(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2017 년 9 월 14 일 (14.09.2017)

WIPO | PCT

(10) 국제공개번호
WO 2017/155280 A2

(51) 국제특허분류:
H04L 29/06 (2006.01) *H04L 12/741* (2013.01)

(21) 국제출원번호: PCT/KR2017/002448

(22) 국제출원일: 2017 년 3 월 7 일 (07.03.2017)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2016-0027900 2016 년 3 월 8 일 (08.03.2016) KR
10-2016-0081195 2016 년 6 월 28 일 (28.06.2016) KR

(71) 출원인: **주식회사 케이티 (KT CORPORATION)** [KR/KR]; 13606 경기도 성남시 분당구 불정로 90, Gyeonggi-do (KR).

(72) 발명자: **안태진 (AHN, Tae Jin)**; 34047 대전시 유성구 유성대로 1689 번길 70, Daejeon (KR). **이세희 (LEE, Se Hui)**; 34047 대전시 유성구 유성대로 1689 번길 70, Daejeon (KR). **김우태 (KIM, Woo Tae)**; 34047 대전시 유성구 유성대로 1689 번길 70, Daejeon (KR).

(74) 대리인: **특허법인 이상 (E-SANG PATENT & TRADEMARK LAW FIRM)**; 06747 서울시 서초구 바우뫼로 188, 3 층, Seoul (KR).

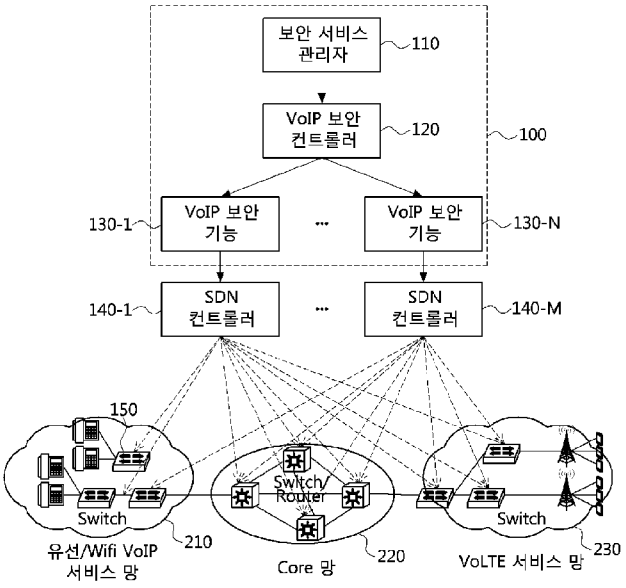
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, 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,

[다음 쪽 계속]

(54) **Title**: SECURITY SYSTEM FOR SDN/NFV-BASED IP CALL SERVICE AND METHOD FOR OPERATING SECURITY SYSTEM

(54) **발명의 명칭** : SDN/NFV 기반 IP 통화 서비스 보안 시스템 및 보안 시스템의 동작 방법



110 ... Security service manager
120 ... VoIP security controller
130-1, 130-N ... VoIP security function
140-1, 140-M ... SDN controller
210 ... Wired/Wifi VoIP service network
220 ... Core network
230 ... VoLTE service network

(57) **Abstract**: Disclosed are a security system and a security processing method for detecting whether an IP-based call service (VoIP or VoLTE) in an SDN and NFV environment is illegally used and blocking such an illegal use. A security system for an SDN-based centralized VoIP service comprises: a security service manager for setting and managing a security service policy necessary for using a VoIP security service; a VoIP security controller for generating the security service policy received through the security service manager, as a predetermined information model and delivering the generated information model to a VoIP security function; and at least one VoIP security function for providing the VoIP security service, on the basis of the information model received from the VoIP security controller. Therefore, it is possible to provide centralized and flexible services because the security service is provided by dynamically building the information model in a software-based SDN/NFV environment, without using an existing hardware-based security equipment.

(57) 요약서:

[다음 쪽 계속]

WO 2017/155280 A2

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:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

SDN 및 NFV 환경에서 IP 기반 통화 서비스(VoIP 또는 VoLTE)의 불법 사용 여부를 탐지하고 차단하는 보안 시스템 및 보안 처리 방법이 개시된다. SDN 기반의 중앙 집중형 VoIP 서비스 보안 시스템은, VoIP 보안 서비스를 이용하기 위해 필요한 보안 서비스 정책을 설정하고 관리하는 보안 서비스 관리자; 보안 서비스 관리자를 통해 전달받은 보안 서비스 정책을 소정의 정보 모델로 생성하여 VoIP 보안 기능에 전달하는 VoIP 보안 컨트롤러; 및 VoIP 보안 컨트롤러로부터 전달받은 정보 모델에 기초하여, VoIP 보안 서비스를 제공하는 적어도 하나의 VoIP 보안 기능을 포함하여 구성된다. 따라서, 기존의 하드웨어 기반 보안 장비가 아닌 소프트웨어 기반의 SDN/NFV 환경에서 정보 모델을 동적으로 구성하여 보안 서비스를 제공하기 때문에 중앙 집중화된 유연한 서비스 제공이 가능하다.

명세서

발명의 명칭: SDN/NFV 기반 IP 통화 서비스 보안 시스템 및 보안 시스템의 동작 방법

기술분야

[1] 본 발명은 유선 또는 무선 VoIP(Voice over) 및 VoLTE(Voice over LTE) 등의 IP 기반 통화 서비스에 대한 보안 시스템 및 보안 처리 방법에 관한 것으로써, 더욱 자세하게는 소프트웨어 정의 네트워크(SDN, Software-defined networking) 및 네트워크 기능 가상화(NFV, Network Function Virtualization) 환경에서 IP 기반 통화 서비스의 불법 사용 여부를 탐지하고 차단하는 기술에 관한 것이다.

배경기술

[2] 최근 들어, 스위치의 트래픽 포워딩 기능과 스위치의 제어 기능을 분리하여 통신 시스템을 효율적으로 운용하는 기술에 대한 표준화가 ONF(Open Networking Foundation), IETF(Internet Engineering Task Force), ETSI ISG NFV(Network Function Virtualization) 및 ITU-T 등을 중심으로 진행되고 있다.

[3] SDN(Software Defined Network)은 라우터나 스위치 등의 기본 네트워크 장비에 관계없이 사용자가 통제 권한을 가지며, 별도의 소프트웨어 컨트롤러가 트래픽 흐름을 제어하는 사용자 중심의 네트워크를 의미한다.

[4] SDN의 기술 중의 하나인 오픈플로우(OpenFlow) 기술 표준화를 추진하고 있는 표준화 단체들 중 ONF는 하드웨어(스위치)와 컨트롤러(Network OS) 사이를 연결하는 인터페이스를 정의하고 있다. 이는 네트워크를 통해 데이터 패킷을 어떻게 전달할 것인지 제어하기 위한 기능(Control Plane)을 물리적 네트워크와 분리하여 데이터 전달 기능(Data Plane)과 상호작용 하기 위한 프로토콜이다. IETF는 NFV(Network Functions Virtualization)를 기본 인프라로 이용하는 네트워크 환경에서 네트워크 보안 서비스(Network Security Service)를 제공하기 위한 표준 인터페이스를 정의하고 구현하는 워킹 그룹을 만들고, 네트워크 서비스 인프라 구축 및 운영 비용을 절감하기 위한 네트워크 기능 가상화인 NFV 연구 및 표준화를 활발히 진행되고 있다.

[5] 한편, VoIP 및 VoLTE 등의 IP 기반 통화 서비스에 대해 상기와 같은 SDN/NFV 기반의 환경에서의 유연하고 중앙집중적인 보안 서비스 시스템의 구조 및 동작 방법에 대해서는 아직 구체화되고 있지 않다.

발명의 상세한 설명

기술적 과제

[6] 상기와 같은 문제점을 해결하기 위한 본 발명의 제1 목적은, SDN 및 NFV 환경에서 IP 기반 통화 서비스(VoIP 또는 VoLTE)의 불법 사용 여부를 탐지하고 차단하는 보안 시스템을 제공하는 것이다.

[7] 상기와 같은 문제점을 해결하기 위한 본 발명의 제2 목적은, SDN 및 NFV

환경에서 IP 기반 통화 서비스의 불법 사용 여부를 탐지하고 차단하는 보안 처리 방법을 제공하는 것이다.

[8] 상기와 같은 문제점을 해결하기 위한 본 발명의 제3 목적은, SDN 및 NFV 환경에서 IP기반 통화 서비스의 불법 사용 여부를 탐지하고 차단하는 보안 시스템을 위해, 전달받은 보안 정책을 소정의 정보 모델로 생성하고, 보안 서비스를 제공하는 보안 기능(security function)들을 제어하는 보안 컨트롤러(security controller)의 동작 방법을 제공하는 것이다.

과제 해결 수단

[9] 상술한 본 발명의 제1 목적을 달성하기 위한 본 발명의 일 측면에 따른 소프트웨어 정의 네트워킹(SDN, software-defined networking) 기반의 중앙 집중형 VoIP(Voice over IP) 서비스 보안 시스템은, VoIP 보안 서비스를 이용하기 위해 필요한 보안 서비스 정책을 설정하고 관리하는 보안 서비스 관리자(Security Service Manager); 상기 보안 서비스 관리자를 통해 전달받은 보안 서비스 정책을 소정의 정보 모델로 생성하여 VoIP 보안 기능(VoIP security function)에 전달하는 VoIP 보안 컨트롤러(VoIP Security Controller); 및 상기 VoIP 보안 컨트롤러로부터 전달받은 정보 모델에 기초하여, VoIP 보안 서비스를 제공하는 적어도 하나의 VoIP 보안 기능(VoIP security function)을 포함하여 구성될 수 있다.

[10] 상기 보안 서비스 관리자는 어플리케이션 게이트웨이(application gateway) 역할을 수행할 수 있다.

[11] 상기 VoIP 보안 기능은, 적어도 하나의 SDN 스위치를 관리하는 적어도 하나의 SDN 컨트롤러에 연결될 수 있다.

[12] 상기 VoIP 보안 기능은, 상기 VoIP 보안 컨트롤러로부터 전달받은 정보 모델을 해석하여, 상기 SDN 컨트롤러가 SDN 스위치로 전달할 수 있는 API를 호출하거나 상기 SDN 컨트롤러와 상기 SDN 스위치의 연동 규격에 맞는 메시지 형태로 변환하여 상기 SN 컨트롤러로 전달할 수 있다.

[13] 상기 정보 모델은, 네트워크 장치를 통해 송수신되는 패킷 또는 특정 플로우에 속하는 패킷에 대해 특정 동작의 적용 여부를 판단하기 위한 조건(condition) 및 상기 조건이 만족되었을 때 수행될 동작(action)을 정의하는 동작 정보를 포함할 수 있다.

[14] 상기 조건은 단일 패킷에서 판단할 수 있는 패킷 값 조건과, 세션(session) 또는 플로우(flow) 등을 통하여 판단할 수 있는 상황(context) 조건을 포함할 수 있다.

[15] 상기 동작 정보는 트래픽 인입 제어 동작, 트래픽 출력 제어 동작, 및 보안 서비스를 제어하는 기능 프로파일(profile)을 적용하는 응용 동작(advanced action)을 포함할 수 있다.

[16] 상기 정보 모델은, 상기 조건과 상기 동작의 적용 대상을 정의하는 사건(event) 정보를 추가로 포함할 수 있다.

[17] 상기 사건 정보는 이벤트 시간(event time) 정보와 사용자 동작(user action)

정보를 포함할 수 있다.

[18] 상기 VoIP 보안 기능은 가상 머신 상에서 동작할 수 있다.

[19] 상술한 본 발명의 제2 목적을 달성하기 위한 본 발명의 일 측면에 따른 소프트웨어 정의 네트워킹(SDN, software-defined networking) 기반의 중앙 집중형 VoIP(Voice over IP) 서비스 보안 처리 방법은, 보안 서비스 관리자(Security Service Manager)가 VoIP 보안 서비스를 이용하기 위해 필요한 보안 서비스 정책을 생성하는 단계; VoIP 보안 기능(VoIP security function)가 상기 보안 서비스 정책을 수신하고, 상기 보안 서비스 정책을 소정의 정보 모델로 생성하여 적어도 하나의 VoIP 보안 기능(VoIP security function)에 전달하는 단계; 및 상기 적어도 하나의 VoIP 보안 기능이, 상기 전달받은 정보 모델에 기초하여, VoIP 보안 서비스를 제공하는 단계를 포함하여 구성될 수 있다.

[20] 상기 보안 서비스 관리자는 어플리케이션 게이트웨이(application gateway) 역할을 수행할 수 있다.

[21] 상기 VoIP 보안 기능은, 적어도 하나의 SDN 스위치를 관리하는 적어도 하나의 SDN 컨트롤러에 연결될 수 있다.

[22] 상기 VoIP 서비스 보안 처리 방법은, 상기 VoIP 보안 기능이 상기 VoIP 보안 컨트롤러로부터 전달받은 정보 모델을 해석하여, 상기 SDN 컨트롤러가 SDN 스위치로 전달할 수 있는 API를 호출하거나 상기 SDN 컨트롤러와 상기 SDN 스위치의 연동 규격에 맞는 메시지 형태로 변환하여 상기 SDN 컨트롤러로 전달하는 단계를 추가로 포함할 수 있다.

[23] 상기 정보 모델은, 네트워크 장치를 통해 송수신되는 패킷 또는 특정 플로우에 속하는 패킷에 대해 특정 동작의 적용 여부를 판단하기 위한 조건(condition) 및 상기 조건이 만족되었을 때 수행될 동작(action)을 정의하는 동작 정보를 포함할 수 있다.

[24] 상기 조건은 단일 패킷에서 판단할 수 있는 패킷 값 조건과, 세션(session) 또는 플로우(flow) 등을 통하여 판단할 수 있는 상황(context) 조건을 포함할 수 있다.

[25] 상기 동작 정보는 트래픽 인입 제어 동작, 트래픽 출력 제어 동작, 및 보안 서비스를 제어하는 기능 프로파일(profile)을 적용하는 응용 동작(advanced action)을 포함할 수 있다.

[26] 상기 정보 모델은, 상기 조건과 상기 동작의 적용 대상을 정의하는 사건(event) 정보를 추가로 포함할 수 있다.

[27] 상기 사건 정보는 이벤트 시간(event time) 정보와 사용자 동작(user action) 정보를 포함할 수 있다.

[28] 상술한 본 발명의 제3 목적을 달성하기 위한 본 발명의 일 측면에 따른, SDN 기반 중앙 집중형 VoIP 보안 시스템에서 보안 서비스 관리자 및 적어도 하나의 VoIP 보안 기능과 연동하는 VoIP 보안 컨트롤러의 동작 방법은, 상기 보안 서비스 관리자로부터 VoIP 보안 서비스를 이용하기 위해 필요한 보안 서비스

정책을 수신하는 단계; 상기 보안 서비스 정책을 소정의 정보 모델로 생성하여 상기 적어도 하나의 VoIP 보안 기능(VoIP security function)에 전달하는 단계; 및 상기 적어도 하나의 VoIP 보안 기능으로부터 상기 소정의 정보 모델에 따라 수행된 상기 보안 서비스 정책의 수행 결과를 수신하는 단계를 포함하여 구성될 수 있다.

[29] 상기 정보 모델은, 네트워크 장치를 통해 송수신되는 패킷 또는 특정 플로우에 속하는 패킷에 대해 특정 동작의 적용 여부를 판단하기 위한 조건(condition) 및 상기 조건이 만족되었을 때 수행될 동작(action)을 정의하는 동작 정보를 포함할 수 있다.

[30] 상기 조건은 단일 패킷에서 판단할 수 있는 패킷 값 조건과, 세션(session) 또는 플로우(flow) 등을 통하여 판단할 수 있는 상황(context) 조건을 포함할 수 있다.

[31] 상기 동작 정보는 트래픽 인입 제어 동작, 트래픽 출력 제어 동작, 및 보안 서비스를 제어하는 기능 프로파일(profile)을 적용하는 응용 동작(advanced action)을 포함할 수 있다.

[32] 상기 정보 모델은, 상기 조건과 상기 동작의 적용 대상을 정의하는 사건(event) 정보를 추가할 수 있다.

[33] 상기 사건 정보는 이벤트 시간(event time) 정보와 사용자 동작(user action) 정보를 포함할 수 있다.

발명의 효과

[34] 상기와 같은 본 발명에 따르면, SDN/NFV 기반의 정보 모델(Information model)을 정의하여, VoIP 및 VoLTE 등 IP기반 통화 서비스를 불법/악의적으로 사용하는 것을 실시간으로 탐지하여 차단한다. 기존의 HW 기반 보안 장비가 아닌 SW기반의 SDN/NFV 환경에서 정보모델을 동적으로 구성하여 서비스를 제공하기 때문에 저비용으로 중앙 집중화된 유연한 서비스 제공이 가능하다.

도면의 간단한 설명

[35] 도 1은 본 발명의 일 실시예에 따른 SDN/NFV 기반 IP 통화 서비스 보안 시스템의 구성을 개략적으로 나타낸 구성도이다.

[36] 도 2는 본 발명의 일 실시예에 따른 SDN/NFV 기반 IP 통화 서비스 보안 시스템에서 VoIP 보안 컨트톨러와 VoIP 보안 기능들 간의 연동 정보 모델의 구성요소들의 예를 설명하기 위한 도면이다.

[37] 도 3은 도 2에서 예시한 본 발명의 일 실시예에 따른 정보 모델의 각 구성 요소별 예시 정보를 설명하기 위한 도면이다.

[38] 도 4는 본 발명의 일 실시예에 따른 SDN/NFV 기반 IP 통화 서비스 보안 처리 방법을 설명하기 위한 순서도이다.

[39] 도 5는 본 발명의 다른 실시예에 따른 SDN/NFV 기반 IP 통화 서비스 보안 시스템에서 VoIP 보안 컨트톨러와 VoIP 보안 기능들 간의 연동 정보 모델의 구성요소들의 예를 설명하기 위한 도면이다.

[40] 도 6은 도 5에서 예시한 본 발명의 다른 실시예에 따른 정보 모델의 각 구성 요소별 예시 정보를 설명하기 위한 도면이다.

[41] 도 7는 본 발명의 다른 실시예에 따른 유선(WiFi 등의 mobile VoIP 포함) 단말의 불법 인증 시도 탐지에서 이중등록 패턴을 탐지하여 불법 인증 시도를 차단하는 방법을 설명하기 위한 흐름도이다.

[42] 도 8은 본 발명의 다른 실시예에 따른 무선 단말의 불법 인증 시도 탐지에서 이중등록 패턴을 탐지하여 불법 인증 시도를 차단하는 방법을 설명하기 위한 흐름도이다.

[43] 도 9는 본 발명의 다른 실시예에 따른 VoIP 및 VoLTE 단말의 불법 인증 시도 탐지에서 인증 만료시간의 비정상 동작 패턴을 탐지하여 불법 인증 시도를 차단하는 방법을 설명하기 위한 흐름도이다.

발명의 실시를 위한 최선의 형태

[44] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[45] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[46] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[47] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의

존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[48] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[49]

[50] 또한, 명세서에 기재된 '컨트롤러(controller)'는 트래픽의 흐름을 제어하기 위해 관련 구성 요소(예를 들면, 스위치, 라우터 등)를 제어하는 기능 요소(entity)를 의미하는 것으로, 물리적인 구현 형태나 구현 위치 등에 한정되지 않는다. 예를 들어, 컨트롤러는 ONF나, IETF, ETSI 및/또는 ITU-T 등에서 정의하고 있는 컨트롤러 기능 요소(entity)를 의미할 수 있다.

[51] 또한, 명세서에 기재된 '스위치'는 트래픽(또는 패킷)을 실질적으로 포워딩하거나 스위칭 또는 라우팅하는 기능 요소를 의미하는 것으로, ONF나, IETF, ETSI 및/또는 ITU-T 등에서 정의하고 있는 스위치, 라우터, 스위치 요소, 라우터 요소, 포워딩 요소 등을 의미할 수 있다.

[52] 또한, 명세서에 기재한 VoIP 서비스는 상기 유선/WiFI/VoLTE 등 다양한 IP 망 기반의 음성/영상 통화 서비스를 통칭한다.

[53]

[54] 이하, 도면을 참조로 하여 본 발명의 실시예에 대하여 상세히 설명한다.

[55] 도 1은 본 발명의 일 실시예에 따른 SDN/NFV 기반 IP 통화 서비스 보안 시스템의 구성을 개략적으로 나타낸 구성도이다.

[56] 도 1을 참조하면, 일 실시예에 따른 IP 통화 서비스 시스템(100)은 보안 서비스 관리자(SSM, Security Service Manager; 110), VoIP 보안 컨트롤러(VSC, VoIP Security Controller; 120) 및 적어도 하나의 VoIP 보안 기능 (VSF, VoIP Security Function; 130-1, ...,130-N)을 포함하여 구성될 수 있다.

[57] 이때, 상기 IP 통화 서비스 시스템(100)은 유선/WiFi VoIP 서비스망(210), 코어 망(core network, 220), 무선 VoLTE 서비스망(230)을 모두 포괄하여 적용될 수 있다. 또한, 각각의 서비스 망은 복수의 스위치(network device)를 포함할 수 있다. 또한, 유선/WiFI VoIP 서비스 망(210)과 무선 VoLTE 서비스 망(230)은 코어 망(220)과 각각 연결된다.

[58] 먼저, 보안 서비스 관리자(110)는 사용자 또는 관리자(administrator)가 VoIP 보안 서비스를 이용하기 위해 필요한 보안 서비스 정책 및/또는 제어 조건을 설정하고 관리하는 어플리케이션 게이트웨이(application gateway)이 역할을 수행할 수 있다. 예를 들어, 사용자 또는 관리자는 사용자 인터페이스(User Interface) 화면 또는 커맨드 라인 인터페이스(CLI, command-line interface) 등을 통해 이용하고자 하는 보안서비스 정책을 상기 보안 서비스 관리자(110)를 통해

요청할 수 있다.

[59] 다음으로, VoIP 보안 컨트롤러(120)는 보안 서비스 관리자(110)를 통해 전달받은 보안 서비스 정책을 적어도 하나의 VoIP 보안 기능들(130-1, ..., 130-N)이 SDN 컨트롤러들(140-1, ..., 140-M) 및 SDN 컨트롤러들의 제어를 받는 스위치들에 적용될 수 있도록 사전 정의된 정보 모델(Information Model)를 생성하여 적어도 하나의 VoIP 보안 기능들로 전달한다. 이 정보 모델에는 네트워크 디바이스(스위치 등)를 통해 송수신되는 패킷 및 이 특정 플로우에 속하는 패킷에 대해 특정 동작을 적용하기 위한 비교 조건 및 그 조건이 만족되었을 때 해당 동작을 어떻게 수행할지에 대한 동작 절차가 정의되어 있다. VoIP 보안 컨트롤러(120)는 VoIP 보안 기능들이 정보모델을 통해 전달해 준 패킷에 대해 발신번호 변작, 해킹을 위한 장비검색(scanning) 탐지/차단 등의 VoIP 보안 서비스 동작을 수행할 수 있도록 하기 위한 논리적인 판단을 수행한다. 도 1에 예시된 바와 같이, 하나의 VoIP 보안 컨트롤러는 1개 이상의 VoIP 보안 컨트롤러에 연결될 수 있다.

[60] VoIP 보안 기능들(130-1, ..., 130-N)은 보안 컨트롤러(120)로부터 전달받은 정보 모델을 해석하여 실제적인 VoIP 보안 서비스를 제공한다. VoIP 보안 기능들 각각은 보안 컨트롤러(120)로부터 전달 받은 정보 모델을 SDN 컨트롤러(140-1, ..., 140-M)가 SDN 스위치들로 전달할 수 있는 API를 호출하거나 둘 간의 연동 규격에 맞는 메시지 형태로 변환하여 SDN 컨트롤러(140-1, ..., 140-M)로 전달한다. VoIP 보안 기능은 독립적인 하드웨어 서버에 구현될 수도 있고, 클라우드(cloud) 환경의 가상 머신(VM, Virtual Machine)으로 또는 가상 머신 상에 구현될 수도 있다. 도 1에서 예시된 바와 같이, 하나의 VoIP 보안 기능은 1개 이상의 SDN 컨트롤러들과 연결될 수 있다.

[61] SDN 컨트롤러(140-1, ..., 140-M)는 트래픽의 흐름을 제어하기 위해 관련 구성 요소(예를 들면, 스위치, 라우터 등)를 제어하는 기능 요소(entity)를 의미하는 것으로, ONF나, IETF, ETSI 및/또는 ITU-T 등에서 정의하고 있는 컨트롤러 기능 요소(entity) 등 다양한 종류의 컨트롤러를 의미할 수 있다.

[62] 스위치(Network Device)는 트래픽(또는 패킷 또는 플로우)을 실질적으로 포워딩하거나 스위칭 또는 라우팅하는 기능 요소를 의미하는 것으로, ONF나, IETF, ETSI 및/또는 ITU-T 등에서 정의하고 있는 스위치, 라우터, 스위치 요소, 라우터 요소, 포워딩 요소 등을 의미할 수 있다.

[63]

[64] 도 2는 본 발명의 일 실시예에 따른 SDN/NFV 기반 IP 통화 서비스 보안 시스템에서 VoIP 보안 컨트롤러와 VoIP 보안 기능들 간의 연동 정보 모델의 구성요소들의 예를 설명하기 위한 도면이다.

[65] 본 발명의 일 실시예에 따른 정보 모델은 정책(policy), 규칙(rule), 조건(condition), 및 동작(action) 4 가지 정보들의 전부 또는 일부를 포함하여 구성될 수 있다. 이때, 도 2에서 예시된 바와 같이, 정책과 정책에 속한 규칙들,

규칙들에 속한 조건과 동작은 계층적인 구조를 가질 수 있다.

[66] 먼저, 정책(policy, 310)은 서비스 레벨에서의 보안 서비스 정책을 정의한다. 일반적으로 정책은 IPS(Intrusion Prevention System(or, service)), IDS(Intrusion Detection System(or, service), 웹 필터(web filter) 등 단위 보안 서비스 등이 될 수 있다. 본 발명의 일 실시예에서는 VoIP/VoLTE 보안 정책이 이에 해당될 수 있다. 정보 모델 내에서 정책은 정책의 명칭(name), 정책의 식별자(identifier) 등을 포함하여 정의될 수 있다.

[67] 다음으로, 규칙(rule, 320)은 트래픽/플로우에 대하여 특정 동작의 수행여부를 결정하기 위한 매칭(matching) 조건들과 상기 조건이 만족되었을 때 해당 트래픽, 플로우에 대해서 수행되는 동작(action)을 정의한다. 도 2에서 예시된 바와 같이, 1개의 정책에는 1개 이상 규칙이 정의될 수 있다. 본 발명의 일 실시예에서는 'VoIP/VoLTE 계정 도용', '발신번호 변작', '다량 메시지 발송' 등의 탐지 및 제어 등이 규칙이 될 수 있다. 도 2에서 예시된 바와 같이, 하나의 규칙은 적어도 하나의 조건들과 적어도 하나의 동작들을 포함하여 구성될 수 있다. 즉, 조건들은 대응되는 동작의 수행 여부를 결정하기 위한 매칭 조건을 의미하며, 동작은 해당 조건이 만족되었을 때 수행되는 동작 절차를 의미할 수 있다. 즉, 규칙 내에 포함되는 조건은 특정 규칙이 만족되는지를 판단하기 위한 1개 이상의 조건의 집합이다.

[68] 여기서, 조건330)은 패킷 값 조건과 상황(context) 조건으로 구분될 수 있다.

[69] 먼저, 패킷 값 조건은 단일 패킷에서 판단할 수 있는 조건들이다. 단말의 MAC(medium access control) 주소, VLAN(Virtual LAN), 소스(source) 및 목적지(destination) IP 주소, 소스 및 목적지 포트(port), 패킷 헤더(header)/페이로드(payload) 값 등 패킷 에서 추출하여 비교할 수 있는 TCP/IP의 Layer1부터 Layer7까지의 조건들이 이에 해당한다.

[70] 다음으로, 상황 조건은 세션 또는 플로우(flow) 등을 통하여 판단할 수 있는 상황(context)과 관련된 조건이다. 본 발명의 실시예에서는 통화 시도 중, 통화 취소, 통화 중, 통화 종료 등 통화 호의 상태, 지역적인 위치 등이 포함될 수 있다.

[71] 한편, 추가적인 정보 요소로서 우선순위(priority)는 비교가 만족되는 복수 개의 규칙이 존재할 경우 동작을 적용해야 할 규칙의 우선순위를 나타낸다.

[72] 동작(340)은 비교 조건이 만족되는 패킷이나 플로우에 대한 처리 방법을 정의한다. 동작은 기본동작(basic action)과 응용동작(advanced action)으로 구분될 수 있다. 예를 들면, 기본 동작은 패킷 차단, 통과, 복사 등의 단순한 제어 동작을 의미하며, 응용동작은 보안 서비스를 제어하는 기능 프로파일의 적용을 의미할 수 있다. 예를 들어, 응용동작은 VoIP/VoLTE 보안 프로파일(Security Profile), IPS 동작 프로파일, URL 필터링(filtering) 프로파일, Anti-virus file 등이 해당될 수 있다.

[73]

[74] 도 3은 도 2에서 예시한 본 발명의 일 실시예에 따른 정보 모델의 각 구성

요소별 예시 정보를 설명하기 위한 도면이다.

[75] 먼저, 패킷 값 조건(331)은 통화 패킷의 발/착신지 IP 주소, 발/착신지 포트 번호, 발신전화번호, 세션의 call-id 유형(길이, 문자/숫자, 도메인 표현 여부 등), 통화 신호 메시지의 헤더 순서(From, To, Via, Cseq 등) 및 음성/영상 통화 세션 정보를 나타내는 SDP(Session Description Protocol) 내의 정보의 전부 또는 일부를 포함할 수 있다.

[76] 다음으로, 상황 조건(332)은 통화 호 상태 정보(통화 시도, 통화중, 통화 종료, 통화 실패 등), 가입자 단말 기종 정보(OS버전, 제조사 정보 등) 및 발신지 IP 위치 정보(할당된 IP 제공 사업자, 국가 등)의 전부 또는 일부를 포함할 수 있다.

[77] 다음으로, 우선순위는 조건이 만족되는 복수 개의 규칙이 존재할 경우 동작을 적용해야 할 규칙의 우선순위를 나타낸다.

[78] 다음으로, 기본 동작(basic action)은 상기 조건이 만족되었을 경우, 해당 패킷을 허용하는 동작, 해당 패킷을 차단하는 동작, 해당 패킷을 복사하여 VoIP 보안 컨트롤러(120)로 전달하는 동작 등을 포함할 수 있다.

[79] 다음으로, 응용 동작(advanced action)은 상기 상황기반 비교에서 호 상태에 따른 호 제어 동작과 네트워크 장치가 VoIP 보안 컨트롤러(120)나 VoIP 보안 컨트롤러(130-1,...,130-N)의 별도 제어 없이 직접 트래픽 차단/허용 여부를 판단할 수 있는 VoIP/VoLTE 보안 프로파일 적용 동작을 포함할 수 있다.

[80]

[81] 도 4는 본 발명의 일 실시예에 따른 SDN/NFV 기반 IP 통화 서비스 보안 처리 방법을 설명하기 위한 순서도이다.

[82] 먼저, 보안 서비스 관리자(110)는 VoIP 보안 컨트롤러(120)로 VoIP 보안 서비스 정책을 포함한 보안 서비스 정책 적용 명령 메시지를 전송한다(S410). 해당 메시지는 앞서 설명한 바와 같이, 사용자 인터페이스 화면이나 커맨드 라인 인터페이스 등을 통해 사용자나 관리자가 설정한 보안 서비스 정책을 포함한다. 보안 서비스 정책으로는 발신번호 변작, 해킹을 위한 단말/장비 검색(scanning), DDOS attack 등의 다량 메시지 발송, 계정 도용 탐지/차단 등이 포함될 수 있다.

[83] 다음으로, VoIP 보안 컨트롤러(120)는 보안 서비스 관리자(110)로부터 전달받은 보안 서비스 정책을 수행할 수 있도록 하는 정보 모델을 생성하며(S420), 생성된 정보 모델을 VoIP 보안 기능들(130)에게 전달한다(S430). 이때, 해당 정보 모델을 수신하는 VoIP 보안 기능들의 범위는 해당 정보 모델이 적용되는 대상에 따라서 달라질 수 있다.

[84] 또한, 앞서 언급된 바와 같이, 정보 모델에는 네트워크 디바이스(스위치 등)를 통해 송수신되는 패킷 및 이 특정 플로우에 속하는 패킷에 대해 특정 동작을 적용하기 위한 조건 및 그 조건이 만족되었을 때 해당 동작을 어떻게 수행할지에 대한 동작 절차가 정의되어 있다.

[85] 다음으로, VoIP 보안 컨트롤러(120)로부터 정보 모델을 전달받은 VoIP 보안 기능(130)은 전달받은 정보모델을 해석하여 실제적인 VoIP 보안 서비스를

제공할 수 있는 SDN 컨트롤러(140)의 API(예컨대, OpenFlow의 North Bound API 등)를 호출할 수 있다(S440, S450). 한편, API 호출을 대신하여, VoIP 보안 기능과 SDN 컨트롤러간에 미리 약속된 연동 규격에 맞는 메시지 형태로 변환하여 상기 정보 모델의 해석 내용이 전달될 수도 있다.

[86] 다음으로, SDN 컨트롤러(140)는 VoIP 보안 기능(130)이 요청한 API(또는, 메시지)를 확인하여, 네트워크 장치(150)가 이해할 수 있는 인터페이스(OpenFlow, NetConf 등)로 변환하여 네트워크 장치(150)에게 전달할 수 있다(S460).

[87] 다음으로, 네트워크 장치(150)는 SDN 컨트롤러(140)가 전달한 명령에 따라 플로우 테이블(flow table) 등을 생성하여, 조건에 맞는 패킷이 유입되는지 모니터링 하여, 해당 조건에 맞는 패킷인 경우 패킷 차단, 허용, 전달 등의 제어를 수행한다(S470).

[88] 마지막으로, 네트워크 장치(150), SDN 컨트롤러(140), VoIP 보안 기능(130), VoIP 보안 컨트롤러(120)는 각각 수신된 요청에 따른 결과를 상위 계층으로 전달할 수 있다(S481, S482, S483, S484).

[89]

[90] 이하에서는, 상술된 본 발명의 일 실시예에 따른 VoIP 서비스 보안 시스템 및 처리 방법이 구체적인 보안 서비스에 적용되는 절차를 예시적으로 설명하기로 한다. 이하에서는 발신번호 변작을 탐지/제어하는 보안 서비스의 적용 절차와 VoIP/VoLTE 해킹 대상 단말/장비 검색(scanning) 탐지/차단 정책 수행 절차를 예시적으로 설명하기로 한다.

[91] 이하의 설명에서, 정보 모델은 아래의 형태로 기술한다.

[92] 규칙 n: [{(패킷 값 조건), (상황 조건), (우선순위)}, {(기본동작), (응용동작)}]

[93] 대괄호[] 내의 중괄호{}는 조건 정보와 동작 정보을 구분하기 위한 것이며, 중괄호 내의 소괄호()는 정보 모델의 세부 사항을 의미한다. 소괄호가 null 값인 경우는 해당 사항이 없음을 의미한다.

[94]

[95] **적용예#1-발신번호 변작 탐지/제어**

[96] VoIP 보안 컨트롤러(120)는 VoIP 보안 기능(130)이 아래 규칙 1과 규칙2에 의해서 통화상태가 통화시도 또는 통화가 연결되어 통화중 상태가 될 경우 해당 신호 패킷을 복사하여 전달할 수 있도록 하기 규칙 1과 규칙 2가 정의된 정보 모델을 전달한다.

[97]

[98] 규칙1: [{(port=5060), (통화시도), (1000)}, {(패킷 복사), ()}]

[99] ⇒ 패킷 값 조건: 발신 또는 착신 패킷의 서비스 포트가 5060으로 지정된다. 여기에서, 포트번호는 5060은 하나의 예시이며, 통화서비스에서 사용하는 포트 값을 입력한다.

[100] ⇒ 상황 조건: 통화시도 상태

[101] ⇒ 우선순위: 1000 (일 실시예에서, 값이 작은 경우가 우선순위가 높음)

[102] ⇒ 기본동작: 패킷을 복사하여 VSC로 전달

[103] ⇒ 응용동작: 해당 없음

[104]

[105] 규칙2: [{(port=5060), (통화중), (1000)}, {(패킷 복사), ()}]

[106] ⇒ 패킷 값 조건: 발신 또는 착신 패킷의 서비스 포트가 5060

[107] ⇒ 상황 조건: 통화 시도하여 상태가 전화를 받은 통화중 상태

[108] ⇒ 우선순위: 1000

[109] ⇒ 기본동작: 패킷을 복사하여 VSC로 전달

[110] ⇒ 응용동작: 해당 없음

[111]

[112] 여기에서, 규칙 2는 VoIP 보안 컨트롤러(120)가 규칙1에 따라 번호 변작호 여부를 판단하고 있는 동안 해당 호를 차단하기 위한 규칙3(후술됨)이 VoIP 보안 기능(130)에 적용되기 전에, 통화 상태가 통화 시도에서 통화 중으로 변경되는 호가 발생할 경우를 대비하여 통화중 상태로 변경되었음을 알리는 신호 메시지(200 OK 등)가 발생할 경우 이를 VoIP 보안 컨트롤러(120)로 전달하여 차단여부 판단 이 전에 통화중 상태로 변경된 발신번호 변작 호까지도 차단하기 위한 규칙이다.

[113] VoIP 보안 컨트롤러(120)는 VoIP 보안 기능(130)에서 복사되어 전달된 신호 패킷에서 발신지 IP 주소(IP_1), 발신번호(From URI번호, 발신번호_1), display name(Caller-ID, CID_1))을 추출하여, 가입자가 개통시에 신청한 display name과 비교하여, 같은 경우 정상이므로 복사된 패킷을 폐기하고, 다른 경우 발신번호 변작호로 판단하고 이 통화를 종료하기 위한 규칙3을 생성하여 VoIP 보안 기능(130)으로 전달한다.

[114]

[115] 규칙3: [{(port=5060, source ip=IP_1, 발신번호_1, CID_1), (),(100)}, {(패킷 차단), (VoIP/VoLTE 보안 프로파일 적용)}]

[116]

[117] 규칙3에 의해 VoIP 보안 기능(130)은 발신지IP가 IP_1이고, 발신번호가 발신번호_1이고, CID_1인 패킷은 차단한다. 그리고, 규칙3은 우선순위가 100이므로 우선순위가 1000인 규칙1, 규칙2보다 우선 적용된다.

[118] 그리고, 응용동작인 VoIP/VoLTE 보안 프로파일 적용에 의해 차단 리스트에 (IP_1, CID_1)을 추가하여 향후 해당 IP와 CID_1로 호가 시도되면 별도의 VoIP 보안 컨트롤러 및 VoIP 보안 기능의 제어 없이 네트워크 장치에서 즉시 차단할 수 있다.

[119] 또한 VoIP 보안 컨트롤러(120)가 상기 규칙3을 VoIP 보안 기능(130)으로 전달할 때, 해당 호가 통화 연결되어 통화 중인 경우 이를 차단하기 위해 상황비교 조건 중 호상태 조건이 "통화중"인 경우 호 차단 메시지를 사용하여

해당 호를 차단할 수 있도록 규칙 4를 생성하여 VoIP 보안 기능(130)으로 전달한다.

[120]

[121] 규칙4: [{(port=5060, source ip= IP_1, 발신번호_1, CID_1), (통화중), (100)}, {(), (호 차단 응용동작 (BYE 메시지 생성하여 호 차단)}]

[122]

[123] VoIP 보안 기능(130)는 규칙4의 응용동작인 호 제어 동작에 의해 이 호를 차단하기 위한 신호 메시지(BYE 등)를 생성하여 발신지 IP와 해당 호를 처리하고 있던 교환장비로 전송하여, 해당 호를 종료 처리 한다.

[124]

[125] **적용예#2-해킹 대상 단말/장비 검색(scanning)**

[126] VoIP 보안 컨트롤러(120)는 VoIP 보안 기능(130)이 규칙 1과 규칙2에 의해서 통화상태가 통화시도 또는 인증(SIP Register 등) 시도인 경우에 해당 신호 패킷을 복사하여 전달하도록 VoIP 보안 기능(130)에게 하기 규칙들을 전달한다. 통화시도와 인증 시도 이외에도 단말/장비 탐색(scanning)에 사용될 수 있는 상황정보(SIP Options 등)는 규칙은 필요에 따라 추가할 수 있다.

[127]

[128] 규칙1: [{(port=5060), (통화 시도), (1000)}, {(패킷 복사), ()}]

[129] ⇒ 패킷 값 조건: 발신 또는 착신 패킷의 서비스 포트가 5060으로 지정된다. 여기에서, 포트번호는 5060은 하나의 예시이며, 통화서비스에서 사용하는 포트 값을 입력한다.

[130] ⇒ 상황 조건: 통화시도 상태

[131] ⇒ 우선순위: 1000

[132] ⇒ 기본동작: 패킷을 복사하여 VoIP 보안 컨트롤러로 전달

[133] ⇒ 응용동작: 해당 없음

[134]

[135] 규칙2: [{(port=5060), (인증 시도), (1000)}, {(패킷 복사), ()}]

[136] ⇒ 패킷 값 조건: 발신 또는 착신 패킷의 서비스 포트가 5060

[137] ⇒ 상황 조건: 인증시도 상태

[138] ⇒ 우선순위: 1000

[139] ⇒ 기본동작: 패킷을 복사하여 VoIP 보안 컨트롤러로 전달

[140] ⇒ 응용동작: 해당 없음

[141]

[142] VoIP 보안 컨트롤러(120)는 VoIP 보안 기능(130)에서 복사되어 전달된 신호 패킷에서 발신지 IP 주소(IP_1), 발신번호(From URI번호, 발신번호_1) 정보를 추출한다. 스캐닝(scanning) 시에는 해커가 다량의 단말/장비로 메시지를 보낼 수 있기 때문에 유사한 메시지가 복수의 VoIP 보안 기능(130)로부터 VoIP 보안 컨트롤러(120)로 전달될 수도 있다. 따라서 VoIP 보안 컨트롤러(120)는 scanning

여부를 판단하기 위해 1개 이상의 VoIP 보안 기능(130)에서 전달된 메시지를 통합하여 scanning 여부를 판단 할 수 있다. VoIP 보안 컨트롤러(120)는 각 VSF별로 추출된 발신지 IP 주소(IP_1)와 발신번호(From URI번호, 발신번호_1) 각각에 대해 주기시간(초/분 단위 등) 단위로 누적하여 합산한 후 그 값이 설정된 임계치를 넘어가는 경우 스캐닝 시도로 판단한다. 스캐닝으로 판단된 경우에 대한 제어 동작 방법은 2가지이다.

[143] 첫 번째 방법은 발신지 IP_1과 발신번호_1인 호의 패킷을 차단하는 규칙3을 생성하여 VoIP 보안 기능(130)으로 전달한다. 두 번째 방법은 스캐닝으로 판단한 호의 SDP(Session Description Protocol)를 VoIP/VoLTE 보안 프로파일에 추가하도록 VoIP 보안 기능(130)으로 전달하여 네트워크 장치에서 즉시 차단할 수 있다.

[144]

[145] 규칙3: [{(port=5060, source ip= IP_1, 발신번호_1), (), ()}, {(패킷 차단), (VoIP/VoLTE Security Profile 업데이트)}] -> 보안 프로파일 중 차단 리스트에 SDP_1추가

[146]

[147] 규칙3에 의해 VoIP 보안 기능(130)는 발신지IP가 IP_1이고, 발신번호가 발신번호_1인 통화에 대한 패킷은 모두 차단한다. 그리고, VoIP/VoLTE 보안 프로파일의 차단 정책 리스트에 SDP_1을 신규 추가하여 향후 동일 SDP를 가지는 호가 시도되면 별도의 VoIP 보안 컨트롤러 및 VoIP 보안 기능의 제어 없이 네트워크 장치에서 즉시 차단할 수 있다.

[148]

[149] 도 5는 본 발명의 다른 실시예에 따른 SDN/NFV 기반 IP 통화 서비스 보안 시스템에서 VoIP 보안 컨트롤러와 VoIP 보안 기능들 간의 연동 정보 모델의 구성요소들의 예를 설명하기 위한 도면이다.

[150] 본 발명의 다른 실시예에 따른 정보 모델은 정책(policy), 규칙(rule), 사건(event), 조건(condition), 및 동작(action) 5 가지 정보들의 전부 또는 일부를 포함하여 구성될 수 있다. 이때, 도 5에서 예시된 바와 같이, 정책과 정책에 속한 규칙들, 규칙들에 속한 사건, 조건과 동작은 계층적인 구조를 취할 수 있다. 한편, 도 2에서 예시된 정보 모델과 도 5에서 예시된 정보 모델의 차이점은, 도 5에서 예시된 정보 모델의 경우, 사건(event) 정보를 추가로 포함하고 있고, 동작 정보의 정의에서 다소 차이가 있다는 점이다.

[151] 먼저, 정책(policy, 510)은 서비스 레벨에서의 보안 서비스 정책을 정의한다. 일반적으로 정책은 IPS, IDS, 웹 필터, IP 통화 보안 등 단위 보안 서비스 등이 될 수 있다. 본 발명의 일 실시예에서는 VoIP/VoLTE 보안 정책이 이에 해당될 수 있다. 정보 모델 내에서 정책은 정책의 명칭(name), 정책의 식별자(identifier) 등을 포함하여 정의될 수 있다.

[152] 다음으로, 규칙(rule, 520)은, 특정 정책을 탐지하기 위한 매칭(matching)

조건들(540), 상기 조건이 만족되었을 때 해당 트래픽, 플로우에 대해서 수행되는 동작(action, 550), 및 상기 조건과 동작의 적용 대상을 정의하는 사건(event, 530)을 포함할 수 있다. 도 5에서 예시된 바와 같이, 1개의 정책에는 1개 이상 규칙이 정의될 수 있다. 본 실시예에서는 'VoIP/VoLTE 계정 도용을 통한 불법 인증 시도', '발신번호 변작', '인증 만료시간 변작' 등의 탐지와 제어 등이 규칙이 될 수 있다. 도 5에서 예시된 바와 같이, 하나의 규칙은 적어도 하나의 사건, 적어도 하나의 조건과 적어도 하나의 동작들을 포함하여 구성될 수 있다. 여기에서, 사건은 조건을 비교하여 동작하기 위한 주요한 대상을 지정하는 것이다. 또한, 즉, 조건은 대응되는 동작의 수행여부를 결정하기 조건을 의미하며, 동작은 해당 조건이 만족되었을 때 수행되는 동작 절차를 의미할 수 있다. 즉, 규칙 내에 포함되는 조건은 특정 규칙이 만족되는지를 판단하기 위한 1개 이상의 조건의 집합이다.

[153] 먼저, 사건(530)은 이벤트 시간(event time)와 사용자 동작(user action)으로 구분될 수 있다. 이벤트 시간의 경우, 이벤트(예컨대, 인증 또는 통화)의 발생 시각 정보를 의미하며, 사용자 동작의 경우 사용자가 수행하는 행위(즉, 이벤트)를 의미한다(예컨대, 단말 등록/인증과 통화 발/착신 등).

[154] 다음으로, 조건540)은 패킷 값 조건과 상황(context) 조건으로 구분될 수 있다.

[155] 먼저, 패킷 값 조건은 단일 패킷에서 판단할 수 있는 조건들이다. 단말의 MAC(medium access control) 주소, VLAN(Virtual LAN), 소스(source) 및 목적지(destination) IP 주소, 소스 및 목적지 포트(port), 패킷 헤더(header)/페이로드(payload) 값 등 패킷 에서 추출하여 비교할 수 있는 TCP/IP의 Layer1부터 Layer7까지의 조건들이 해당한다.

[156] 다음으로, 상황 조건은 세션 또는 플로우(flow) 등을 통하여 판단할 수 있는 상황(context)과 관련된 조건이다. 본 실시예에서는 인증 시도, 인증 및 통화시 단말 IP의 위치정보(지리적 위치 또는 국가 단위) 등이 포함될 수 있다.

[157] 한편, 조건(540)의 추가적인 정보 요소로서 우선순위(priority)는 비교가 만족되는 복수 개의 규칙이 존재할 경우 동작을 적용해야 할 규칙의 우선순위를 나타낸다.

[158] 동작(550)은 상기 조건이 만족되는 패킷이나 플로우에 대한 처리 방법을 정의한다. 동작은 트래픽 인입 제어 동작, 트래픽 출력 제어 동작, 응용 동작으로 구분될 수 있다. 예를 들면, 트래픽 인입 제어 동작은 패킷 허용, 차단, 복사 등의 특정 네트워크 장치로 인입되는 트래픽에 대한 제어 동작이다. 또한, 트래픽 출력 제어 동작은 패킷 전달 등 특정 네트워크 장치에 출력되는 트래픽에 대한 제어 동작이다. 마지막으로, 응용 동작은 트래픽의 인입/출력 제어 이외의 보안 서비스를 제어하는 기능 프로파일의 적용을 의미할 수 있다. 예컨대, 응용동작은 VoIP/VoLTE 보안 프로파일(Security Profile), IPS 동작 프로파일, URL 필터링(filtering) 프로파일, Anti-virus file 등을 포함할 수 있다.

[159] 한편, 도 2 및 도 3에서 설명된 본 발명의 일 실시예에 따른 정보 모델에서는

동작 정보를 기본 동작과 응용 동작으로 구분하였으나, 도 5 및 도 6에서 설명되는 실시예에 따른 정보 모델에서는 동작 정보를 트래픽 인입 제어 동작, 트래픽 출력 제어 동작, 응용 동작으로 구분하고 있다. 여기에서, 트래픽 인입 제어 동작과 트래픽 출력 제어 동작은 기본 동작을 보다 세분화한 것으로 이해될 수 있다.

[160]

[161] 도 6은 도 5에서 예시한 본 발명의 다른 실시예에 따른 정보 모델의 각 구성 요소별 예시 정보를 설명하기 위한 도면이다.

[162] 먼저, 사건(event)은 앞서 언급된 바와 같이 이벤트 시간(event time)와 사용자 동작(user action)으로 구분될 수 있다. 이벤트 시간(631)의 경우, 인증/통화 시각 정보를 포함할 수 있다. 사용자 동작(632)의 경우 단말 등록/인증과 통화 발/착신을 포함할 수 있다.

[163] 패킷 값 조건(6411)은 통화 패킷의 발/착신지 IP 주소, 발/착신지 포트 번호, 발신전화번호, 세션의 call-id 유형(길이, 문자/숫자, 도메인 표현 여부 등), 통화 신호 메시지의 헤더 순서(From, To, Via, Cseq 등) 및 음성/영상 통화 세션 정보를 나타내는 SDP(Session Description Protocol) 내의 정보의 전부 또는 일부를 포함할 수 있다.

[164] 상황 조건(642)은 통화 호 상태 정보(통화 시도, 통화중, 통화 종료, 통화 실패 등), 가입자 단말 기종 정보(OS버전, 제조사 정보 등) 및 발신지 IP 위치 정보(할당된 IP 제공 사업자, 국가 등), 인증 만료 시간(expire time), 이중 등록 여부, 및 기지국(cell) 위치 정보의 전부 또는 일부를 포함할 수 있다.

[165] 우선순위는 조건이 만족되는 복수 개의 규칙이 존재할 경우 동작을 적용해야 할 규칙의 우선순위를 나타낸다.

[166] 트래픽 인입 제어 동작(651)은 상기 조건이 만족되었을 경우, 해당 패킷을 허용하는 동작, 차단하는 동작, 및 미러링(mirroring)하는 동작을 포함할 수 있다.

[167] 트래픽 출력 제어 동작(652)는 해당 패킷을 복사하여 VoIP 보안 컨트롤러(120)로 전달하기(mirroring) 등을 포함할 수 있다.

[168] 마지막으로, 응용 동작(653)은 인증 실패시 동작, 상기 상황 조건에 따른 호 상태 별 호 제어 동작, 네트워크 장치가 VoIP 보안 컨트롤러(120)나 VoIP 보안 컨트롤러(130-1,...,130-N)의 별도 제어 없이 직접 트래픽 차단/허용 여부를 판단할 수 있는 VoIP/VoLTE 보안 프로파일 적용 동작을 포함할 수 있다.

[169]

[170] 본 발명의 다른 실시예에 따른 SDN/NFV 기반 IP 통화 서비스 보안 처리 방법은, 정보 모델에 사건(event) 정보가 추가되고, 적용 목적에 따라서 정보 모델에 포함되는 구체적인 정보의 종류가 달라진다는 점을 제외하면, 도 4를 통해서 설명된 실시예에 따른 방법과 크게 차이가 나지 않는다. 이하에서는, 도 4를 다시 참조하여, 본 발명의 다른 실시예에 따른 SDN/NFV 기반 IP 통화 서비스 보안 처리 방법을 설명한다.

[171] 먼저, 보안 서비스 관리자(110)는 VoIP 보안 컨트롤러(120)로 VoIP 보안 서비스 정책을 포함한 보안 서비스 정책 적용 명령 메시지를 전송한다(S410). 해당 메시지는 앞서 설명한 바와 같이, 사용자 인터페이스 화면이나 커맨드 라인 인터페이스 등을 통해 사용자나 관리자가 설정한 보안 서비스 정책을 포함한다. 보안 서비스 정책으로는 인증 시도, 인증 및 통화시 단말 IP의 위치 정보, 발신번호 변작, 해킹을 위한 단말/장비 검색(scanning), DDOS attack 등의 다량 메시지 발송, 계정 도용 탐지/차단 등이 포함될 수 있다.

[172] 다음으로, VoIP 보안 컨트롤러(120)는 보안 서비스 관리자(110)로부터 전달받은 보안 서비스 정책을 수행할 수 있도록 하는 정보 모델을 생성하며(S420), 생성된 정보 모델을 VoIP 보안 기능들(130)에게 전달한다(S430). 이때, 해당 정보 모델을 수신하는 VoIP 보안 기능들의 범위는 해당 정보 모델이 적용되는 대상에 따라서 달라질 수 있다.

[173] 또한, 앞서 언급된 바와 같이, 정보 모델에는 네트워크 장치(스위치, 라우터 등)를 통해 송수신되는 패킷 및 특정 플로우에 속하는 패킷에 대해 특정 동작을 적용하기 위한 사건(event), 조건(condition) 및 그 조건이 만족되었을 때 해당 동작(action)을 어떻게 수행할지에 대한 동작 절차가 정의되어 있다.

[174] 다음으로, VoIP 보안 컨트롤러(120)로부터 정보 모델을 전달받은 VoIP 보안 기능(130)은 전달받은 정보모델을 해석하여 실제적인 VoIP 보안 서비스를 제공할 수 있는 SDN 컨트롤러(140)의 API(예컨대, OpenFlow의 North Bound API 등)를 호출할 수 있다(S440, S450). 한편, API 호출을 대신하여, VoIP 보안 기능과 SDN 컨트롤러간에 미리 약속된 연동 규격에 맞는 메시지 형태로 변환하여 상기 정보 모델의 해석 내용이 전달될 수도 있다.

[175] 다음으로, SDN 컨트롤러(140)는 VoIP 보안 기능(130)이 요청한 API(또는, 메시지)를 확인하여, 네트워크 장치(150)가 이해할 수 있는 인터페이스(OpenFlow, NetConf 등)로 변환하여 네트워크 장치(150)에게 전달할 수 있다(S460).

[176] 다음으로, 네트워크 장치(150)는 SDN 컨트롤러(140)가 전달한 명령에 따라 플로우 테이블(flow table) 등을 생성하여, 조건에 맞는 패킷이 유입되는지 모니터링 하여, 해당 조건에 맞는 패킷인 경우 패킷 차단, 허용, 전달 등의 제어를 수행한다(S470).

[177] 마지막으로, 네트워크 장치(150), SDN 컨트롤러(140), VoIP 보안 기능(130), VoIP 보안 컨트롤러(120)는 각각 수신된 요청에 따른 결과를 상위 계층으로 전달할 수 있다(S481, S482, S483, S484).

[178]

[179] 이하에서는, 상술된 본 발명의 다른 실시예에 따른 VoIP 서비스 보안 시스템 및 처리 방법이 구체적인 보안 서비스에 적용되는 절차를 예시적으로 설명하기로 한다. 이하에서는 IP 통화 서비스의 불법 인증 시도를 탐지하고 차단하는 보안 서비스의 적용 절차를 예시적으로 설명하기로 한다.

[180] 이하의 설명에서, 정보 모델은 아래의 형태로 기술한다.

[181] 규칙 n: [{(이벤트 시간), (사용자 동작)}, {(패킷 값 조건), (상황 조건)}, {(트래픽 인입 제어), (트래픽 출력 제어), (응용 제어)}]

[182] 대괄호[] 내의 중괄호{}는 사건, 조건, 동작 정보를 구분하며, 중괄호 내의 소괄호()는 정보 모델의 세부 사항을 의미한다. 소괄호가 null인 경우는 해당 사항이 없음을 의미한다.

[183]

[184] <u>적용예#3 - 불법 인증 시도 탐지/차단</u>

[185] VoIP 보안 컨트롤러(120)는 VoIP 보안 기능(130)이 아래 규칙 1 에 의해서 단말에서 인증 시도 이벤트가 발생될 경우 해당 신호 패킷을 복사(미러)하여 복사된 패킷만 VoIP 보안 컨트롤러(120)에게 전달하도록 하고 원 패킷은 라우팅 경로에 따라 전달하여 통화 서비스가 신호 지연 없이 진행되도록 규칙을 설정할 수 있다. 또한, 다소간의 서비스의 지연이 발생하더라도, 정상적인 호/인증 인지 아닌지를 판단한 후 정상인 호/인증인 경우에만 호/인증 flow를 설정하기 위해서 패킷을 복사하지 않고, 그대로 VoIP 보안 컨트롤러(120)로 전달하도록 하는 규칙을 설정할 수도 있다.

[186]

[187] 규칙1: [{(이벤트 시각), (인증시도)}, {(인증시도 메시지), ()}, {(패킷 복사), (), ()}]

[188] 규칙 1은 아래의 의미로 해석될 수 있다.

[189] ⇒ 이벤트 시각: 이벤트 발생 시각(본 적용예에서는 단말 인증 시도 시각)

[190] ⇒ 사용자 동작: 단말 인증 시도

[191] ⇒ 패킷 값 조건: 인증 메시지(SIP인 경우 'Register')

[192] ⇒ 트래픽 인입 제어: 패킷 복사

[193]

[194] 규칙2는 블랙 리스트(black list)로 지정된 IP 주소나 포트(port) 값, 단말 기종 등에서 인증 시도 메시지가 인입된 경우이거나, 인증 만료시간이 임계값 이하인 경우에, 다른 조건을 판단하지 않고 즉시 차단해야 하는 불법적인 인증시도이므로 트래픽 인입 제어에서 패킷 차단 정책을 적용하기 위한 규칙이다. 따라서 규칙2는 정의된 정보 모델에 따라 다음의 형태로 정의될 수 있다.

[195]

[196] 규칙2: [{(이벤트시각), (인증시도)}, {(인증시도 메시지, 블랙리스트로 지정된 IP, port, 인증만료시간(expire time) 값, 단말기종(UserAgent)), ()}, {(패킷 차단), (), ()}]

[197] ⇒ 이벤트 시각: 발생 시각(본 적용예에서는 단말 인증 시도 시각)

[198] ⇒ 사용자 동작: 단말 인증 시도

[199] ⇒ 패킷 값 조건: 인증 메시지 중 블랙 리스트에 저장된 IP, port,

인증만료시간값, 단말기종에 해당하는 조건 값

[200] ⇒ 트래픽 인입 제어: 패킷 차단

[201]

[202] VoIP 보안 컨트롤러(120)는, 상기 규칙1에 의해 VoIP 보안 기능(130)이 관리하는 네트워크 영역(데이터 센터 등의 cloud 영역 또는 SDN 제어 영역 등) 내의 네트워크 장치에서 VoIP 보안 컨트롤러(120)로 복사되어 전달된 인증 시도 패킷에서, 기지국ID(cell-id, Cell_1), 발신지 IP주소(IP_1), 포트번호(port_1), 발신번호(From URI번호, 발신번호_1), 인증 만료 시간(expire time, ET_1), display name (Caller-ID, CID_1))을 추출하여 정상 인증 시도 여부를 판단하여 결과에 맞는 제어를 결정할 수 있다.

[203] 이하에서는, 상기 적용예#3의 불법 인증 시도 탐지/차단에 있어서, 유선(WiFi 등의 mobile VoIP 포함) 단말의 이중등록 패턴 탐지에 기초한 방법, 무선 단말의 이중등록 패턴 탐지에 기초한 방법, 및 인증 만료 시간 비정상 동작 패턴 탐지에 기초한 방법을 보다 구체적으로 설명한다.

[204]

[205] 도 7는 본 발명의 다른 실시예에 따른 유선(WiFi 등의 mobile VoIP 포함) 단말의 불법 인증 시도 탐지에서 이중등록 패턴을 탐지하여 불법 인증 시도를 차단하는 방법을 설명하기 위한 흐름도이다.

[206] 도 7을 참조하면, 유선(WiFi 등의 mobile VoIP포함) 단말의 이중 등록 패턴을 탐지하여 불법 인증 시도를 차단하는 과정은 다음과 같다.

[207] 앞서 설명된 규칙1에 의거하여, VoIP 보안 컨트롤러(120)는, 네트워크 장치로부터 복사/전달된 인증 시도 패킷으로부터, 발신 IP(IP2) 및 발신번호(From 번호)를 추출할 수 있다(S710).

[208] 다음으로, 추출한 발신번호가 현재 시스템의 인증 DB에 저장되어 있는지 조회할 수 있다(S720).

[209] 단계(S720)에서의 조회 결과를 판단하여(S730), 추출된 발신 번호가 인증 DB에 존재하지 않는다면, 해당 인증 시도 패킷을 발송한 단말을 신규 가입(new subscription) 등의 이유로 최초 인증 요청하는 단말로 판단하여, 인증 DB에 추가하고 인증을 진행한다(S740). 만약 추출된 발신 번호가 인증 DB에서 조회가 된다면 이중 등록 여부를 판단하기 위한 다음 단계로 진행한다.

[210] 만약 추출된 발신 번호가 인증 DB에서 조회가 된다면, 현재 인증 요청 패킷의 발신 IP(IP2)와, 해당 번호로 이전에 인증 요청 메시지를 보낸 발신 IP(예컨대, IP1)가 일치하는지 비교하고(S750), 만약 양자가 동일하다면, 단말의 이동(예컨대, IP 변동 등)이 없는 상황 하에서 인증 만료시간 값(ET1)의 인증 주기에 따라 주기적으로 발송되는 재인증 요청 메시지인 것으로 판단하고 다음 처리를 진행한다.

[211] 단계(S750)에서, 현재 인증 요청 패킷의 발신 IP(IP2)와, 해당 번호로 이전에 인증 요청 메시지를 보낸 발신 IP(IP1)가 일치하지 않는 것으로 판단된 경우,

정상적인 단말의 이동(예컨대, IP 변경)인지, 부정적인 인증시도인지를 판단하기 위해 ET2(현재 인증요청 메시지의 인증 만료시간(expire time) 값)과 ET1(이전 인증요청 메시지의 인증 만료시간 값)를 각각 추출 한다(S760).

[212] 정상적인 단말 이동(예컨대, IP변경)이라면, 기존 IP(IP1)에서는 인증요청 메시지가 더 이상 유입되지 않고, 새로운 IP 주소인 IP2에서만 인증요청 메시지가 유입될 것이기 때문에, IP1에서 인증 요청 메시지를 보냈을 때의 ET1 시간 범위 내에 IP1에서 인증 요청메시지가 들어오는지 확인한다(S770).

[213] 상기 단계(S770)에서의 확인 결과, ET1 시간 범위 내에 IP1에서 인증 요청 메시지가 유입되는 경우, 기존 단말은 위치 변경 없이 그대로 있음을 알 수 있고, 이 경우 IP2에서 유입된 인증 요청 메시지는 해킹 등에 의해 부정적인 사용을 목적으로 타 단말 또는 장비에서 인증을 시도하는 것으로 판단할 수 있다.

[214] 따라서, 상기 단계(S770)에서 ET1 시간 범위 내에 IP1에서 인증 요청 메시지가 유입되는 경우, IP2로부터의 인증 요청 메시지를 부정 인증 요청으로 판단하고 IP2에서의 인증 요청을 차단하거나, 기 인증 성공 처리한 경우에는 인증 실패 메시지를 전송하여 인증 차단한다(S780). 그리고, 인증 DB에서 해당 단말 번호의 인증 IP는 IP1으로 유지한다. 블랙리스트 IP 관리를 위해 부정적인 인증 시도가 발생한 IP2(또는 port(port2)), 인증 만료시간 값(ET2), 단말기종(UserAgent2) 값 및 값들의 조합 조건)는 블랙리스트 후보 DB에 저장/관리할 수 있다. IP2에서의 인증 또는 호 시도가 일정 횟수를 초과하는 경우 블랙리스트 정보에 추가할 수 있다. 블랙리스트 DB에 추가할 경우 향후 IP2(또는 port(port2)), 인증 만료시간 값(ET2), 단말기종(UserAgent2) 값 및 값들의 조합 조건)에서 유입되는 인증 또는 통화시도 메시지는 상기 규칙2에 의해서 모두 차단된다.

[215] 상기 단계(S770)에서, ET1 시간 범위 내에 IP1에서 인증 요청 메시지가 유입되지 않는 경우, 정상적으로 단말의 IP가 IP1에서 IP2로 이동(또는 DHCP 등으로 IP 변경)된 것으로 판단하여, IP2에서 유입된 인증 요청 메시지를 정상적으로 처리하고(S790), 이후 인증 DB에서 해당 단말 번호의 인증 IP는 IP2로 관리한다.

[216] 한편 상기 단계(S780)에서 IP2에서 유입되는 인증 요청 및 통화 요청 메시지를 차단하기 위해서 VoIP 보안 기능(130)이 보안 컨트롤러(120)으로 IP2에서 부정 인증 시도가 발생했음을 통보할 수 있다. 이 경우, 보안 컨트롤러(120)는 VoIP 보안 기능(130)에서 IP2로부터 시도되는 인증 및 통화를 차단하기 위해 하기 규칙3 및 규칙4를 VoIP 보안 기능(130)으로 전달할 수 있다.

[217]

[218] 규칙3: [{(), (인증 시도)}, {(인증시도 메시지, IP2), ()}, {(패킷 차단), (), ()}]

[219] ⇒ 사용자 동작: 인증 시도

[220] ⇒ 패킷 값 조건: 인증 메시지 중 발신지 IP가 IP2에 해당하는 조건 값(또는 port(port2)), 인증 만료시간 값(ET2), 단말기종(UserAgent2) 값 및 값들의 조합 조건)

[221] ⇒ 트래픽 인입 제어: 패킷 차단

[222]

[223] 규칙4: [{(), (통화 시도)}, {(통화시도 메시지, IP2), ()}, {(패킷 차단), (), ()}]

[224] ⇒ 사용자 동작: 통화 시도

[225] ⇒ 패킷 값 조건: 통화 메시지 중 발신지 IP가 IP2에 해당하는 조건 값(또는 port(port2)), 인증 만료시간 값(ET2), 단말기종(UserAgent2) 값 및 값들의 조합 조건)

[226] ⇒ 트래픽 인입 제어: 패킷 차단

[227]

[228] 도 8은 본 발명의 다른 실시예에 따른 무선 단말의 불법 인증 시도 탐지에서 이중등록 패턴을 탐지하여 불법 인증 시도를 차단하는 방법을 설명하기 위한 흐름도이다.

[229] 도 8을 참조하면, 무선 단말(예컨대, 셀룰러 이동통신 단말(VoLTE 단말))의 이중 등록 패턴을 탐지하여 불법 인증 시도를 차단하는 과정은 다음과 같다.

[230] 도 7을 통해서도 설명된 바와 같이, VoIP 보안 컨트롤러(120)는, 앞서 설명된 규칙1에 의거하여, 네트워크 장치로부터 복사되어 전달된 인증 시도 패킷으로부터, 기지국 ID(기지국 코드값, SIP P-Access-Network-Info 헤더 값, Cell-ID2) 및 발신번호(From 번호)를 추출할 수 있다(S810).

[231] 다음으로, 추출한 발신번호가 현재 시스템의 인증 DB에 저장되어 있는지 조회할 수 있다(S820).

[232] 단계(S820)에서의 조회 결과를 판단하여(S830), 추출된 발신 번호가 인증 DB에 존재하지 않는다면, 해당 인증 시도 패킷을 발송한 단말을 신규 가입(new subscription) 등의 이유로 최초 인증 요청하는 단말로 판단하여, 인증 DB에 추가하고 인증을 진행한다(S840). 만약 추출된 발신 번호가 인증 DB에서 조회가 된다면 이중 등록 여부를 판단하기 위한 다음 단계로 진행한다.

[233] 만약 추출된 발신 번호가 인증 DB에서 조회가 된다면, 현재 인증 요청 메시지의 기지국 ID(Cell-ID2)와 해당 번호로 이전에 인증 요청 메시지를 보낸 기지국 ID(Cell-ID1)가 일치하는지 비교하고(S850), 만약 양자가 동일하다면, 단말의 이동(즉, 기지국 변경; 핸드오버)이 없는 상황 하에서 인증 만료시간 값(ET1)의 인증 주기 에 따라 주기적으로 발송되는 재인증 요청 메시지인 것으로 판단하고 다음 처리를 진행한다.

[234] 단계(S850)에서, 현재 인증 요청 메시지의 기지국 ID(Cell-ID2)와 이전 인증 요청 메시지의 기지국 ID(Cell-ID1)가 일치하지 않는 것으로 판단된 경우, 정상적인 단말 이동(기지국 변경)인지, 부정적인 인증시도인지 판단하기 위해 ET1(현 인증요청 메시지의 인증 만료시간(expire time) 값)과 ET2(이전 인증요청 메시지의 인증 만료시간 값)를 각각 추출 한다(S860).

[235] 정상적인 단말 이동(예컨대, 기지국 변경)이라면, 기존 기지국(Cell-ID1)에서는 인증요청 메시지가 더 이상 유입되지 않고, 새로운 기지국(Cell-ID2) 에서만

인증요청 메시지가 유입될 것이기 때문에, Cell-ID1에서 인증 요청 메시지를 보냈을 때의 ET1 시간 범위 내에 Cell-ID1 에서 인증 요청메시지가 유입되는지 확인한다(S870).

[236] 상기 단계(S870)에서의 확인 결과, ET1 시간 범위 내에 Cell-ID1에서 인증 요청 메시지가 유입되는 경우, 기존 단말은 위치 변경 없이 그대로 있음을 알 수 있고, 이 경우 Cell-ID2에서 유입된 인증 요청 메시지는 해킹 등에 의해 부정적인 사용을 목적으로 타 단말 또는 장비에서 인증을 시도하는 것으로 판단할 수 있다.

[237] 따라서, 상기 단계(S870)에서 ET1 시간 범위 내에 Cell-ID1에서 인증 요청 메시지가 유입되는 경우, Cell-ID2로부터의 인증 요청 메시지를 부정 인증 요청으로 판단하고 Cell-ID2에서의 인증 요청을 차단하거나, 기 인증 성공 처리한 경우에는 인증 실패 메시지를 전송하여 인증 차단한다(S880).

[238] 상기 단계(S870)에서 ET1 시간 범위 내에 Cell-ID1에서 인증 요청 메시지가 유입되지 않는 경우, 정상적으로 단말의 기지국 ID가 Cell-ID1에서 Cell-ID2로 변동된 것으로 판단하여, Cell-ID2에서 유입된 인증 요청 메시지를 정상적으로 처리하고(S890), 이후 인증 DB에서 해당 단말 번호의 인증 기지국 ID는 Cell-ID2로 관리한다.

[239]

[240] 도 9는 본 발명의 다른 실시예에 따른 VoIP 및 VoLTE 단말의 불법 인증 시도 탐지에서 인증 만료시간의 비정상 동작 패턴을 탐지하여 불법 인증 시도를 차단하는 방법을 설명하기 위한 흐름도이다.

[241] 도 9를 참조하면, VoIP 및 VoLTE 단말의 인증 만료시간의 비정상 동작 패턴을 탐지하여 불법 인증 시도를 차단하는 과정은 다음과 같다.

[242] 도 7을 통해서도 설명된 바와 같이, VoIP 보안 컨트롤러(120)는, 앞서 설명된 규칙1에 의거하여, 네트워크 장치로부터 복사되어 전달된 인증 시도 패킷으로부터, 발신 IP(IP2) 및 발신번호(From 번호)를 추출할 수 있다(S910).

[243] 다음으로, 추출한 발신번호가 현재 시스템의 인증 DB에 저장되어 있는지 조회할 수 있다(S920).

[244] 단계(S920)에서의 조회 결과를 판단하여(S930), 추출된 발신 번호가 인증 DB에 존재하지 않는다면, 해당 인증 시도 패킷을 발송한 단말을 신규 가입(new subscription) 등의 이유로 최초 인증 요청하는 단말로 판단하여, 인증 DB에 추가하고 인증을 진행한다(S940). 만약 추출된 발신 번호가 인증 DB에서 조회가 된다면 이중 등록 여부를 판단하기 위한 다음 단계로 진행한다.

[245] 만약 추출된 발신 번호가 인증 DB에서 조회가 된다면, 현재 인증 요청 메시지의 발신 IP(IP2)와, 해당 번호로 이전에 인증 요청 메시지를 보낸 발신 IP(IP1)가 일치하는지 비교하고(S950), 만약 양자가 동일하다면, 단말의 이동(예컨대, IP 변동 등)이 없는 상황하에서 인증 만료시간 값(ET1)의 인증 주기에 따라 주기적으로 발송되는 재인증 요청 메시지인 것으로 판단하고 다음

처리를 진행한다.

[246] 단계(S950)에서, 현재 인증 요청 패킷의 발신 IP(IP2)와, 해당 번호로 이전에 인증 요청 메시지를 보낸 발신 IP(IP1)가 일치하지 않는 것으로 판단된 경우, 정상적인 단말의 이동(예컨대, IP 변경)인지, 부정적인 인증시도인지를 판단하기 위해 ET2(현재 인증요청 메시지의 인증 만료시간(expire time) 값)과 ET1(이전 인증요청 메시지의 인증 만료시간 값)를 각각 추출 한다(S960).

[247] 일반적으로, 부정적인 인증을 시도하는 목적은 인증 성공 후 통화요금을 내지 않고 통화하거나, 사업자 간에 정산되어야 하는 망 접속료를 중간에서 편취하거나, 또는 고가의 요금이 부과되는 번호(예컨대, 국제전화 등)로 불법적인 전화를 걸어 그 요금을 수익화하기 위한 목적이라 할 수 있다. 따라서 부정적인 인증을 시도하는 경우 정상적인 인증 만료시간(Expire Time)보다 매우 작은 값의 인증 만료시간값으로 조작하여 사용한다.

[248] 따라서, 단계(S970)에서는, ET1 값과 ET2 값을 상호 비교한다.

[249] 단계(S970)에서, ET2가 ET1과 같거나 큰 것으로 판단된다면(즉, 현재 인증요청 메시지의 인증 만료시간 값이 이전 인증요청메시지의 인증 만료시간 값보다 작지 않게 설정된 경우), 부정 인증이 아닌 것으로 판단하여 다음 처리를 진행한다.

[250] 그러나, 단계(S970)에서, ET2가 ET1보다 작은 것으로 판단된다면(즉, 현재 인증요청 메시지의 인증 만료시간 값이 이전 인증요청메시지의 인증 만료시간 값보다 작게 설정된 경우), 부정 인증여부 가능성이 있는 것으로 판단할 수 있다. 이 경우, 보다 정확한 판단을 위해 이 후 인증 요청 메시지의 실제 발생 주기를 측정할 수 있다. 정상적인 경우는 ET2의 1/3~1/2 시간 이내에 재인증을 요청하지만, 부정 인증을 시도하는 경우는 이보다 월등히 짧은 시간 주기로 재인증을 요청한다. 따라서 운용자가 지정한 임계 주기값(1/5, 1/10, 1/100 등) 보다 짧은 주기로 재인증 요청이 발생하는지를 판단할 수 있다(S980).

[251] 단계(S980)에서 판단한 결과, 재인증 요청 주기가 임계값보다 짧지 않은 경우, 정상적인 주기값 변경으로 판단하고 인증처리를 진행한다.

[252] 단계(S980)에서 판단한 결과, 재인증 요청 주기가 임계값보다 짧은 경우, 부정 인증 요청으로 판단하고, 해당 IP(IP2)에서 전송되는 인증 요청은 실패처리를 하거나, 기 인증 성공 처리한 경우에는 인증 실패 메시지를 전송하여 인증 차단한다(S990). 그리고, 인증 DB에서 해당 단말 번호의 인증 IP는 IP1으로 유지한다. 블랙리스트 IP 관리를 위해 부정적인 인증 시도가 발생한 IP2는 블랙리스트 후보 DB에 저장/관리할 수 있다. IP2에서의 인증 또는 호 시도가 일정 횟수를 초과하는 경우 블랙리스트 IP에 추가할 수 있다. 블랙리스트 DB에 추가할 경우 향후 IP2에서 유입되는 인증 또는 통화시도 메시지는 상기 규칙2에 의해서 모두 차단된다.

[253]

[254] 본 발명에 따른 방법들은 다양한 컴퓨터 수단을 통해 수행될 수 있는 프로그램

명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 컴퓨터 판독 가능 매체에 기록되는 프로그램 명령은 본 발명을 위해 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[255] 컴퓨터 판독 가능 매체의 예에는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함한다. 상술한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 적어도 하나의 소프트웨어 모듈로 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[256] 이상 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

[257]

청구범위

[청구항 1] 소프트웨어 정의 네트워킹(SDN, software-defined networking) 기반의 중앙 집중형 VoIP(Voice over IP) 서비스 보안 시스템으로서,
VoIP 보안 서비스를 이용하기 위해 필요한 보안 서비스 정책을 설정하고 관리하는 보안 서비스 관리자(Security Service Manager);
상기 보안 서비스 관리자를 통해 전달받은 보안 서비스 정책을 소정의 정보 모델로 생성하여 VoIP 보안 기능(VoIP security function)에 전달하는 VoIP 보안 컨트롤러(VoIP Security Controller); 및
상기 VoIP 보안 컨트롤러로부터 전달받은 정보 모델에 기초하여, VoIP 보안 서비스를 제공하는 적어도 하나의 VoIP 보안 기능(VoIP security function)을 포함하는, VoIP 서비스 보안 시스템.

[청구항 2] 청구항 1에 있어서,
상기 보안 서비스 관리자는 어플리케이션 게이트웨이(application gateway) 역할을 수행하는, VoIP 서비스 보안 시스템.

[청구항 3] 청구항 1에 있어서,
상기 VoIP 보안 기능은, 적어도 하나의 SDN 스위치를 관리하는 적어도 하나의 SDN 컨트롤러에 연결되는, VoIP 서비스 보안 시스템.

[청구항 4] 청구항 3에 있어서,
상기 VoIP 보안 기능은, 상기 VoIP 보안 컨트롤러로부터 전달받은 정보 모델을 해석하여, 상기 SDN 컨트롤러가 SDN 스위치로 전달할 수 있는 API를 호출하거나 상기 SDN 컨트롤러와 상기 SDN 스위치의 연동 규격에 맞는 메시지 형태로 변환하여 상기 SN 컨트롤러로 전달하는, VoIP 서비스 보안 시스템.

[청구항 5] 청구항 1에 있어서,
상기 정보 모델은, 네트워크 장치를 통해 송수신되는 패킷 또는 특정 플로우에 속하는 패킷에 대해 특정 동작의 적용 여부를 판단하기 위한 조건(condition) 및 상기 조건이 만족되었을 때 수행될 동작(action)을 정의하는 동작 정보를 포함하는, VoIP 서비스 보안 시스템.

[청구항 6] 청구항 5에 있어서,
상기 조건은 단일 패킷에서 판단할 수 있는 패킷 값 조건과, 세션(session) 또는 플로우(flow) 등을 통하여 판단할 수 있는 상황(context) 조건을 포함하는, VoIP 서비스 보안 시스템.

[청구항 7] 청구항 5에 있어서,
상기 동작 정보는 트래픽 인입 제어 동작, 트래픽 출력 제어 동작, 및 보안 서비스를 제어하는 기능 프로파일(profile)을 적용하는 응용 동작(advanced action)을 포함하는, VoIP 서비스 보안 시스템.

[청구항 8] 청구항 5에 있어서,

상기 정보 모델은, 상기 조건과 상기 동작의 적용 대상을 정의하는 사건(event) 정보를 추가로 포함하는, VoIP 서비스 보안 시스템.

[청구항 9] 청구항 8에 있어서,
상기 사건 정보는 이벤트 시간(event time) 정보와 사용자 동작(user action) 정보를 포함하는, VoIP 서비스 보안 시스템.

[청구항 10] 청구항 1에 있어서,
상기 VoIP 보안 기능은 가상 머신 상에서 동작하는, VoIP 서비스 보안 시스템.

[청구항 11] 소프트웨어 정의 네트워킹(SDN, software-defined networking) 기반의 중앙 집중형 VoIP(Voice over IP) 서비스 보안 처리 방법으로서,
보안 서비스 관리자(Security Service Manager)가 VoIP 보안 서비스를 이용하기 위해 필요한 보안 서비스 정책을 생성하는 단계;
VoIP 보안 기능(VoIP security function)가 상기 보안 서비스 정책을 수신하고, 상기 보안 서비스 정책을 소정의 정보 모델로 생성하여 적어도 하나의 VoIP 보안 기능(VoIP security function)에 전달하는 단계; 및
상기 적어도 하나의 VoIP 보안 기능이, 상기 전달받은 정보 모델에 기초하여, VoIP 보안 서비스를 제공하는 단계를 포함하는, VoIP 서비스 보안 처리 방법.

[청구항 12] 청구항 11에 있어서,
상기 보안 서비스 관리자는 어플리케이션 게이트웨이(application gateway) 역할을 수행하는, VoIP 서비스 보안 처리 방법.

[청구항 13] 청구항 11에 있어서,
상기 VoIP 보안 기능은, 적어도 하나의 SDN 스위치를 관리하는 적어도 하나의 SDN 컨트롤러에 연결되는, VoIP 서비스 보안 처리 방법.

[청구항 14] 청구항 13에 있어서,
상기 VoIP 보안 기능이, 상기 VoIP 보안 컨트롤러로부터 전달받은 정보 모델을 해석하여, 상기 SDN 컨트롤러가 SDN 스위치로 전달할 수 있는 API를 호출하거나 상기 SDN 컨트롤러와 상기 SDN 스위치의 연동 규격에 맞는 메시지 형태로 변환하여 상기 SDN 컨트롤러로 전달하는 단계를 추가로 포함하는, VoIP 서비스 보안 처리 방법.

[청구항 15] 청구항 11에 있어서,
상기 정보 모델은, 네트워크 장치를 통해 송수신되는 패킷 또는 특정 플로우에 속하는 패킷에 대해 특정 동작의 적용 여부를 판단하기 위한 조건(condition) 및 상기 조건이 만족되었을 때 수행될 동작(action)을 정의하는 동작 정보를 포함하는, VoIP 서비스 보안 처리 방법.

[청구항 16] 청구항 15에 있어서,
상기 조건은 단일 패킷에서 판단할 수 있는 패킷 값 조건과, 세션(session) 또는 플로우(flow) 등을 통하여 판단할 수 있는 상황(context) 조건을

포함하는, VoIP 서비스 보안 처리 방법.

[청구항 17] 청구항 15에 있어서,
상기 동작 정보는 트래픽 인입 제어 동작, 트래픽 출력 제어 동작, 및 보안 서비스를 제어하는 기능 프로파일(profile)을 적용하는 응용 동작(advanced action)을 포함하는, VoIP 서비스 보안 처리 방법.

[청구항 18] 청구항 15에 있어서,
상기 정보 모델은, 상기 조건과 상기 동작의 적용 대상을 정의하는 사건(event) 정보를 추가로 포함하는, VoIP 서비스 보안 처리 방법.

[청구항 19] 청구항 8에 있어서,
상기 사건 정보는 이벤트 시간(event time) 정보와 사용자 동작(user action) 정보를 포함하는, VoIP 서비스 보안 처리 방법.

[청구항 20] 소프트웨어 정의 네트워킹(SDN, software-defined networking) 기반의 중앙 집중형 VoIP(Voice over IP) 보안 시스템에서, 보안 서비스 관리자(Security Service Manager) 및 적어도 하나의 VoIP 보안 기능(VoIP security function)과 연동하는 VoIP 보안 컨트롤러(VoIP Security Controller)의 동작 방법으로서,
상기 보안 서비스 관리자로부터 VoIP 보안 서비스를 이용하기 위해 필요한 보안 서비스 정책을 수신하는 단계;
상기 보안 서비스 정책을 소정의 정보 모델로 생성하여 상기 적어도 하나의 VoIP 보안 기능(VoIP security function)에 전달하는 단계; 및
상기 적어도 하나의 VoIP 보안 기능으로부터 상기 소정의 정보 모델에 따라 수행된 상기 보안 서비스 정책의 수행 결과를 수신하는 단계를 포함한, VoIP 서비스 보안 컨트롤러의 동작 방법.

[청구항 21] 청구항 20에 있어서,
상기 정보 모델은, 네트워크 장치를 통해 송수신되는 패킷 또는 특정 플로우에 속하는 패킷에 대해 특정 동작의 적용 여부를 판단하기 위한 조건(condition) 및 상기 조건이 만족되었을 때 수행될 동작(action)을 정의하는 동작 정보를 포함하는, VoIP 서비스 보안 컨트롤러의 동작 방법.

[청구항 22] 청구항 21에 있어서,
상기 조건은 단일 패킷에서 판단할 수 있는 패킷 값 조건과, 세션(session) 또는 플로우(flow) 등을 통하여 판단할 수 있는 상황(context) 조건을 포함하는, VoIP 서비스 보안 컨트롤러의 동작 방법.

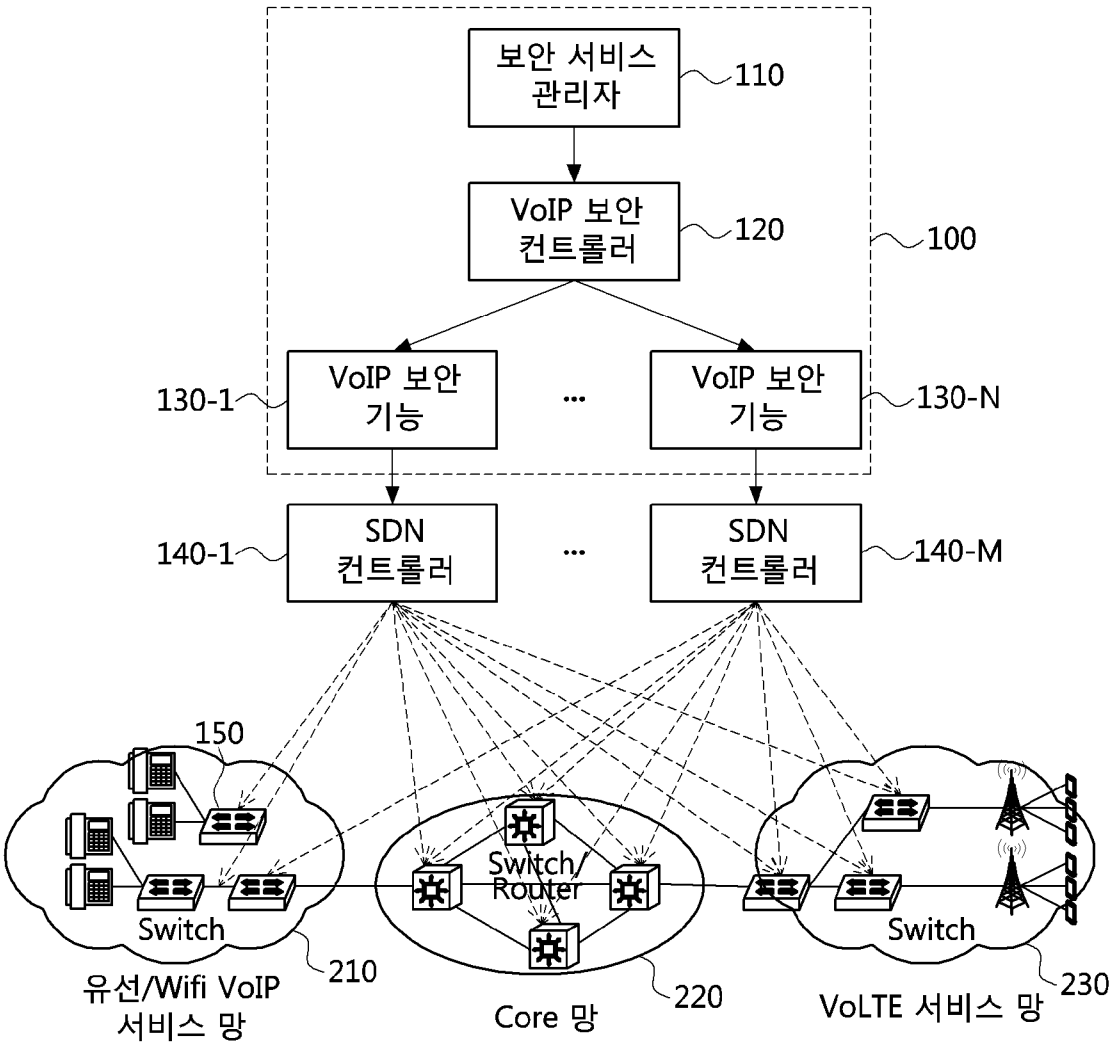
[청구항 23] 청구항 21에 있어서,
상기 동작 정보는 트래픽 인입 제어 동작, 트래픽 출력 제어 동작, 및 보안 서비스를 제어하는 기능 프로파일(profile)을 적용하는 응용 동작(advanced action)을 포함하는, VoIP 서비스 보안 컨트롤러의 동작 방법.

[청구항 24] 청구항 21에 있어서,

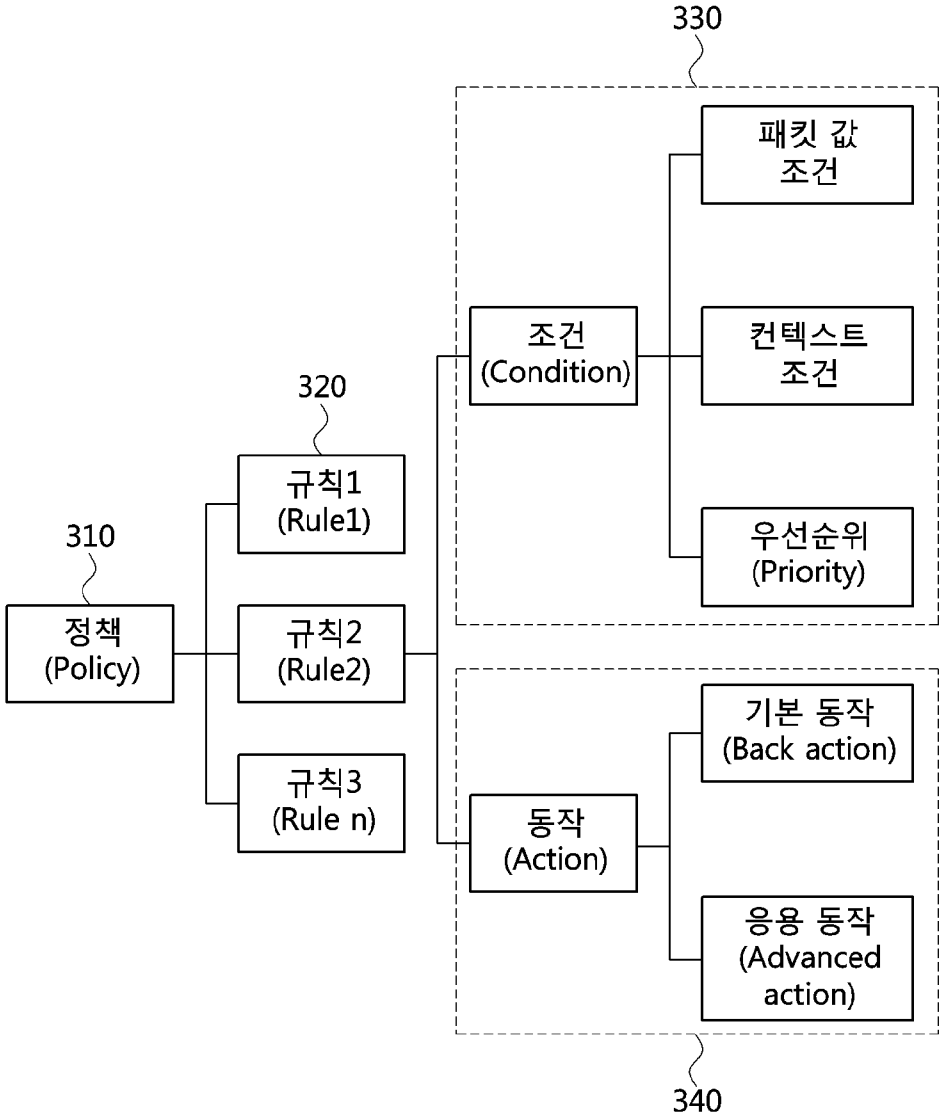
상기 정보 모델은, 상기 조건과 상기 동작의 적용 대상을 정의하는 사건(event) 정보를 추가로 포함하는, VoIP 서비스 보안 컨트롤러의 동작 방법.

[청구항 25] 청구항 24에 있어서,
상기 사건 정보는 이벤트 시간(event time) 정보와 사용자 동작(user action) 정보를 포함하는, VoIP 서비스 보안 컨트롤러의 동작 방법.

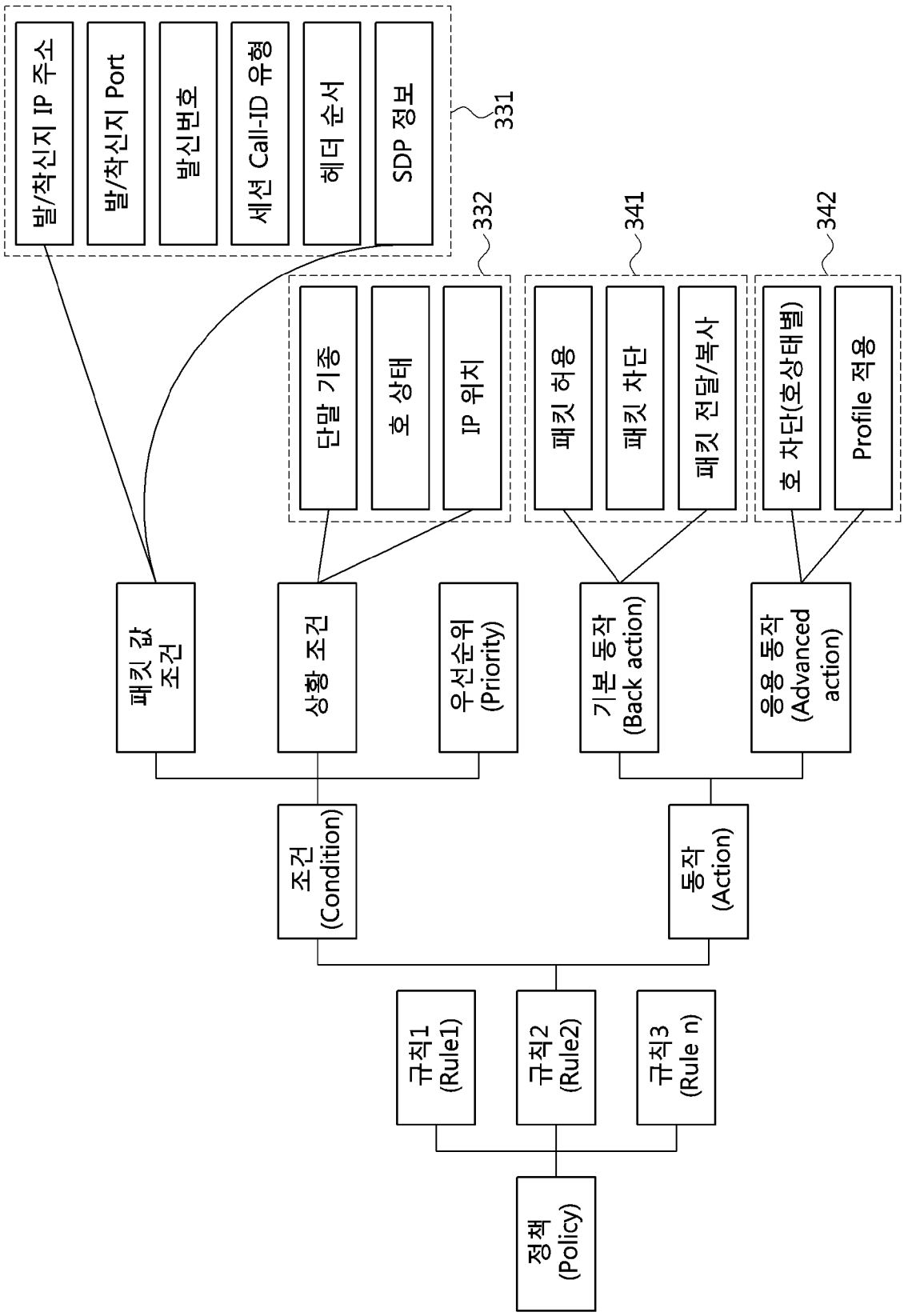
[도1]


보안 서비스 관리자
110
VoIP 보안 컨트롤러
120
100
VoIP 보안 기능
130-1
...
VoIP 보안 기능
130-N
SDN 컨트롤러
140-1
...
SDN 컨트롤러
140-M
150
Switch
유선/Wifi VoIP 서비스 망
210
Switch/ Router
Core 망
220
Switch
VoLTE 서비스 망
230

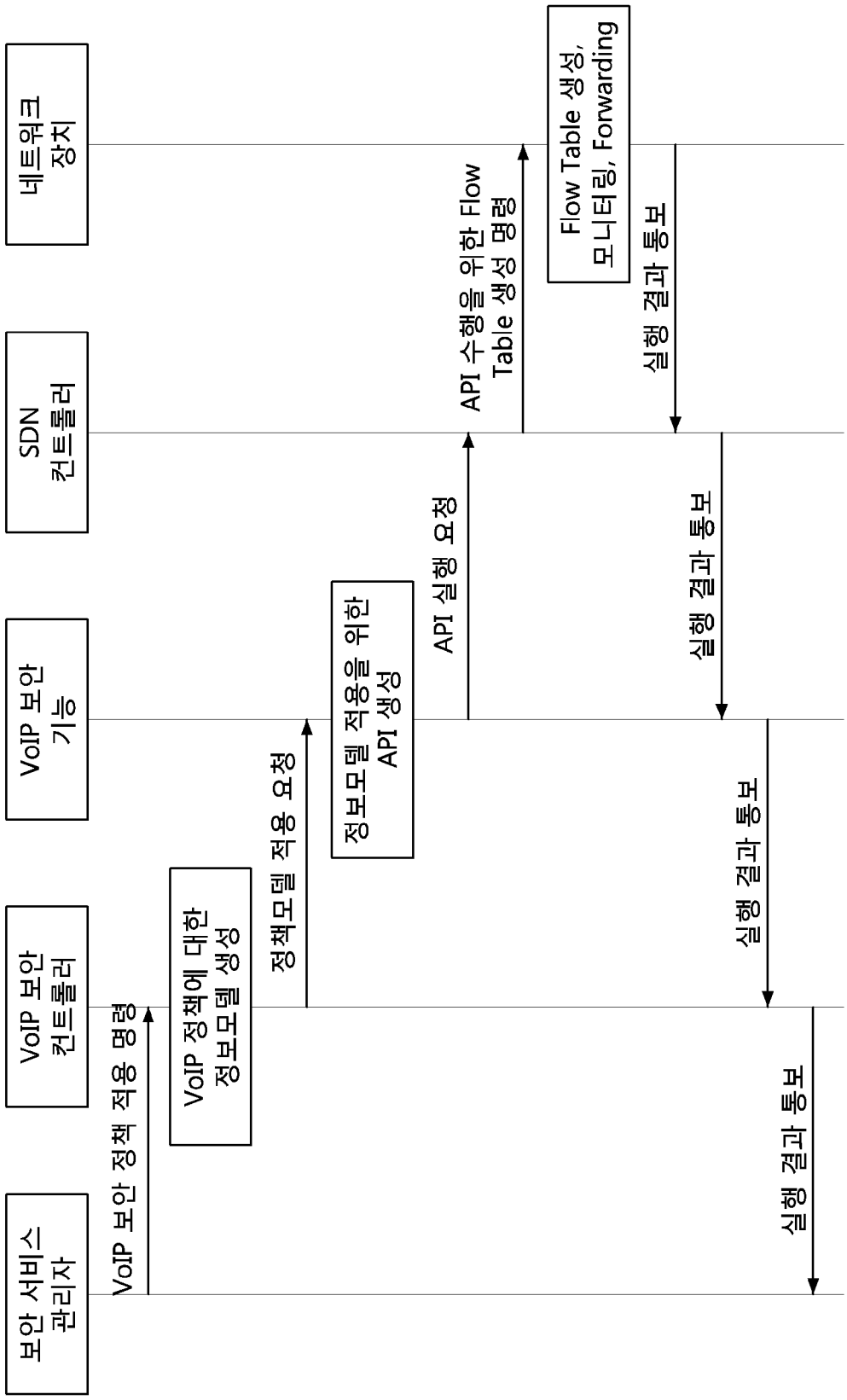
[도2]


330
패킷 값
조건
조건
(Condition)
컨텍스트
조건
320
규칙1
(Rule1)
310
우선순위
(Priority)
정책
(Policy)
규칙2
(Rule2)
기본 동작
(Back action)
규칙3
(Rule n)
동작
(Action)
응용 동작
(Advanced
action)
340

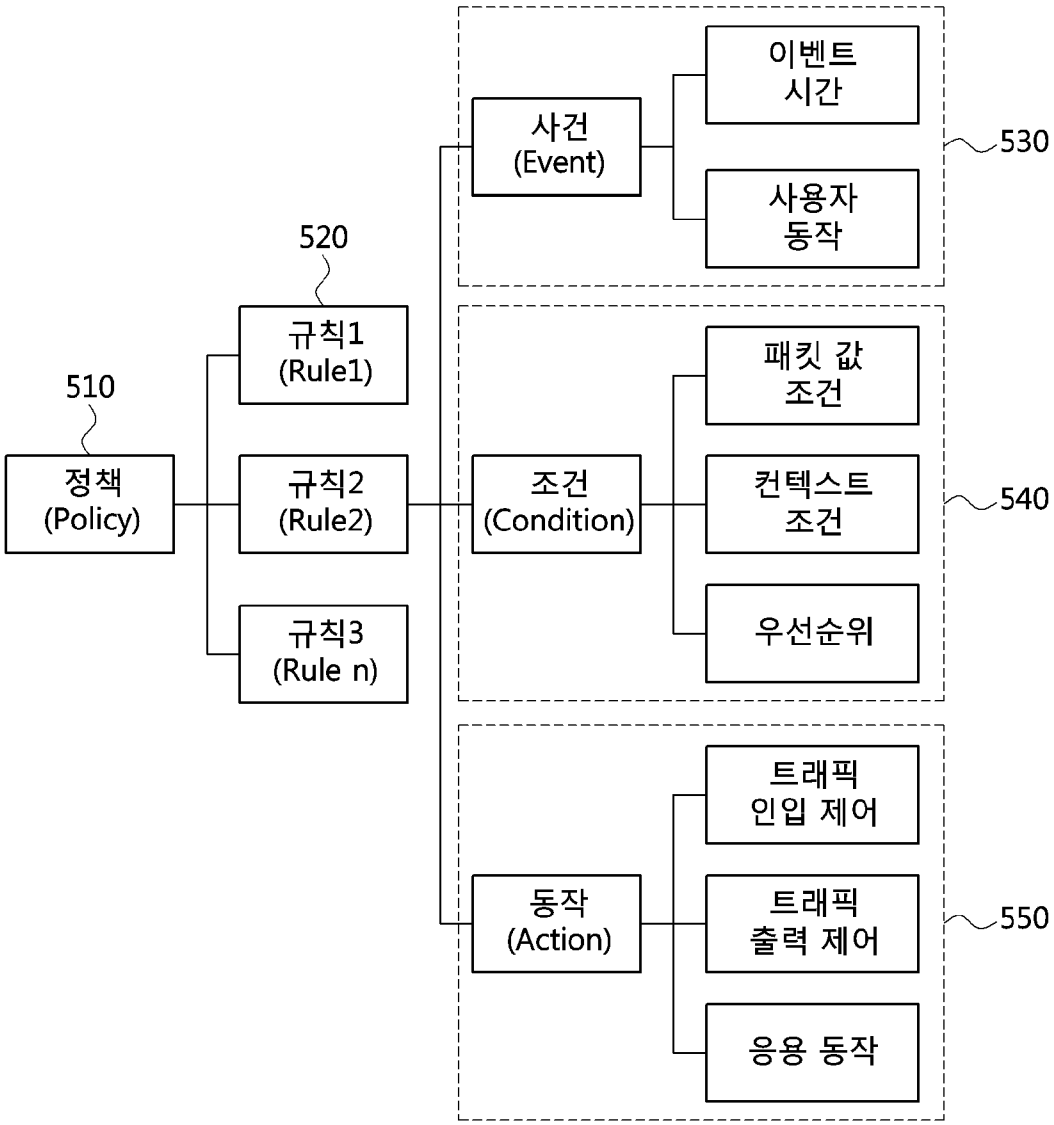
[도3]


정책 (Policy)
규칙1 (Rule1)
규칙2 (Rule2)
규칙3 (Rule n)
조건 (Condition)
동작 (Action)
패킷 값 조건
상황 조건
우선순위 (Priority)
기본 동작 (Back action)
응용 동작 (Advanced action)
발/착신지 IP 주소
발/착신지 Port
발신번호
세션 Call-ID 유형
헤더 순서
SDP 정보
331
단말 기종
호 상태
IP 위치
332
패킷 허용
패킷 차단
패킷 전달/복사
341
호 차단(호상태별)
Profile 적용
342

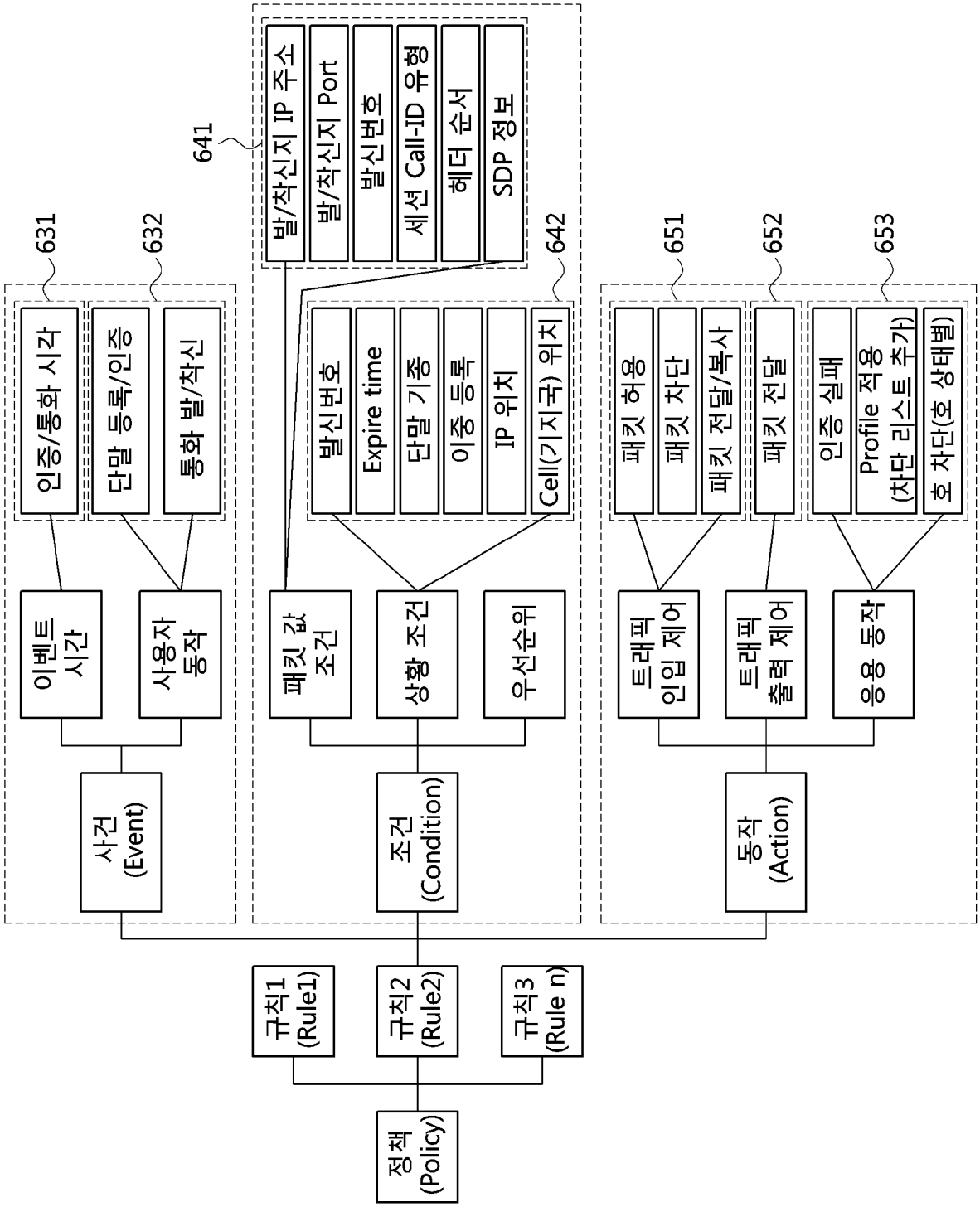
[도4]


보안 서비스 관리자
VoIP 보안 컨트롤러
VoIP 보안 기능
SDN 컨트롤러
네트워크 장치
VoIP 보안 정책 적용 명령
VoIP 정책에 대한 정보모델 생성
정책모델 적용 요청
정보모델 적용을 위한 API 생성
API 실행 요청
API 수행을 위한 Flow Table 생성 명령
Flow Table 생성, 모니터링, Forwarding
실행 결과 통보
실행 결과 통보
실행 결과 통보
실행 결과 통보

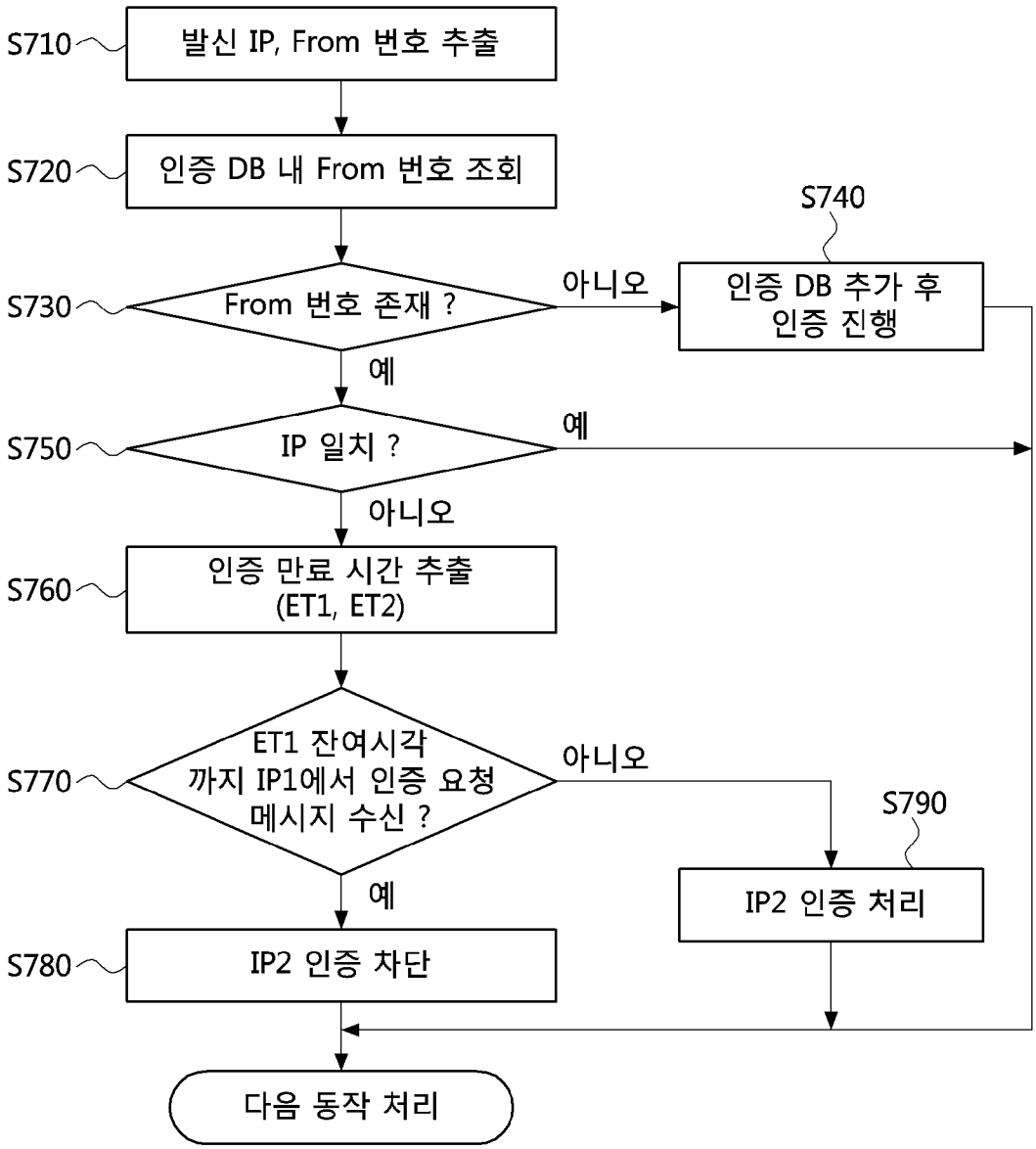
[도5]


510
정책
(Policy)
520
규칙1
(Rule1)
규칙2
(Rule2)
규칙3
(Rule n)
사건
(Event)
조건
(Condition)
동작
(Action)
이벤트
시간
사용자
동작
530
패킷 값
조건
컨텍스트
조건
우선순위
540
트래픽
인입 제어
트래픽
출력 제어
응용 동작
550

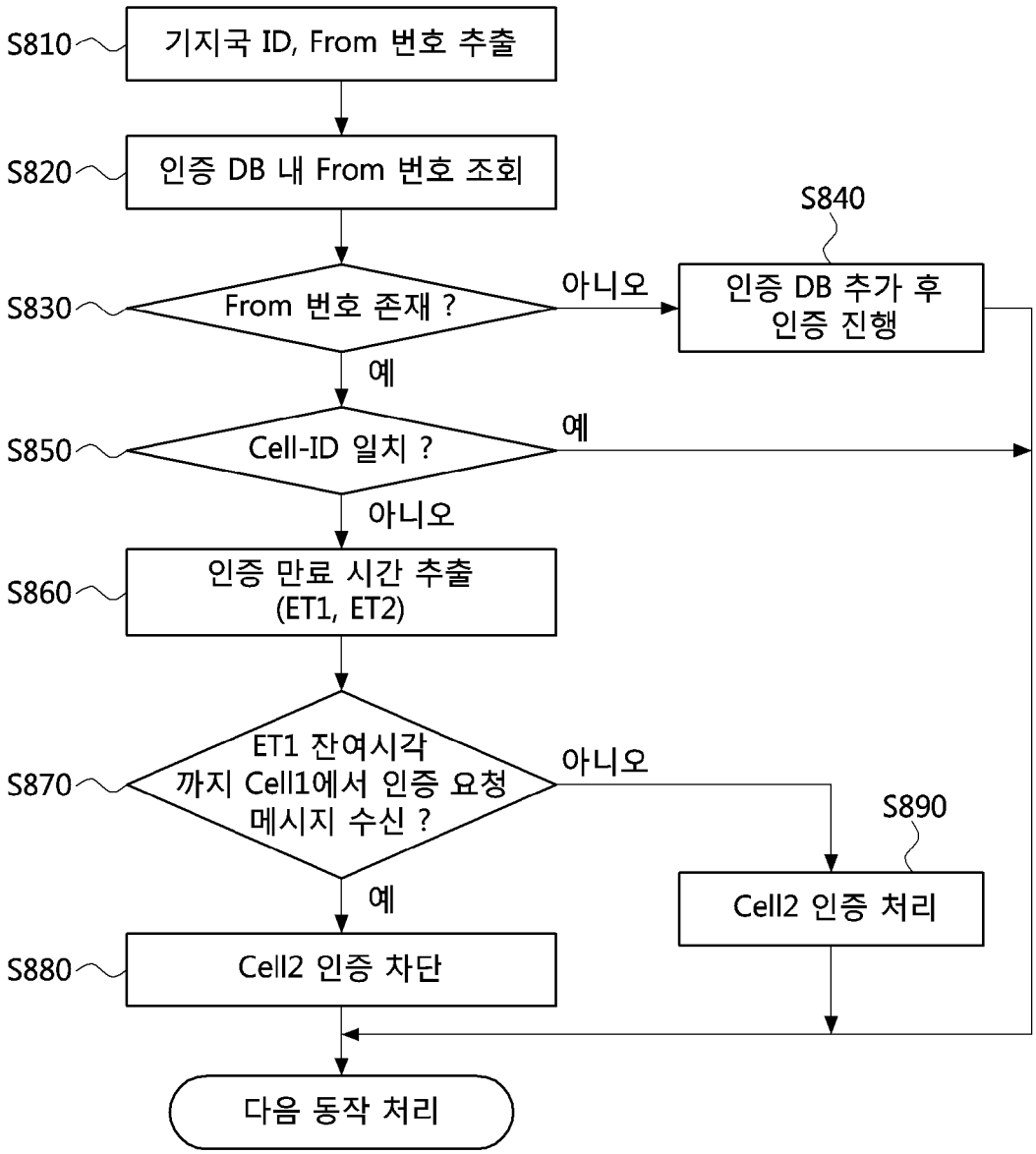
[도6]


641
631
632
642
651
652
653
발/착신지 IP 주소
발/착신지 Port
발신번호
세션 Call-ID 유형
헤더 순서
SDP 정보
인증/통화 시각
단말 등록/인증
통화 발/착신
발신번호
Expire time
단말 기종
이중 등록
IP 위치
Cell(기지국) 위치
패킷 허용
패킷 차단
패킷 전달/복사
패킷 전달
인증 실패
Profile 적용
(차단 리스트 추가)
호 차단(호 상태별)
이벤트 시간
사용자 동작
패킷 값 조건
상황 조건
우선순위
트래픽 인입 제어
트래픽 출력 제어
응용 동작
사건 (Event)
조건 (Condition)
동작 (Action)
규칙1 (Rule1)
규칙2 (Rule2)
규칙3 (Rule n)
정책 (Policy)

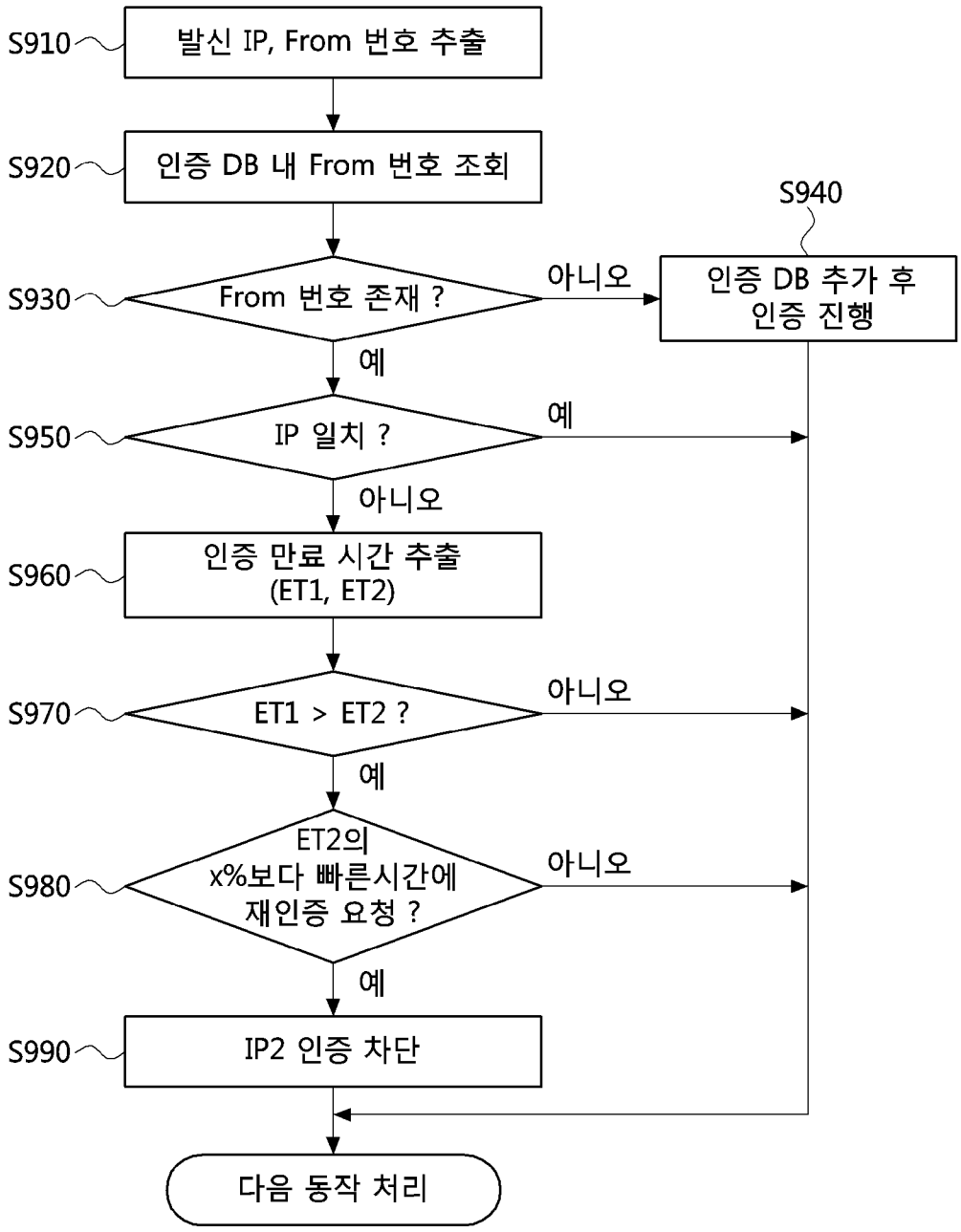
[도7]


S710
발신 IP, From 번호 추출
S720
인증 DB 내 From 번호 조회
S730
From 번호 존재 ?
아니오
S740
인증 DB 추가 후 인증 진행
예
S750
IP 일치 ?
예
아니오
S760
인증 만료 시간 추출 (ET1, ET2)
S770
ET1 잔여시각 까지 IP1에서 인증 요청 메시지 수신 ?
아니오
S790
IP2 인증 처리
예
S780
IP2 인증 차단
다음 동작 처리

[도8]


S810
기지국 ID, From 번호 추출
S820
인증 DB 내 From 번호 조회
S830
From 번호 존재 ?
아니오
S840
인증 DB 추가 후 인증 진행
예
S850
Cell-ID 일치 ?
예
아니오
S860
인증 만료 시간 추출 (ET1, ET2)
S870
ET1 잔여시각 까지 Cell1에서 인증 요청 메시지 수신 ?
아니오
S890
Cell2 인증 처리
예
S880
Cell2 인증 차단
다음 동작 처리

[도9]


S910
발신 IP, From 번호 추출
S920
인증 DB 내 From 번호 조회
S940
S930
From 번호 존재 ?
아니오
인증 DB 추가 후
인증 진행
예
S950
IP 일치 ?
예
아니오
S960
인증 만료 시간 추출
(ET1, ET2)
S970
ET1 > ET2 ?
아니오
예
S980
ET2의
x%보다 빠른시간에
재인증 요청 ?
아니오
예
S990
IP2 인증 차단
다음 동작 처리