이스 정보 모델

기술분야

[1] 본 발명은 등록 인터페이스 정보 모델에 관한 것으로서, 보다 상세하게 I2NSF(Interface to Network Security Functions)에서 네트워크 보안 능력(Network Security Functions: NSF)의 등록 인터페이스를 위한 정보 모델과 보안 관리 서비스를 위한 것이다.

[2]

배경기술

[3] 네트워크를 전세계에 연결하면 지리적 거리에 관계없이 신속하게 정보에 액세스 할 수 있다. 인터넷은 본질적으로 서로 다른 레벨들의 계층 구조가 서로 연결된 수많은 네트워크이다.

[4] 인터넷은 IETF (Internet Engineering Task Force)에서 공표 한 TCP/IP (전송 제어 프로토콜/인터넷 프로토콜)에 따라 운영되며, TCP/IP는 RFC (Request For Comments) 703 및 IETF에서 발행 한 RFC 791에서 찾을 수 있다.

[5]

발명의 상세한 설명

기술적 과제

[6] 본 발명의 목적은, NSF 등록 및 인스턴스화를 지원하기 위하여 보안 제어기와 개발자 관리 시스템간 등록 인터페이스에 필요한 정보 모델을 제안한다.

[7] 또한, 본 발명의 목적은, 등록 인터페이스를 통해 보안 제어기와 개발자 관리 시스템에 의해 수행되는 정보 모델에 기반한 절차를 제안한다.

[8] 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.

[9]

과제 해결 수단

[10] 본 발명의 일 양상은, 등록 인터페이스(Registration Interface)를 통해 네트워크 보안 기능(NSF: Network Secure Function)을 관리하는 보안 관리 시스템에서, 보안 제어기(Security Controller)에 의해 수행되는 방법은, 상기 보안 관리 시스템에서 필요한 NSF에 대한 인스턴스화(instantiation) 요청 메시지를 개발자 관리 시스템(Developer's Management System)으로 전송하는 단계; 및 상기 요청 메시지에 대한 응답으로 상기 필요한 NSF에 대한 NSF 인스턴스의 등록을 지시하는 등록 메시지를 상기 개발자 관리 시스템으로부터 수신하는 단계를

포함할 수 있다.

[11] 바람직하게, 상기 보안 관리 시스템에서 필요한 NSF의 능력 정보(Capability Information) 또는 서명(signature)을 인식하는 단계를 더 포함하고, 상기 인스턴스화 요청 메시지는 상기 능력 정보 또는 상기 서명을 포함할 수 있다.

[12] 바람직하게, 상기 NSF 인스턴스는 상기 인스턴스화 요청 메시지에 기초하여 개발자 관리 시스템에 의해 생성될 수 있다.

[13] 바람직하게, 상기 보안 관리 시스템에서 불필요한 NSF에 대한 역인스턴스화(de-instantiation) 요청 메시지를 개발자 관리 시스템으로 전송하는 단계를 더 포함하고, 상기 역인스턴스화 요청 메시지에 대응되는 NSF 인스턴스가 상기 개발자 관리 시스템에 의해 삭제될 수 있다.

[14] 바람직하게, 상기 등록 메시지는 NSF 인스턴스의 보안 능력을 나타내는 NSF 능력 정보(Capability Information) 또는 새로운 인스턴스에 대한 네트워크 접근을 위해 이용되는 NSF 접근 정보(Access Information) 중 적어도 하나를 포함할 수 있다.

[15] 바람직하게, 상기 NSF 접근 정보는 IPv4(Internet Protocol version 4) 주소(address), IPv6(Internet Protocol version 6) 주소, 포트 번호(port number) 또는 지원되는 전송 프로토콜(transport protocol) 중 적어도 하나를 포함할 수 있다.

[16] 바람직하게, 상기 지원되는 전송 프로토콜은 가상 확장(Virtual Extensible) LAN(VXLAN), VXLAN를 위한 일반 프로토콜 확장(VXLAN-GPE(Generic Protocol Extension)), 일반 경로 캡슐화(GRE: Generic Route Encapsulation) 또는 이더넷(Ethernet) 중 적어도 하나를 포함할 수 있다.

[17] 바람직하게, 상기 NSF 능력 정보는 네트워크 보안 능력(Network-Security Capabilities), 컨텐츠 보안 능력(Content-Security Capabilities), 공격 완화 능력(Attack Mitigation Capabilities), 수행 능력(performance capabilities) 중 적어도 하나를 포함할 수 있다.

[18] 바람직하게, 상기 수행 능력은 처리(Processing) 및 대역폭(Bandwidth) 정보를 포함할 수 있다.

[19] 바람직하게, 상기 역할 기반 접근 제어 리스트는 엔티티의 역할 식별에 이용되는 하나 이상의 역할 ID를 포함하고, 상기 역할 ID는 특정 유형의 접근 요청을 식별하는데 사용되는 하나 이상의 접근 유형을 포함할 수 있다.

[20] 본 발명의 다른 일 양상은 등록 인터페이스(Registration Interface)를 통해 네트워크 보안 기능(NSF: Network Secure Function)을 관리하는 보안 제어기(Security Controller)에 있어서, 외부 장치와 무선 또는 유선으로 통신하기 위한 통신부; 및 상기 통신부와 기능적으로 연결되는 프로세서를 포함하되, 상기 프로세서는, 상기 보안 관리 시스템에서 필요한 NSF에 대한 인스턴스화(instantiation) 요청 메시지를 개발자 관리 시스템(Developer's Management System)으로 전송하고, 및 상기 요청 메시지에 대한 응답으로 상기 필요한 NSF에 대한 NSF 인스턴스의 등록을 지시하는 등록 메시지를 상기

개발자 관리 시스템으로부터 수신할 수 있다.

[21]

발명의 효과

[22] 본 발명의 실시예에 따르면, 기존의 I2NSF 등록 인터페이스의 활용도를 확장할 수 있다.

[23] 또한, 본 발명의 실시예에 따르면, NSF 능력 정보(capability information)모델을 정의함으로써 I2NSF 프레임 워크의 구성 요소들이 NSF 능력(Capability)들의 세트를 표준화된 방식으로 교환할 수 있다.

[24] 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.

[25]

도면의 간단한 설명

[26] 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.

[27] 도 1은 본 발명의 일 실시예에 따른 I2NSF(Interface to Network Security Functions) 시스템을 예시한다.

[28] 도 2는 본 발명의 다른 실시예에 따른 I2NSF 시스템의 아키텍처를 예시한다.

[29] 도 3은 본 발명이 적용되는 실시예로서, 등록 인터페이스를 통해 NSF 인스턴스를 등록하는 방법을 나타내는 흐름도이다.

[30] 도 4는 본 발명의 일 실시예에 따른 등록 인터페이스의 정보 모델을 예시하는 도면이다.

[31] 도 5는 본 발명의 일 실시예에 따른 인스턴스 관리 서브 모델(Instance Management Sub-Model)을 예시하는 도면이다.

[32] 도 6은 본 발명의 일 실시예에 따른 등록 서브 모델(Registration Sub-Model)을 예시하는 도면이다.

[33] 도 7은 본 발명의 일 실시예에 따른, NSF 능력 정보(Capability Information)를 개략적으로 나타내는 도면이다.

[34] 도 8은 본 발명의 일 실시예에 따른, 수행 능력(Performance Capabilities) 정보를 개략적으로 나타내는 도면이다.

[35] 도 9 및 도 10은 본 발명의 일 실시예에 따른 역할 기반 ACL(Role-based Access Control List)을 예시하는 도면이다.

[36] 도 11는 본 발명의 일 실시예에 따른 네트워크 장치의 블록 구성도를 예시한다.

[37]

발명의 실시를 위한 형태

[38] 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.

[39] 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.

[40] 아울러, 본 발명에서 사용되는 용어는 가능한 한 현재 널리 사용되는 일반적인 용어를 선택하였으나, 특정한 경우는 출원인이 임의로 선정한 용어를 사용하여 설명한다. 그러한 경우에는 해당 부분의 상세 설명에서 그 의미를 명확히 기재하므로, 본 발명의 설명에서 사용된 용어의 명칭만으로 단순 해석되어서는 안 될 것이며 그 해당 용어의 의미까지 파악하여 해석되어야 함을 밝혀두고자 한다.

[41] 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.

[42] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다.

[43] 본 명세서 전체에서, 어떤 부재가 다른 부재 “상에” 위치하고 있다고 할 때, 이는 어떤 부재가 다른 부재에 접해 있는 경우뿐 아니라 두 부재 사이에 또 다른 부재가 존재하는 경우도 포함한다.

[44] 본 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함" 한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다. 본원 명세서 전체에서 사용되는 정도의 용어 "~(하는) 단계" 또는 "~의 단계"는 "~ 를 위한 단계"를 의미하지 않는다.

[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]

[49] 도 1은 본 발명의 일 실시예에 따른 I2NSF(Interface to Network Security Functions) 시스템을 예시한다.

[50] 도 1을 참조하면, I2NSF 시스템은 I2NSF 사용자(user), 네트워크 운영 관리 시스템(Network Operator Management System), 개발자 관리 시스템(Developer's Management System) 및/또는 적어도 하나의 NSF(Network Security Function)을 포함한다.

[51] I2NSF 사용자는 I2NSF 소비자-직면 인터페이스(I2NSF Consumer-Facing Interface)를 통해 네트워크 운영 관리 시스템과 통신한다. 네트워크 운영 관리 시스템은 I2NSF NSF-직면 인터페이스(I2NSF NSF-Facing Interface)를 통해 NSF(들)과 통신한다. 개발자 관리 시스템은 I2NSF 등록 인터페이스(I2NSF Registration Interface)를 통해 네트워크 운영 관리 시스템과 통신한다. 이하에서는 I2NSF 시스템의 각 컴포넌트(I2NSF 컴포넌트) 및 각 인터페이스(I2NSF 인터페이스)에 설명한다.

[52] I2NSF 사용자

[53] I2NSF 사용자는 다른 I2NSF 컴포넌트(예컨대, 네트워크 운영 관리 시스템)에서 정보(예컨대, NSF의 정보)를 요청하거나 및/또는 다른 I2NSF 컴포넌트(예컨대, 개발자 관리 시스템)에 의해 제공되는 보안 서비스(예컨대, 네트워크 보안 서비스)를 사용하는 I2NSF 컴포넌트이다. 예를 들면, I2NSF 사용자는 오버레이 네트워크 관리 시스템, 기업 네트워크 관리자 시스템, 다른 네트워크 도메인 관리자 등일 수 있다. I2NSF 사용자는 I2NSF 클라이언트로 지칭될 수 있다.

[54] 이러한 I2NSF 사용자 컴포넌트에 할당된 역할을 수행하는 대상은 I2NSF 소비자로 지칭될 수 있다. I2NSF 소비자의 예로는, 일정 기간(time span) 동안 패킷의 특정 필드에 기초하여 흐름을 허용, 속도-제한(rate-limit), 또는 거부하기 위해 언더레이 네트워크(underlay network)에 동적으로 알릴 필요가 있는 화상 회의 네트워크 관리자(video-conference network manager), 특정 흐름에 대한 특정 I2NSF 정책을 시행(enforce)하기 위해 제공자 네트워크를 요청할 필요가 있는 기업 네트워크 관리자(Enterprise network administrators) 및 관리 시스템(management systems), 특정 조건의 세트와 일치하는 흐름을 차단하기 위해 언더레이 네트워크에 요청을 전송하는 IoT 관리 시스템(IoT management system)이 포함될 수 있다.

[55] I2NSF 사용자는 고수준(high-level) 보안 정책(security policy)을 생성 및 배포할 수 있다. 구체적으로 설명하면, I2NSF 사용자는 다양한 악의적인(malicious) 공격으로부터 네트워크 트래픽(traffic)을 보호하기 위하여 네트워크 보안 서비스(network security service)를 이용할 필요가 있다. 이 보안 서비스를

요청하기 위하여, I2NSF 사용자는 자신이 원하는 보안 서비스에 대한 고수준 보안 정책을 생성하고 네트워크 운영 관리 시스템에게 이를 알릴 수 있다.

[56] 한편, 고수준 보안 정책을 준비하는 과정에서, I2NSF 사용자는 각 NSF(들)를 위한 보안 서비스 또는 보안 정책 규칙 구성(security policy rule configuration)을 실현하기 위하여 요구되는 NSF(들)의 타입에 대하여 고려하지 않을 수 있다.

[57] 또한, I2NSF 사용자는 네트워크 운영 관리 시스템에 의해 기본적인(underlying) NSF(들) 내에서 발생되는 보안 이벤트(들)(security event)를 통지 받을 수 있다. 이들의 보안 이벤트(들)을 분석함으로써, I2NSF 사용자는 새로운 공격을 식별하고, 새로운 공격에 대처하기 위한 고수준 보안 정책을 업데이트(또는 생성)할 수 있다. 이와 같이, I2NSF 사용자는 보안 정책을 정의, 관리 및 모니터링할 수 있다.

[58] 네트워크 운영 관리 시스템

[59] 네트워크 운영 관리 시스템은 보안 제공, 모니터링 및 기타 동작을 위한 수집(collection) 및 배포(distribution) 지점(point)의 역할을 수행하는 컴포넌트이다. 예를 들면, 네트워크 운영 관리 시스템은 보안 제어기(Security Controller)에 해당하거나, 또는 보안 제어기를 포함하는 컴포넌트일 수 있다. 이러한 네트워크 운영 관리 시스템은 네트워크 운영자에 의해 관리될 수 있고, I2NSF 관리 시스템으로 지칭될 수도 있다.

[60] 네트워크 운영 관리 시스템(또는 보안 제어기)의 주요한 역할 중 하나는 I2NSF 사용자로부터의 고수준 보안 정책(또는 정책 규칙)을 특정 NSF(들)을 위한 저수준(low-level) 보안 정책 규칙으로 번역(translate)하는 것이다. 네트워크 운영 관리 시스템(또는 보안 제어기)은 고수준 보안 정책을 I2NSF 사용자로부터 수신한 후, 우선 I2NSF 사용자에 의해 요구되는 정책을 시행하기 위하여 요구되는 NSF(들)의 타입을 결정할 수 있다. 그리고, 네트워크 운영 관리 시스템(또는 보안 제어기)은 요구되는 각 NSF(들)을 위한 저수준(low-level) 보안 정책을 생성할 수 있다. 결국, 네트워크 운영 관리 시스템(또는 보안 제어기)는 생성된 저수준 보안 정책을 각 NSF(들)에게 설정할 수 있다.

[61] 또한, 네트워크 운영 관리 시스템(또는 보안 제어기)은 I2NSF 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, 네트워크 운영 관리 시스템(또는 보안 제어기)은 개발자 관리 시스템의 도움을 받아 NSF 인스턴스의 동적인 수명시간(life-cycle) 관리를 통해 NSF 인스턴스(instance)의 풀(pool)을 동적으로 관리할 수 있다.

[62] NSF

[63] NSF는 보안 관련 서비스를 제공하는 논리적 엔티티(logical entity) 또는 소프트웨어 컴포넌트이다. 예를 들면, NFC(예컨대, 방화벽)는 저수준 보안정책을 수신하고, 이에 기초하여 악의적인 네트워크 트래픽을 감지하고, 이를 차단하거나 완화할 수 있다. 이를 통해, 네트워크 통신 스트림의

무결성(integrity) 및 기밀성(confidentiality)이 보장될 수 있다.

[64] 개발자 관리 시스템

[65] 개발자 관리 시스템은 다른 I2NSF 컴포넌트(예컨대, 네트워크 운영 관리 시스템)으로 정보(예컨대, NSF의 정보)를 보내거나, 및/또는 보안 서비스(예컨대, 네트워크 보안 서비스)를 제공하는 I2NSF 컴포넌트이다. 개발자 관리 시스템은 벤더 관리 시스템(Vendor's Management System)으로 지칭될 수도 있다. 이러한 개발자 관리 시스템에 할당된 역할을 수행하는 대상은 I2NSF 생산자(producer)로 지칭될 수 있다.

[66] 개발자 관리 시스템은 네트워크 운영자에게 NSF(들)을 제공하는 제3자(third-party) 보안 벤더에 의해 관리될 수 있다. 다양한 보안 벤더의 다수의 개발자 관리 시스템(들)이 존재할 수 있다.

[67] I2NSF 소비자-직면 인터페이스(간단히, 소비자-직면 인터페이스(CFI))

[68] CFI는 I2NSF 사용자와 네트워크 운영 관리 시스템 사이에 위치하는, 사용자의 I2NSF 시스템으로의 인터페이스이다. 이렇게 설계됨으로써, I2NSF 시스템은 하위(underlying) NSF(들)의 상세한 내용을 숨기고, 사용자에게 NSF(들)의 추상적인 시각(abstract view)만을 제공할 수 있다.

[69] 이 CFI는 주어진 I2NSF 시스템의 상이한 사용자가 관리 도메인 내의 특정 흐름(flow)에 대한 보안 정책을 정의, 관리 및 모니터링할 수 있게 하기 위해 사용될 수 있다. I2NSF 사용자에 의해 생성된 고수준 보안 정책(또는 정책 규칙)은 이 CFI를 통해 네트워크 운영 관리 시스템으로 전달될 수 있다. 또한, NSF(들)에 의한 보안 경보(alert)는 이 CFI를 통해 네트워크 운영 관리 시스템으로부터 I2NSF 사용자로 전달될 수 있다.

[70] I2NSF NSF-직면 인터페이스(간단히, NSF-직면 인터페이스(NFI))

[71] NFI는 네트워크 운영 관리 시스템(또는 보안 제어기)과 NSF(들) 사이에 위치하는 인터페이스이다.

[72] 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, 보안 정책 규칙을 NSF에게 설정할 때, 네트워크 운영 관리 시스템은 벤더 특정한 차이 및/또는 NSF의 폼 팩터(form factor)를 고려할 필요가 없다. 이 NFI는 하나 이상의 NSF에 의해 시행되는 흐름-기반(flow-based) 보안 정책을 지정하고 모니터링하기 위해 사용될 수 있다. 예를 들면, 네트워크 운영 관리 시스템은 I2NSF 사용자에 의한 고수준 보안 정책을 시행하기 위하여 흐름-기반(flow-based) 보안 정책을 NFI 인터페이스를 통해, 각 흐름-기반 NSF에게 전달할 수 있다. 여기서, 흐름-기반 NSF는 보안 특성을 강화하기 위해 정책의 세트에 따라 네트워크 흐름을 검사하는 NSF이다. 이러한 흐름-기반 NSF에 의한 흐름-기반 보안은 수신된 순서대로 패킷들이 검사되고, 검사 프로세스에 따라 패킷에 대한 수정이 없는

것을 의미한다. 흐름-기반 NSF에 대한 인터페이스는 다음과 같이 분류될 수 있다:

[73] - NSF 운영 및 관리 인터페이스(NSF Operational and Administrative Interface): NSF의 운영 상태를 프로그래밍하기 위해 I2NSF 관리 시스템에 의해 사용되는 인터페이스 그룹; 이 인터페이스 그룹은 또한 관리 제어 기능을 포함한다. I2NSF 정책 규칙은 일관된 방식으로 이 인터페이스 그룹을 변경하는 한가지 방법을 나타낸다. 어플리케이션 및 I2NSF 컴포넌트가 그들이 송신 및 수신하는 트래픽의 동작을 동적으로 제어할 필요가 있기 때문에, I2NSF 노력(effort)의 대부분이 이 인터페이스 그룹에 집중된다.

[74] - 모니터링 인터페이스(Monitoring Interface): 하나 이상의 선택된 NSF로부터의 모니터링 정보를 획득하기 위해 I2NSF 관리 시스템에 의해 사용되는 인터페이스 그룹; 이 인터페이스 그룹의 각 인터페이스는 쿼리 또는 리포트 기반 인터페이스일 수 있다. 둘 사이의 차이점은 쿼리 기반 인터페이스는 정보를 획득하기 위해 I2NSF 관리 시스템에 의해 사용되고, 이에 반하여 리포트 기반 인터페이스는 정보를 제공하기 위해 NSF에 의해 사용된다는 것이다. 이 인터페이스 그룹의 기능은 또한 SYSLOG 및 DOTS와 같은 다른 프로토콜에 의해 정의될 수 있다. I2NSF 관리 시스템은 정보의 수신에 기초하여 하나 이상의 동작(action)을 취할 수 있다. 이는 I2NSF 정책 규칙에 의해 지정되어야 한다. 이 인터페이스 그룹은 NSF의 운영 상태를 변경하지 않는다.

[75] 이와 같이, NFI는 흐름-기반 패러다임을 사용하여 개발될 수 있다. 흐름-기반 NSF의 공동 특성(common trait)은 수신된 패킷의 컨텐츠(예컨대, 헤더/페이로드) 및/또는 컨텍스트(예컨대, 세션 상태 및 인증 상태)에 기초하여 패킷을 처리하는 것이다. 이 특징은 I2NSF 시스템의 동작을 정의하기 위한 요구사항(requirement) 중 하나이다.

[76] 한편, I2NSF 관리 시스템은 주어진 NSF의 모든 기능들을 사용할 필요가 없으며, 모든 사용 가능한 NSF들을 사용할 필요도 없다. 따라서, 이 추상화(abstraction)는 NSF 특징(feature)을 NSF 시스템에 의해 빌딩 블록(building block)으로 취급될 수 있게 해준다. 그러므로, 개발자는 벤더 및 기술에 독립적인 NSF에 의해 정의되는 보안 기능을 자유롭게 사용할 수 있게 된다.

[77] I2NSF 등록 인터페이스(간단히, 등록 인터페이스(RI))

[78] RI는 네트워크 운영 관리 시스템 및 개발자 관리 시스템 사이에 위치하는 인터페이스이다. 상이한 벤더에 의해 제공되는 NSF는 상이한 능력(capability)을 가질 수 있다. 따라서, 상이한 벤더에 의해 제공되는 여러 유형의 보안 능력을 이용하는 프로세스를 자동화하기 위해, 벤더가 그들의 NSF의 기능을 정의하기 위한 전용 인터페이스를 가질 필요가 있다. 이러한 전용 인터페이스는 I2NSF 등록 인터페이스(RI)로 지칭될 수 있다.

[79] NSF의 능력은 미리 구성되거나 또는 I2NSF 등록 인터페이스를 통해 동적으로 검색될 수 있다. 만일 소비자에게 노출되는 새로운 기능이 NSF에 추가된다면,

관심 있는(interested) 관리 및 제어 엔티티가 그것들을 알 수 있도록, 그 새로운 기능의 능력이 이 RI를 통해 I2NSF 레지스트리(registry)에 등록될 필요가 있다.

[80] 도 2는 본 발명의 다른 실시예에 따른 I2NSF 시스템의 아키텍처를 예시한다. 도 2의 I2NSF 시스템은 도 1의 I2NSF 시스템에 비하여 I2NSF 사용자 및 네트워크 운영 관리 시스템의 구성을 더 구체적으로 나타낸다. 도 2에서는 도 1에서 상술한 설명과 중복된 설명은 생략한다.

[81] 도 2를 참조하면, I2NSF 시스템은 I2NSF 사용자, 보안 관리 시스템(Security Management System), 및 NSF 인스턴스(instances) 계층을 포함한다. I2NSF 사용자 계층은 어플리케이션 로직(Application Logic), 정책 업데이터(Policy Updater), 및 이벤트 수집기(Event Collector)을 컴포넌트로서 포함한다. 보안 관리 시스템 계층은 보안 제어기 및 개발자 관리 시스템을 포함한다. 보안 관리 시스템 계층의 보안 제어기는 보안 정책 관리자(Security policy manager) 및 NSF 기능 관리자(NSF capability manager)를 컴포넌트로서 포함한다.

[82] I2NSF 사용자 계층은 소비자-직면 인터페이스를 통해 보안 관리 시스템 계층과 통신한다. 예를 들면, I2NSF 사용자 계층의 정책 업데이터 및 이벤트 수집기는 소비자-직면 인터페이스를 통해 보안 관리 시스템 계층의 보안 제어기와 통신한다. 또한, 보안 관리 시스템 계층은 NSF-직면 인터페이스를 통해 NFC 인스턴스 계층과 통신한다. 예를 들면, 보안 관리 시스템 계층의 보안 제어기는 NSF-직면 인터페이스를 통해 NFC 인스턴스 계층의 NSF 인스턴스(들)과 통신한다. 또한, 보안 관리 시스템 계층의 개발자 관리 시스템은 등록 인터페이스를 통해 보안 관리 시스템 계층의 보안 제어기와 통신한다.

[83] 도 2의 I2NSF 사용자 계층, 보안 관리 시스템 계층의 보안 제어기 컴포넌트, 보안 관리 시스템 계층의 개발자 관리 시스템 컴포넌트 및 NSF 인스턴스 계층은 각각 도 1의 I2NSF 사용자 컴포넌트, 네트워크 운영 관리 시스템 컴포넌트, 개발자 관리 시스템 컴포넌트 및 NSF 컴포넌트에 대응된다. 또한, 도 2의 소비자-직면 인터페이스, NSF-직면 인터페이스 및 등록 인터페이스는 도 1의 소비자-직면 인터페이스, NSF-직면 인터페이스 및 등록 인터페이스에 대응된다. 이하에서는, 각 계층에 포함된 새로 정의된 컴포넌트들에 대하여 설명한다.

[84] <u>I2NSF 사용자</u>

[85] 상술한 것처럼, I2NSF 사용자 계층은 다음 3 개의 컴포넌트를 포함한다: 어플리케이션 로직(Application Logic), 정책 업데이터(Policy Updater), 및 이벤트 수집기(Event Collector). 각각의 역할 및 동작을 설명하면 다음과 같다.

[86] 어플리케이션 로직은 고수준 보안 정책을 생성하는 컴포넌트이다. 이를 위해, 어플리케이션 로직은 이벤트 수집기로부터 고수준 정책을 업데이트(또는 생성)하기 위한 이벤트를 수신하고, 수집된 이벤트에 기초하여 고수준 정책을 업데이트(또는 생성)한다. 그 이후에, 고수준 정책은 보안 제어기로 배포하기 위해 정책 업데이터로 보내진다. 고수준 정책을 업데이트(또는 생성)하기 위해, 이벤트 수집기는 보안 수집기에 의해 보내진 이벤트를 수신하고, 그들을

어플리케이션 로직으로 보낸다. 이 피드백에 기초하여, 어플리케이션 로직은 고수준 보안 정책을 업데이트(또는 생성)할 수 있다.

[87] 도 2에서는, 어플리케이션 로직, 정책 업데이터 및 이벤트 수집기를 각각 별도의 구성으로 도시하고 있으나, 본 발명의 이에 한정되지 않는다. 다시 말해, 각각은 논리적인 컴포넌트로서, I2NSF 시스템에서 하나 또는 복수의 컴포넌트로 구현될 수도 있다. 예를 들면, 도 1과 같이 단일의 I2NSF 사용자 컴포넌트에 의해 구현될 수 있다.

[88] 보안 관리 시스템

[89] 상술한 것처럼, 보안 관리 시스템 계층의 보안 제어기는 다음 2개의 컴포넌트를 포함한다: 보안 정책 관리자(Security policy manager) 및 NSF 능력 관리자(NSF capability manager). 각각의 역할 및 동작을 설명하면 다음과 같다.

[90] 보안 정책 관리자는 CFI를 통해 정책 업데이터로부터 고수준 정책을 수신하고, 이 정책을 여러 저수준 정책으로 맵핑할 수 있다. 이 저수준 정책은 NSF 능력 관리자에 등록된 주어진 NSF 능력과 관련된다. 또한, 보안 정책 관리자는 이 정책을 NFI를 통해 NSF(들)로 전달할 수 있다.

[91] NSF 능력 관리자는 주어진 NSF 능력과 관련된 저수준 정책을 생성하기 위해, 개발자 관리 시스템에 의해 등록된 NSF의 능력을 지정하고, 그것을 보안 정책 관리자와 공유할 수 있다. 새로운 NSF가 등록될 때마다, NSF 능력 관리자는 등록 인터페이스를 통해 NSF 능력 관리자의 관리 테이블에 NSF의 기능/능력을 등록하도록 개발자 관리 시스템에 요청할 수 있다. 개발자 관리 시스템은 새로운 NSF의 능력을 NSF 능력 관리자로 등록하기 위한 보안 관리 시스템의 다른 부분에 해당한다.

[92] 도 2에서는, 보안 정책 관리자 및 NSF 능력 관리자를 각각 별도의 구성으로 도시하고 있으나, 본 발명의 이에 한정되지 않는다. 다시 말해, 각각은 논리적인 컴포넌트로서, I2NSF 시스템에서 하나의 컴포넌트로 구현될 수도 있다.

[93] NSF 인스턴스(NSF Instances)

[94] 도 2에 도시된 것처럼, NSF 인스턴스 계층은 NSF들을 포함한다. 이때, 모든 NSF들은 이 NSF 인스턴스 계층에 위치된다. 한편, 고수준 정책을 저수준 정책에 맵핑한 후에, 보안 정책 관리자는 NFI를 통해 정책을 NSF(들)로 전달한다. 이 경우, NFC는 수신된 저수준 보안 정책에 기초하여 악의적인 네트워크 트래픽을 감지하고, 이를 차단하거나 완화할 수 있다.

[95]

[96] 능력 정보 모델(Capability Information Model)

[97] 이하에서는, 보안 제어기(Security Controller)와 개발자 관리 시스템(Developer's Management System)간 I2NSF 등록 인터페이스에 대한 능력 정보 모델을 설명한다. 능력 정보 모델은 등록 인터페이스를 통해 NSF 인스턴스(instance) 생성, 등록 및 삭제 요청을 지원해야 한다. 본 명세서에서는 이러한 기능을 위한 I2NSF 등록 인터페이스를 통한 절차를 설명한다. 또한, I2NSF 등록

인터페이스를 통해 교환하는 구체적인 정보를 설명한다.

[98] 다수의 가상 NSF 인스턴스는 일반적으로 I2NSF 프레임 워크에 존재한다. 이러한 NSF 인스턴스는 서로 다른 보안 기능을 가질 수 있기 때문에, 각각의 NSF 인스턴스의 보안 기능을 생성된 이후 보안 제어기에 등록하는 것이 중요하다. 또한, 필요시 일부 보안 기능의 NSF를 인스턴스화 해야 한다. 예를 들어, I2NSF 사용자가 요구하는 새로운 보안 요구 사항을 충족하기 위해 추가 보안 기능이 필요한 경우, 보안 제어기는 필요한 보안 기능이 있는 NSF를 인스턴스화 하도록 개발자 관리 시스템에 요청할 수 있어야 한다.

[99] 본 발명에서는, NSF 등록 및 인스턴스화를 지원하기 위하여 보안 제어기와 개발자 관리 시스템간 등록 인터페이스에 필요한 능력 정보 모델을 제안한다.

[100] 또한, 본 발명에서는, 등록 인터페이스를 통해 보안 제어기와 개발자 관리 시스템에 의해 수행되는 능력 정보 모델에 기반한 절차를 제안한다.

[101] 기존의 I2NSF 등록 인터페이스는 보안 제어기에 새로운 NSF 인스턴스를 등록하는 경우에 한하여 사용되었다. 반면에, 본 발명에서는 필요한 경우 NSF 인스턴스화(instantiation)/역인스턴스화(deinstantiation)를 지원하기 위해 그 활용도를 확장하고 기능을 위하여 등록 인터페이스를 통해 교환되어야 하는 정보를 제안한다. 또한, 본 발명에서는, 등록 인터페이스의 경우 NSF 능력 정보(즉, NSF의 능력)을 명확히하여 I2NSF 프레임 워크의 구성 요소가 능력들의 세트를 표준화된 방식으로 교환할 수 있어야 하기 때문에, 이를 위한 NSF 능력 정보 모델을 정의한다.

[102] 본 명세서에서, NSF(Network Security Function)는 수신된 패킷의 특정 처리를 담당하는 기능을 말한다. NSF는 프로토콜 스택의 다양한 계층(예를 들어, 네트워크 계층 또는 다른 개방형 시스템간 상호 접속(OSI: Open System Interconnection) 계층)에서 작동할 수 있다.

[103] 또한, 본 명세서에서, NSF(또는 네트워크 보안 서비스 기능)은, 예를 들어, 방화벽, 침입 방지 시스템/침입 탐지 시스템(IPS: Intrusion Prevention System/IDS: Intrusion Detection System), 딥 패킷 검사(DPI: Deep Packet Inspection), 어플리케이션 가시성 및 제어(AVC: Application Visibility and Control), 네트워크 바이러스 및 맬웨어 검사(malware scanning), 샌드 박스(sandbox), 데이터 손실 방지(DLP: Data Loss Prevention)), 디도스(DDoS: Distributed Denial of Service) 완화(mitigation) 및 전송 계층 보안(TLS: Transport Layer Security) 프록시(proxy)와 같은 서비스를 나타낼(또는 제공할) 수 있다.

[104] 또한, 본 명세서에서, 고급 검사/조치(Advanced Inspection/Action)는 NSF 직면 인터페이스에 대한 I2NSF 정보 모델과 마찬가지로, 보안 기능이 자체 검사 결과에 기반하여 추가 검사를 위해 다른 보안 기능을 호출함을 나타낼 수 있다.

[105] 또한, 본 명세서에서, NSF 능력 정보 모델은 NSF 인스턴스의 보안 능력 및 수행 능력을 나타낸다. 각각의 NSF 인스턴스에는 제공할 수 있는 보안 서비스의 유형과 수행 능력을 나타내는 자체 NSF 능력 정보 모델을 가진다.

[106] 본 발명의 일 실시예에서, 보안 제어기와 개발자 관리 시스템간 등록 인터페이스를 통해 NSF 인스턴스를 등록할 수 있다.

[107] 도 3은 본 발명이 적용되는 실시예로서, 등록 인터페이스를 통해 NSF 인스턴스를 등록하는 방법을 나타내는 흐름도이다.

[108] 도 3을 참조하면, 보안 제어기는 인스턴스화 요청 메시지를 개발자 관리 시스템으로 전송한다(S301). 보안 제어기 및 개발자 관리 시스템은 앞서 도 2에서 설명한 I2NSF 프레임 워크의 구성 요소를 나타낸다.

[109] 보안 제어기로부터 인스턴스화 요청 메시치를 수신하면, 개발자 관리 시스템은 해당 NSF 인스턴스를 생성할 수 있다. 예를 들어, S301 단계에 앞서, 보안 제어기는 현재 시스템에서 필요한 능력들 세트(즉, NSF 능력 정보) 또는 특정 NSF의 서명을 인식할 수 있다. 그리고, 보안 제어기는 인식된 정보를 포함하는 인스턴스화 요청 메시지를 개발자 관리 시스템으로 전송할 수 있다. 개발자 관리 시스템은 수신된 정보를 능력 정보 모델 정의에 기반한 NSF와 일치시키고, 상기 수신된 정보와 일치하는 NSF 인스턴스를 생성할 수 있다.

[110] 또는, 보안 제어기는 역인스턴스화 요청 메시지를 개발자 관리 시스템으로 전송할 수 있다. 보안 제어기로부터 역인스턴스화 요청 메시지를 수신하면, 개발자 관리 시스템은 해당 NSF 인스턴스를 제거할 수 있다.

[111] 예를 들어, 예를 들어, S301 단계에 앞서, 보안 제어기는 현재 시스템에서 불필요한 능력들 세트(즉, NSF 능력 정보) 또는 특정 NSF의 서명을 인식할 수 있다. 보안 제어기는 인식된 정보를 포함하는 역인스턴스화 요청 메시지를 개발자 관리 시스템으로 전송할 수 있다. 개발자 관리 시스템은 수신된 정보를 능력 정보 모델 정의에 기반한 NSF와 일치시키고, 상기 수신된 정보와 일치하는 NSF 인스턴스를 제거할 수 있다.

[112] 보안 제어기는 NSF 인스턴스의 등록을 위한 등록 메시지를 개발자 관리 시스템으로부터 수신한다(S302). 이 경우, 보안 제어기는 등록 메시지를 수신한 후 해당 NSF 인스턴스를 시스템의 사용 가능한 NSF 인스턴스 목록에 추가할 수 있다.

[113] 만약 S301 단계에서 보안 제어기가 인스턴스화 요청 메시지가 아닌 역인스턴스화 요청 메시지를 전송한 경우, 보안 제어기는 개발자 관리 시스템으로부터 삭제 메시지를 수신할 수 있다. 이 경우, 보안 제어기는 해당 NSF 인스턴스를 시스템의 사용 가능한 NSF 인스턴스 목록에서 제거할 수 있다.

[114] 또한, 일 실시예에서, 개발자 관리 시스템은 NSF 인스턴스를 등록할 수 있다. 구체적으로, 시스템의 보안 요구 사항에 따라 일부 NSF가 기본적으로 요구될 수 있다. 이 경우, 개발자 관리 시스템은 보안 제어기의 요청 없이 이러한 기본 NSF 인스턴스를 생성할 수 있다. 개발자 관리 시스템은 NSF 인스턴스들을 생성한 후, 등록 인터페이스를 통해 보안 제어기에 NSF 인스턴스(또는 NSF 인스턴스에 관련된 정보)를 통지할 수 있다.

[115] 또한, 일 실시예에서, 등록 인터페이스를 통해 다른 NSF에 의해 트리거된 고급

검사/조치를 제공하는 NSF 인스턴스가 생성될 수 있다. 즉, I2NSF 프레임 워크에서 NSF는 트래픽(traffic)의 고급 보안 검사를 위하여 다른 유형의 NSF를 트리거할 수 있다. 이때, 다음 NSF는 현재 NSF의 검사 결과 및 I2NSF 사용자 정책에 의해 결정될 수 있다. 그러나, 만약 이전 NSF에 의해 트리거된 고급 검사/조치를 제공할 수 있는 NSF 인스턴스가 없는 경우, 보안 제어기는 등록 인터페이스를 통해 개발자 관리 시스템에 요청하여 NSF 인스턴스를 생성할 수 있다.

[116] 또한, 일 실시예에서, I2NSF 사용자로부터 수신된 보안 정책 규칙을 시행함에 있어서 필요한 NSF 인스턴스가 생성될 수 있다. 즉, I2NSF 프레임 워크에서 I2NSF 사용자는 시스템에 필요한 보안 서비스를 결정할 수 있다. 만약 I2NSF 사용자가 요청한 보안 정책을 시행할 NSF 인스턴스가 없는 경우, 보안 제어기는 등록 인터페이스를 통해 개발자 관리 시스템에 요청하여 필요한 NSF 인스턴스를 생성할 수 있다.

[117] 또한, 일 실시예에서, 더 이상 필요하지 않은 NSF 인스턴스는 삭제될 수 있다. 다양한 유형의 NSF 인스턴스가 I2NSF 프레임 워크에서 실행될 수 있고, 시스템에서 수행될 보안 정책의 동적 변경에 따라 일부 유형의 NSF 인스턴스가 더 이상 필요하지 않을 수 있다. 이 경우, 보안 제어기는 등록 인터페이스를 통해 NSF 인스턴스를 파기하도록 개발자 관리 시스템에 요청할 수 있다.

[118] 도 4는 본 발명의 일 실시예에 따른 등록 인터페이스의 정보 모델을 예시하는 도면이다.

[119] 도 4를 참조하면, 등록 인터페이스의 정보 모델은 인스턴스 관리 서브 모델(또는 하위 모델) 및/또는 등록 서브 모델을 포함할 수 있다. 인스턴스 관리 기능 및 등록 기능은 목적 달성을 위하여 NSF 능력 정보 모델이 사용될 수 있다. 여기서, NSF 능력 정보 모델은 NSF 인스턴스가 제공할 수 있는 검사 능력을 설명 및/또는 규정하는 능력 객체를 나타낸다.

[120] 즉, 등록 인터페이스 정보 모델 중에서 인스턴스 관리 서브 모델을 통해 NSF 인스턴스가 생성/제거될 수 있고, 등록 서브 모델에서 NSF 능력 정보 모델을 구성하는 세부 정보들이 정의될 수 있다.

[121]

[122] NSF 인스턴스 관리 메커니즘(Instance Management Mechanism)

[123] 도 5는 본 발명의 일 실시예에 따른 인스턴스 관리 서브 모델(Instance Management Sub-Model)을 예시하는 도면이다.

[124] 도 5를 참조하면, I2NSF 프레임 워크의 보안 제어기는 NSF의 인스턴스 관리를 위해 인스턴스화 요청 및/또는 역인스턴스화(Deinstantiation) 요청을 수행할 수 있다.

[125] 도 5(a)를 참조하면, 보안 제어기는 필요한 경우 개발자 제어 시스템에 인스턴스화 요청 메시지를 전송할 수 있다. 보안 제어기로부터 요청을 수신한 개발자 제어 시스템은 NSF 능력 정보에 기반하여 해당 NSF 인스턴스를

생성하고 보안 제어기에 처리 결과에 관련된 정보를 포함하는 응답 메시지를 전송할 수 있다.

[126] 도 5(b)를 참조하면, 보안 제어기는 필요한 경우 개발자 제어 시스템에 역인스턴스화 요청 메시지를 전송할 수 있다. 보안 제어기로부터 요청을 수신한 개발자 제어 시스템은 NSF 접근 정보에 기반하여 해당 NSF 인스턴스를 제거하고 보안 제어기에 처리 결과에 관련된 정보를 포함하는 응답 메시지를 전송할 수 있다.

[127]

[128] NSF 등록 메커니즘(Registration Mechanism)

[129] 도 6은 본 발명의 일 실시예에 따른 등록 서브 모델(Registration Sub-Model)을 예시하는 도면이다.

[130] 도 6을 참조하면, 개발자 관리 시스템은 새로운 NSF 인스턴스를 등록하기 위하여 보안 제어기에 등록 메시지를 전송(또는 생성)할 수 있다. 이때, 상기 등록 메시지는 NSF 능력 정보(Capability Information) 및 NSF 접근 정보(Access Information) 를 포함할 수 있다.

[131] NSF 능력 정보는 새로운 NSF 인스턴스의 검사 능력을 나타낸다. 그리고, NSF 접근 정보는 다른 구성 요소의 새로운 인스턴스에 대한 네트워크 접근을 가능하게 하는 정보를 나타낸다. NSF 능력 정보와 NSF 접근 정보의 세부 정보 모델은 자세히 후술한다.

[132] 위와 같은 등록 프로세스 이후, I2NSF 능력 인터페이스(capability interface)는 새롭게 등록된 NSF 인스턴스를 제어하고 모니터링할 수 있다.

[133]

[134] NSF 접근 정보(Access Information)

[135] NSF 접근 정보는 NSF와 통신을 수행하기 위하여 요구되는 정보를 나타낸다. 본 발명의 일 실시예에서, NSF 접근 정보는 IPv4(Internet Protocol version 4) 주소(address), IPv6(Internet Protocol version 6) 주소, 포트 번호(port number) 및/또는 지원되는 전송 프로토콜(transport protocol)을 포함할 수 있다.

[136] 여기서 지원되는 전송 프로토콜은, 예를 들어, 가상 확장(Virtual Extensible) LAN(VXLAN), VXLAN를 위한 일반 프로토콜 확장(VXLAN-GPE(Generic Protocol Extension)), 일반 경로 캡슐화(GRE: Generic Route Encapsulation), 이더넷(Ethernet) 등을 포함할 수 있다.

[137] NSF 접근 정보는 전반적인 시스템(또는 NSF 인스턴스 리스트) 내에서 NSF 인스턴스의 서명(또는 고유 식별자)를 나타낸다. NSF 접근 정보는 특정 NSF 인스턴스를 식별하는 데 사용될 수 있다.

[138]

[139] NSF 능력 정보(Capability Information)

[140] 도 7은 본 발명의 일 실시예에 따른, NSF 능력 정보(Capability Information)를 개략적으로 나타내는 도면이다.

[141] 도 7을 참조하면, NSF 인스턴스의 보안 능력을 나타내는 NSF 능력 정보는 다양한 NSF 인스턴스의 능력 객체 (capability object)들을 포함할 수 있다.

[142] 구체적으로, NSF 능력 정보(또는 능력 객체)는 네트워크 보안 능력(Network-Security Capabilities), 컨텐츠 보안 능력(Content-Security Capabilities), 공격 완화 능력(Attack Mitigation Capabilities), 수행 능력(performance capabilities)을 포함할 수 있다.

[143] 네트워크 보안 능력은 미리 정의된 보안 정책을 사용하여 네트워크 트래픽을 검사하고 처리하는 능력을 나타낸다. 컨텐츠 보안 능력 어플리케이션(application) 레이어에서 전달되는 트래픽 내용을 분석하는 능력을 나타낸다. 또한, 공격 완화 능력은 다양한 유형의 네트워크 공격을 탐지하고 완화하는 능력을 나타낸다.

[144] 수행 능력과 역할 기반 ACL은 이하에서 상세히 설명한다.

[145]

[146] 수행 능력(Performance Capabilities)

[147] 도 8은 본 발명의 일 실시예에 따른, 수행 능력(Performance Capabilities) 정보를 개략적으로 나타내는 도면이다.

[148] 도 8을 참조하면, 수행 능력 정보는 처리(Processing) 및/또는 대역폭(Bandwidth) 필드(또는 정보)를 포함할 수 있다. 여기서, 수행 능력 정보는 NSF의 처리 능력(processing capability)을 나타낸다.

[149] 수행 능력 정보는 NSF가 현재 담당하는 작업량(workload)과 해당 정보의 비교를 통해 NSF가 정체(congestion) 상태인지 여부를 결정하는 데 사용될 수 있다. 또한, 수행 능력 정보는 NSF에서 이용 가능한 능력과 같은 각각의 유형의 자원의 이용 가능한 양을 지정하는 데 사용될 수 있다.

[150] 또한, 처리 정보는 NSF의 사용 가능한 처리 능력(processing power)를 나타낸다. 대역폭은 아웃 바운드(outbound), 인바운드(inbound)의 두 가지 경우에 사용 가능한 네트워크 양에 대한 정보를 나타낸다. 처리 정보 및 대역폭 정보는 보안 제어기에 의한 NSF의 인스턴스(또는 인스턴스화) 요청에 사용될 수 있다.

[151] 본 명세서 제안하는 등록 인터페이스는 생성된 인스턴스의 사용 및 제한을 제어할 수 있으며, 상태(status)에 따라 적절한 요청을 수행할 수 있다.

[152]

[153] 역할 기반 ACL(Role-based Access Control List)

[154] 역할 기반 ACL 정보는 엔티티(entity)에 부여된 역할에 따라 NSF에 대한 엔티티 접근을 허용할지 또는 거부할지 결정하기 위하여 NSF의 접근 정책을 지정할 수 있다. 각각의 NSF는 역할 기반 ACL과 연결되어 엔티티의 접근 요청을 허용할지 또는 거부할지 결정할 수 있다.

[155] 도 9 및 도 10은 본 발명의 일 실시예에 따른 역할 기반 ACL(Role-based Access Control List)을 예시하는 도면이다.

[156] 도 9를 참조하면, 역할 기반 ACL는 하나 이상의 역할 ID를 포함할 수 있다.

여기서, 역할 ID는 엔티티(예: 관리자, 개발자 등)의 역할을 식별하는데 이용되는 정보를 나타낸다.

[157] 도 10을 참조하면, 역할 기반 ACL에 포함되는 각각의 역할 ID는 허용/거부로 분류되는 접근 유형들을 포함할 수 있다. 즉, 역할 기반 ACL은 각각의 역할 ID에서 허용되거나 거부되는 접근 유형들의 집합으로 구성될 수 있다. 여기서, 접근 유형은 NSF 규칙(rule) 구성(configuration), NSF 규칙 업데이트(update) 및/또는 NSF 모니터링(monitoring)과 같은 특정 유형의 접근 요청을 식별하는데 사용될 수 있다.

[158] 본 명세서에서 제안하는 등록 인터페이스의 정보 모델은 아키텍처 변경없이 I2NSF 프레임 워크를 기반으로 할 수 있다. 따라서, 이 문서는 제안된 아키텍처에서 컴포넌트 간 안전한 통신을 달성하기 위하여 상술한 IETF 드래프트 문서(예컨대, rfc8329.txt)에서 명시된 I2NSF 프레임 워크의 보안 고려 사항을 공유할 수 있다.

[159] 도 11는 본 발명의 일 실시예에 따른 네트워크 장치의 블록 구성도를 예시한다. 네트워크 장치는 상술한 I2NSF 시스템(또는 보안 관리 시스템)에 해당하거나, I2NSF 시스템 내에 포함되는 장치일 수 있다. I2NSF 시스템 내에 포함되는 장치의 예로는 상술한 I2NSF, 보안 제어기, 개발자 관리 시스템, NSF 등이 포함될 수 있다.

[160] 도 11을 참조하면, 네트워크 장치(1100)는 프로세서(processor, 1110), 메모리(memory, 1120) 및 통신 모듈(communication module, 1130)을 포함한다.

[161] 프로세서(1110)는 앞서 도 1 내지 도 10에서 제안된 기능, 과정 및/또는 방법을 구현한다. 메모리(1120)는 프로세서(1110)와 연결되어, 프로세서(1110)를 구동하기 위한 다양한 정보를 저장한다. 통신 모듈(1130)은 프로세서(1110)와 연결되어, 유/무선 신호를 송신 및/또는 수신한다.

[162] 메모리(1120)는 프로세서(1110) 내부 또는 외부에 있을 수 있고, 잘 알려진 다양한 수단으로 프로세서(1110)와 연결될 수 있다.

[163] 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.

[164] 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.

[165] 또한, 펌웨어나 소프트웨어에 의한 구현의 경우, 본 발명의 일 실시예는 이상에서 설명된 기능 또는 동작들을 수행하는 모듈, 절차, 함수 등의 형태로 구현되어, 다양한 컴퓨터 수단을 통하여 판독 가능한 기록매체에 기록될 수 있다. 여기서, 기록매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 기록매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 예컨대 기록매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함한다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 이러한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[166] 아울러, 본 발명에 따른 장치나 단말은 하나 이상의 프로세서로 하여금 앞서 설명한 기능들과 프로세스를 수행하도록 하는 명령에 의하여 구동될 수 있다. 예를 들어 그러한 명령으로는, 예컨대 JavaScript나 ECMAScript 명령 등의 스크립트 명령과 같은 해석되는 명령이나 실행 가능한 코드 혹은 컴퓨터로 판독 가능한 매체에 저장되는 기타의 명령이 포함될 수 있다. 나아가 본 발명에 따른 장치는 서버 팜(Server Farm)과 같이 네트워크에 걸쳐서 분산형으로 구현될 수 있으며, 혹은 단일의 컴퓨터 장치에서 구현될 수도 있다.

[167] 또한, 본 발명에 따른 장치에 탑재되고 본 발명에 따른 방법을 실행하는 컴퓨터 프로그램(프로그램, 소프트웨어, 소프트웨어 어플리케이션, 스크립트 혹은 코드로도 알려져 있음)은 컴파일 되거나 해석된 언어나 선험적 혹은 절차적 언어를 포함하는 프로그래밍 언어의 어떠한 형태로도 작성될 수 있으며, 독립형 프로그램이나 모듈, 컴포넌트, 서브루틴 혹은 컴퓨터 환경에서 사용하기에 적합한 다른 유닛을 포함하여 어떠한 형태로도 전개될 수 있다. 컴퓨터 프로그램은 파일 시스템의 파일에 반드시 대응하는 것은 아니다. 프로그램은 요청된 프로그램에 제공되는 단일 파일 내에, 혹은 다중의 상호 작용하는 파일(예컨대, 하나 이상의 모듈, 하위 프로그램 혹은 코드의 일부를 저장하는

파일) 내에, 혹은 다른 프로그램이나 데이터를 보유하는 파일의 일부(예컨대, 마크업 언어 문서 내에 저장되는 하나 이상의 스크립트) 내에 저장될 수 있다. 컴퓨터 프로그램은 하나의 사이트에 위치하거나 복수의 사이트에 걸쳐서 분산되어 통신 네트워크에 의해 상호 접속된 다중 컴퓨터나 하나의 컴퓨터 상에서 실행되도록 전개될 수 있다.

[168] 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.

[169]

산업상 이용가능성

[170] 이상, 전술한 본 발명의 바람직한 실시예는, 예시의 목적을 위해 개시된 것으로, 당업자라면 이하 첨부된 특허청구범위에 개시된 본 발명의 기술적 사상과 그 기술적 범위 내에서, 다양한 다른 실시예들을 개량, 변경, 대체 또는 부가 등이 가능할 것이다.

청구범위

[청구항 1] 등록 인터페이스(Registration Interface)를 통해 네트워크 보안 기능(NSF: Network Secure Function)을 관리하는 보안 관리 시스템에서, 보안 제어기(Security Controller)에 의해 수행되는 방법은,
상기 보안 관리 시스템에서 필요한 NSF에 대한 인스턴스화(instantiation) 요청 메시지를 개발자 관리 시스템(Developer's Management System)으로 전송하는 단계; 및
상기 요청 메시지에 대한 응답으로 상기 필요한 NSF에 대한 NSF 인스턴스의 등록을 지시하는 등록 메시지를 상기 개발자 관리 시스템으로부터 수신하는 단계를 포함하는 방법.

[청구항 2] 제1 항에 있어서,
상기 보안 관리 시스템에서 필요한 NSF의 능력 정보(Capability Information) 또는 서명(signature)을 인식하는 단계를 더 포함하고,
상기 인스턴스화 요청 메시지는 상기 능력 정보 또는 상기 서명을 포함하는 방법.

[청구항 3] 제1 항에 있어서,
상기 NSF 인스턴스는 상기 인스턴스화 요청 메시지에 기초하여 개발자 관리 시스템에 의해 생성되는 방법.

[청구항 4] 제1 항에 있어서,
상기 보안 관리 시스템에서 불필요한 NSF에 대한 역인스턴스화(de-instantiation) 요청 메시지를 개발자 관리 시스템으로 전송하는 단계를 더 포함하고,
상기 역인스턴스화 요청 메시지에 대응되는 NSF 인스턴스가 상기 개발자 관리 시스템에 의해 삭제되는 방법.

[청구항 5] 제1 항에 있어서,
상기 등록 메시지는 NSF 인스턴스의 보안 능력을 나타내는 NSF 능력 정보(Capability Information) 또는 새로운 인스턴스에 대한 네트워크 접근을 위해 이용되는 NSF 접근 정보(Access Information) 중 적어도 하나를 포함하는 방법.

[청구항 6] 제5 항에 있어서,
상기 NSF 접근 정보는 IPv4(Internet Protocol version 4) 주소(address), IPv6(Internet Protocol version 6) 주소, 포트 번호(port number) 또는 지원되는 전송 프로토콜(transport protocol) 중 적어도 하나를 포함하는 방법.

[청구항 7] 제6 항에 있어서,
상기 지원되는 전송 프로토콜은 가상 확장(Virtual Extensible) LAN(VXLAN), VXLAN를 위한 일반 프로토콜 확장(VXLAN-GPE(Generic

Protocol Extension)), 일반 경로 캡슐화(GRE: Generic Route Encapsulation) 또는 이더넷(Ethernet) 중 적어도 하나를 포함하는 방법.

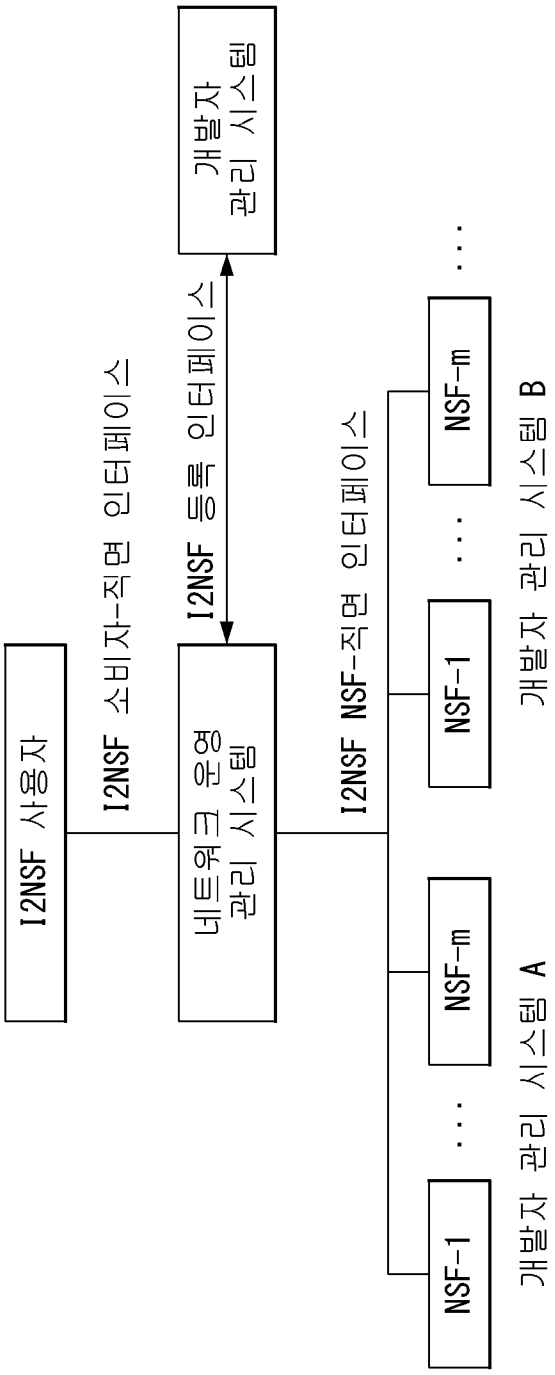
[청구항 8] 제5 항에 있어서,
상기 NSF 능력 정보는 네트워크 보안 능력(Network-Security Capabilities), 컨텐츠 보안 능력(Content-Security Capabilities), 공격 완화 능력(Attack Mitigation Capabilities), 수행 능력(performance capabilities) 중 적어도 하나를 포함하는 방법.

[청구항 9] 제8 항에 있어서,
상기 수행 능력은 처리(Processing) 및 대역폭(Bandwidth) 정보를 포함하는 방법.

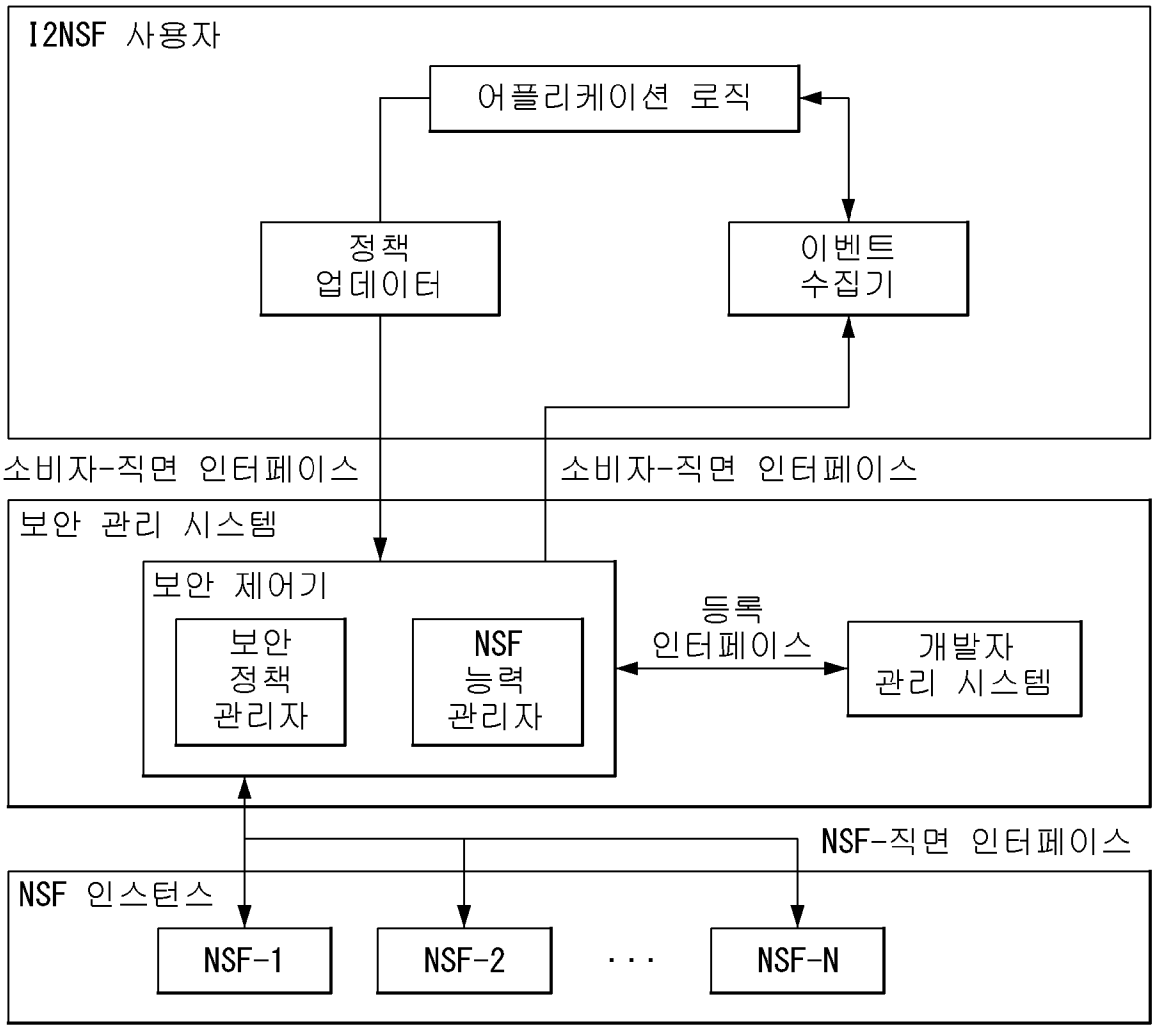
[청구항 10] 제8 항에 있어서,
상기 역할 기반 접근 제어 리스트는 엔티티의 역할 식별에 이용되는 하나 이상의 역할 ID를 포함하고,
상기 역할 ID는 특정 유형의 접근 요청을 식별하는데 사용되는 하나 이상의 접근 유형을 포함하는 방법.

[청구항 11] 등록 인터페이스(Registration Interface)를 통해 네트워크 보안 기능(NSF: Network Secure Function)을 관리하는 보안 제어기(Security Controller)에 있어서,
외부 장치와 무선 또는 유선으로 통신하기 위한 통신부; 및
상기 통신부와 기능적으로 연결되는 프로세서를 포함하되, 상기 프로세서는,
상기 보안 관리 시스템에서 필요한 NSF에 대한 인스턴스화(instantiation) 요청 메시지를 개발자 관리 시스템(Developer's Management System)으로 전송하고, 및
상기 요청 메시지에 대한 응답으로 상기 필요한 NSF에 대한 NSF 인스턴스의 등록을 지시하는 등록 메시지를 상기 개발자 관리 시스템으로부터 수신하는 장치.

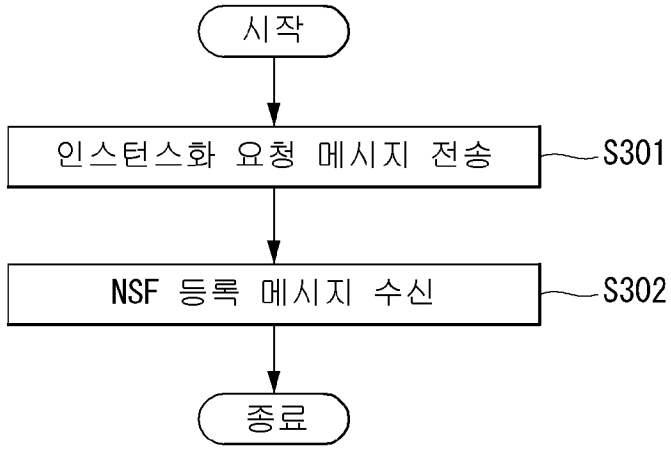
[도1]


I2NSF 사용자
I2NSF 소비자-직면 인터페이스
네트워크 운영 관리 시스템
I2NSF 등록 인터페이스
개발자 관리 시스템
I2NSF NSF-직면 인터페이스
NSF-1
NSF-m
...
개발자 관리 시스템 A
NSF-1
NSF-m
...
개발자 관리 시스템 B

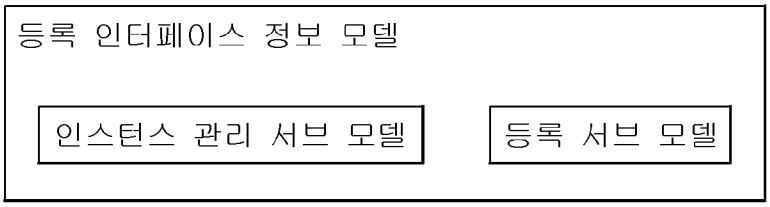
[도2]


I2NSF 사용자
어플리케이션 로직
정책
업데이터
이벤트
수집기
소비자-직면 인터페이스
소비자-직면 인터페이스
보안 관리 시스템
보안 제어기
보안
정책
관리자
NSF
능력
관리자
등록
인터페이스
개발자
관리 시스템
NSF-직면 인터페이스
NSF 인스턴스
NSF-1
NSF-2
· · ·
NSF-N

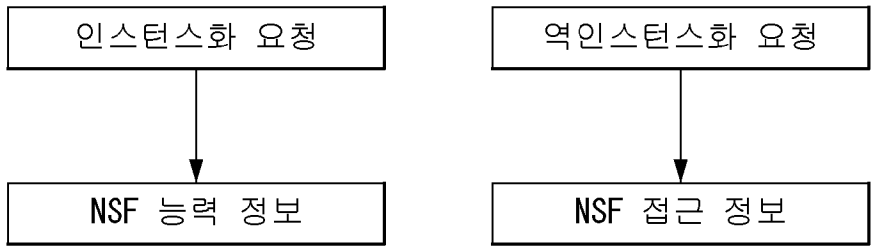
[도3]


시작
인스턴스화 요청 메시지 전송
S301
NSF 등록 메시지 수신
S302
종료

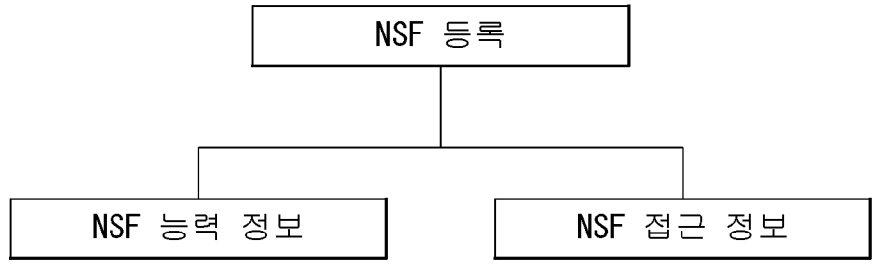
[도4]


등록 인터페이스 정보 모델
인스턴스 관리 서브 모델
등록 서브 모델

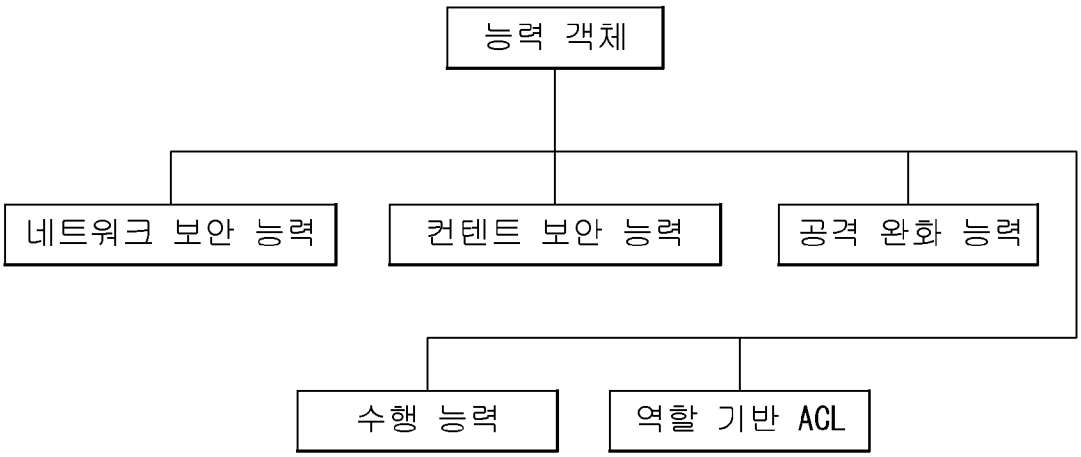
[도5]


인스턴스화 요청
NSF 능력 정보
역인스턴스화 요청
NSF 접근 정보
(a)
(b)

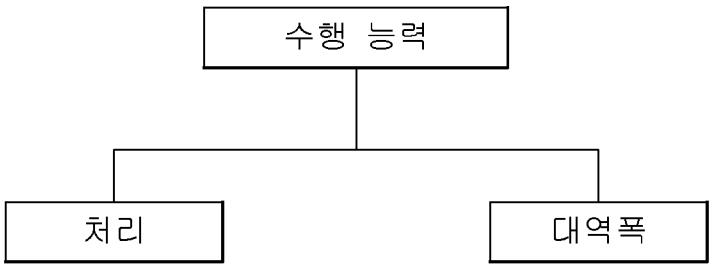
[도6]


NSF 등록
NSF 능력 정보
NSF 접근 정보

[도7]


능력 객체
네트워크 보안 능력
컨텐트 보안 능력
공격 완화 능력
수행 능력
역할 기반 ACL

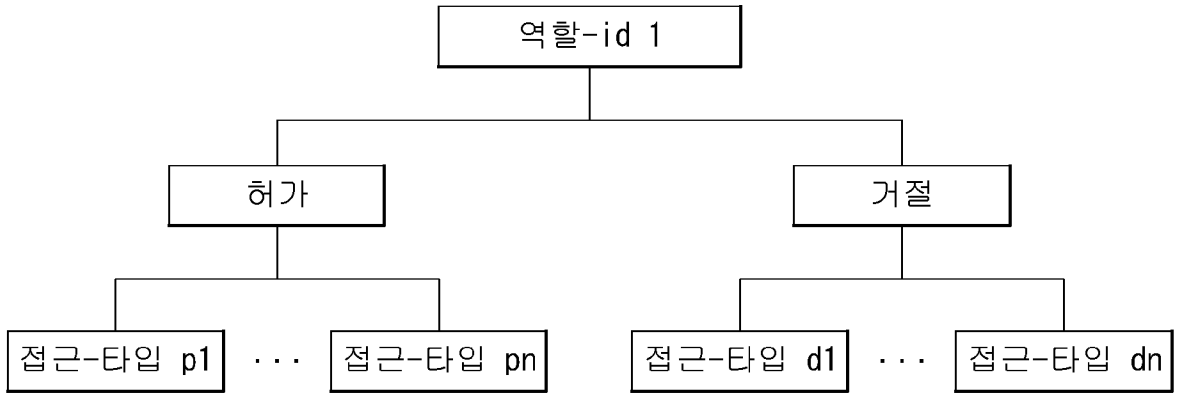
[도8]


수행 능력
처리
대역폭

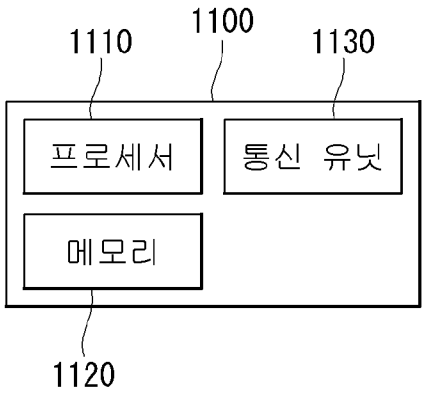
[도9]


역할 기반 ACL
역할-id 1
· · ·
역할-id N

[도10]


역할-id 1
허가
거절
접근-타입 p1
· · ·
접근-타입 pn
접근-타입 d1
· · ·
접근-타입 dn

[도11]


1110
1100
1130
프로세서
통신 유닛
메모리
1120

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2018/002954

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; G06F 15/173; G06F 9/445; H04M 7/00; G06F 15/167; G06F 21/00; H04L 12/24

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, function, management, instantiation, request, message, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010-0217850 A1 (FERRIS, James Michael) 26 August 2010 See paragraphs [0013], [0035]; and figures 1, 4.	1-11
A	US 2016-0226835 A1 (BLACKROCK FINANCIAL MANAGEMENT, INC.) 04 August 2016 See paragraphs [0016]-[0082]; and figures 1-7.	1-11
A	US 2017-0012968 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 12 January 2017 See paragraphs [0122]-[0650]; and figures 1-5.	1-11
A	US 2004-0042609 A1 (DELANEY, Robert J. et al.) 04 March 2004 See paragraphs [0029]-[0059]; and figures 2-7.	1-11
A	US 2015-0207813 A1 (VORSTACK, INC.) 23 July 2015 See paragraphs [0036]-[0048]; and figures 1-4B.	1-11

☐ 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
21 JUNE 2018 (21.06.2018)	**21 JUNE 2018 (21.06.2018)**

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.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2018/002954

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2010-0217850 A1	26/08/2010	US 8977750 B2	10/03/2015
US 2016-0226835 A1	04/08/2016	US 2016-0226718 A1	04/08/2016
		US 2017-0257280 A1	07/09/2017
		US 2017-0257282 A1	07/09/2017
		US 2017-0272332 A1	21/09/2017
		US 9705752 B2	11/07/2017
		US 9712398 B2	18/07/2017
US 2017-0012968 A1	12/01/2017	CN 105122738 A	02/12/2015
		EP 3107246 A1	21/12/2016
		EP 3107246 A4	12/04/2017
		WO 2015-143651 A1	01/10/2015
US 2004-0042609 A1	04/03/2004	AU 2003-268466 A1	29/03/2004
		US 7043000 B2	09/05/2006
		WO 2004-023775 A1	18/03/2004
US 2015-0207813 A1	23/07/2015	US 2015-0222656 A1	06/08/2015
		US 2016-0164890 A1	09/06/2016
		US 2016-0269427 A1	15/09/2016
		US 2017-0279824 A1	28/09/2017
		US 2017-0316203 A1	02/11/2017
		US 8914406 B1	16/12/2014
		US 9038183 B1	19/05/2015
		US 9137258 B2	15/09/2015
		US 9167001 B1	20/10/2015
		US 9680846 B2	13/06/2017
		US 9710644 B2	18/07/2017
		US 9756082 B1	05/09/2017

국 제 조 사 보 고 서

국제출원번호
PCT/KR2018/002954

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; G06F 15/173; G06F 9/445; H04M 7/00; G06F 15/167; G06F 21/00; H04L 12/24

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: network, security, function, management, instantiation, request, message, 및 유사 용어.

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	US 2010-0217850 A1 (FERRIS, JAMES MICHAEL) 2010.08.26 단락 [0013], [0035]; 및 도면 1, 4 참조.	1-11
A	US 2016-0226835 A1 (BLACKROCK FINANCIAL MANAGEMENT, INC.) 2016.08.04 단락 [0016]-[0082]; 및 도면 1-7 참조.	1-11
A	US 2017-0012968 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 2017.01.12 단락 [0122]-[0260]; 및 도면 1-5 참조.	1-11
A	US 2004-0042609 A1 (DELANEY, ROBERT J. 등) 2004.03.04 단락 [0029]-[0059]; 및 도면 2-7 참조.	1-11
A	US 2015-0207813 A1 (VORSTACK, INC.) 2015.07.23 단락 [0036]-[0048]; 및 도면 1-4B 참조.	1-11

☐ 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
2018년 06월 21일 (21.06.2018)	2018년 06월 21일 (21.06.2018)

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

심사관
강희곡
전화번호 +82-42-481-8264

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2018/002954

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2010-0217850 A1	2010/08/26	US 8977750 B2	2015/03/10
US 2016-0226835 A1	2016/08/04	US 2016-0226718 A1	2016/08/04
		US 2017-0257280 A1	2017/09/07
		US 2017-0257282 A1	2017/09/07
		US 2017-0272332 A1	2017/09/21
		US 9705752 B2	2017/07/11
		US 9712398 B2	2017/07/18
US 2017-0012968 A1	2017/01/12	CN 105122738 A	2015/12/02
		EP 3107246 A1	2016/12/21
		EP 3107246 A4	2017/04/12
		WO 2015-143651 A1	2015/10/01
US 2004-0042609 A1	2004/03/04	AU 2003-268466 A1	2004/03/29
		US 7043000 B2	2006/05/09
		WO 2004-023775 A1	2004/03/18
US 2015-0207813 A1	2015/07/23	US 2015-0222656 A1	2015/08/06
		US 2016-0164890 A1	2016/06/09
		US 2016-0269427 A1	2016/09/15
		US 2017-0279824 A1	2017/09/28
		US 2017-0316203 A1	2017/11/02
		US 8914406 B1	2014/12/16
		US 9038183 B1	2015/05/19
		US 9137258 B2	2015/09/15
		US 9167001 B1	2015/10/20
		US 9680846 B2	2017/06/13
		US 9710644 B2	2017/07/18
		US 9756082 B1	2017/09/05