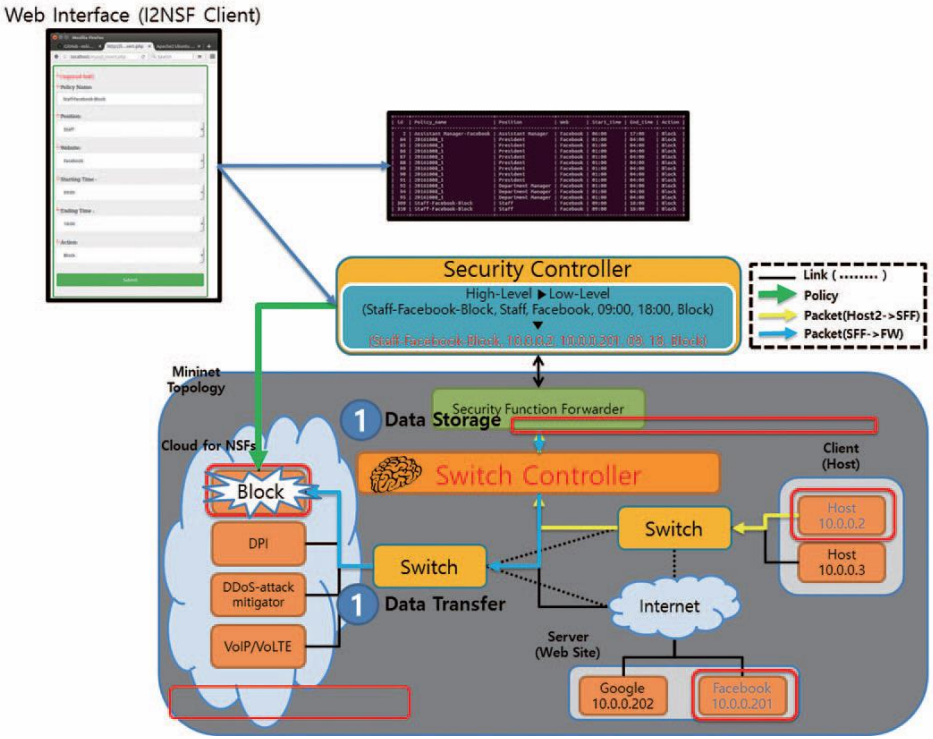
성균관대학교

맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술

맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술

기술 개요

- SDN/NFV를 통한 맞춤형 네트워크 보안 서비스를 항시 제공하는 Software-Defined Security Controller, 네트워크 보안 기능들 간의 표준 인터페이스 및 통신 모듈
- 보안 시스템 관리자로부터 생성된 사용자 입장의 보안 정책들을 효과적으로 네트워크 보안 기능들에게 전달 및 집행 할 수 있는 기술



<SDNSNA>

맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술

세부 기술 내용

- **보안 정책의 생성 및 집행을 위한 Web UI 개발**
  - **네트워크 보안 기능들 (NSFs)을 위한 보안 정책 생성 UI**
  - 보안 정책의 CRUD (CREATE, READ, UPDATE, DELETE) 작업이 가능하게 하도록 사용자 편의성을 고려한 UI
  - 다양한 보안 서비스 별 상이한 보안 정책들의 집행을 수용할 수 있도록 Yang을 이용한 data modeling
- **보안 시스템 관리자와 보안 컨트롤러 간 표준 인터페이스**
  - **I2NSF 클라이언트를 이용하여 사용자 입장에서의 보안 정책을 보안 컨트롤러에게 전달하는 인터페이스**
  - 보안 프레임워크를 구성하고 보안 컨트롤러와 보안 관리 시스템, 네트워크 보안 기능(NSF)으로 구성된 보안 관리
- **RESTCONF 프로토콜을 이용한 통신 기법**
  - **RESTCONF 클라이언트 및 서버**
  - 보안 시스템 관리자의 어플리케이션 측과 보안 컨트롤러간의 안전한 통신을 위해 RESTCONF 프로토콜을 사용하는 클라이언트 및 서버
  - **표준화 진행•Yang Data Modeling 및 표준 인터페이스 API를 위한 표준화 진행**

맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술

기술의 특징

- SDN/NFV 인프라를 이용한 다양한 소프트웨어 보안 솔루션의 가상화
  - 사용자의 요구사항에 최적화된 보안 서비스를 효과적으로 제공
- 기존의 Legacy 시스템과의 비교
  - 네트워크 가상화가 지원되지 않는 보안 관리 시스템은 이종의 하드웨어 관리가 복잡, 네트워크 가상화를 통해 하드웨어 장비 설치 비용 감소 및 소프트웨어 중심의 제어 프로토콜 제공
  - 신속하고 간편한 새로운 보안 프로토콜의 추가

관련 특허

No.	특허번호	발명의 명칭
1	10-2016-0163114	네트워크 가상화 환경에서 보안 관리를 위한 장치 및 방법

활용분야

- 국내외 보안 장비 및 솔루션의 통합 관리
  - 국내외 기업에서 제공하는 보안 장비 및 솔루션의 상이한 기준을 통합하여 벤더 간 호환성을 확보하여 유지보수 비용, 인력 절감 및 새로운 보안 서비스 도입의 확정성, 유연성 관리용이성, 보안의 효율성을 확보
- IoT와 클라우드 서비스 분야에 활용
  - IoT와 클라우드 서비스 등 새롭게 등장하는 인터넷 환경 서비스에 다양한 제품과 수많은 서비스를 통합 관리 및 보안 통제에 활용
- 국내외 사이버테러 및 보안위협 대응에 활용
  - 진화하는 사이버테러 및 보안위협에 보안기능을 동적으로 재구성하고 지능적으로 분석/대응할 수 있는 자립형 보안기술을 활용하여 다양한 형태의 사이버테러 예방 및 대응

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년06월01일
(11) 등록번호 10-1863236
(24) 등록일자 2018년05월25일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 63/20 (2013.01)
(21) 출원번호 10-2017-0079120
(22) 출원일자 2017년06월22일
심사청구일자 2017년07월25일
(30) 우선권주장
1020160163114 2016년12월01일 대한민국(KR)
(56) 선행기술조사문헌
Framework for Interface to Network Security Functions fraft-ietf-i2nsf-framework-04(I2NSF internet draft, 2016.10.30.)*
I2NSF Data Model of Consumer-Facing Interface for Security Management draft-jeong-i2nsf-consumer-facing-interface-dm-00(Network Working Group Internet-Draft, 2016.11.13.)*
WO2016000160 A1
KR101669518 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
성균관대학교산학협력단
경기도 수원시 장안구 서부로 2066 (천천동, 성균관대학교내)
(72) 발명자
정재훈
부산광역시 금정구 금강로 225 장전동 717 벽산블루밍장전디자인시티 204동 1501호
김형식
경기도 수원시 장안구 화산로 85 천천동 333 천천푸르지오아파트 132-401
(뒷면에 계속)
(74) 대리인
특허법인로알

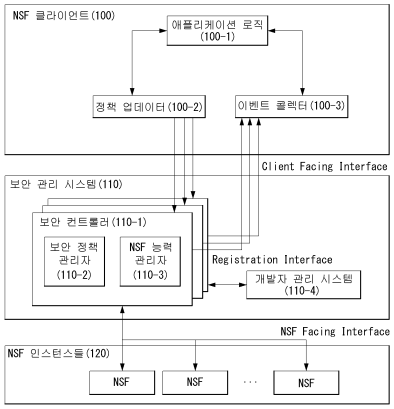
전체 청구항 수 : 총 18 항 심사관 : 남기영

(54) 발명의 명칭 **네트워크 가상화 환경에서 보안 관리를 위한 장치 및 방법**

(57) 요 약

본 발명은 네트워크 가상화 기반의 네트워크 보안 기능(Network Security Function, NSF) 제공에 관한 I2NSF (Interface to Network Security Functions) 프레임워크에서 NSF 클라이언트가 효과적으로 NSF의 보안 관리를 실현하기 위한 구조를 제시한다. 제안하는 구조를 통해 NSF 클라이언트가 직접 상위 수준의 보안 정책을 수립하고 NSF에서 발생하는 이벤트를 피드백 받음으로써 결과적으로 효과적인 보안 관리를 실현할 수 있다. 본 발명에서는 I2NSF 프레임워크에서 NSF 클라이언트의 보안 관리를 위해 추가되는 구성 요소들이 어떤 기능들을 수행하는지를 기술한다.

대 표 도 - 도1



(72) 발명자

오상학

경기도 수원시 장안구 서부로 2066 천천동 300 성균관대학교자연과학캠퍼스 38-22 (율전동) 슬기샘 302호

김은수

경기도 수원시 장안구 서부로 2066 천천동 300 성균관대학교자연과학캠퍼스 26-35, 205호[율전동 439-10]

이 발명을 지원한 국가연구개발사업

과제고유번호 2016-0-00078
부처명 정부)미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신.방송 기술개발사업 및 표준화사업
연구과제명 [EZ-IITP]맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발
기 여 율 1/1
주관기관 한국전자통신연구원
연구기간 2016.04.01 ~ 2016.12.31

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

보안 관리 시스템의 보안 관리 방법에 있어서,

NSF(Network Security Functions) 클라이언트로부터 보안 공격을 차단 또는 완화하기 위한 상위 수준(high-level) 보안 정책을 수신하는 단계;

상기 상위 수준 보안 정책을 상기 보안 관리 시스템에 등록된 NSF 능력(capability)과 관련된 하위 수준(low-level) 보안 정책들에 매핑하는 단계; 및

상기 하위 수준 보안 정책들을 적어도 하나의 NSF에 전달하는 단계; 를 포함하되, 상기 NSF 클라이언트는 애플리케이션 로직, 정책 업데이터 및/또는 이벤트 콜렉터를 포함하는, 보안 관리 방법.

청구항 2

삭제

청구항 3

제 1 항에 있어서,

상기 애플리케이션 로직은 상기 상위 수준 보안 정책을 생성 및 업데이트하여 상기 정책 업데이터로 전송하며,

상기 정책 업데이터는 상기 상위 수준 보안 정책을 클라이언트 지향 인터페이스(Client Facing Interface)를 통해 상기 보안 관리 시스템으로 전달하며,

상기 이벤트 콜렉터는 상기 상위 수준 보안 정책의 생성 또는 업데이트에 기초가 되는 이벤트를 수신하여 상기 애플리케이션 로직으로 전송하는, 보안 관리 방법.

청구항 4

제 3 항에 있어서,

상기 상위 수준 보안 정책은 특정 공격 호스트, 서버 및 네트워크의 IP(Internet Protocol) 주소가 포함된 블랙리스트를 기반으로 생성되는, 보안 관리 방법.

청구항 5

제 4 항에 있어서,

상기 이벤트는 상기 블랙리스트로의 포함 기준을 만족하는 IP 주소에 해당하는, 보안 관리 방법.

청구항 6

제 3 항에 있어서,

상기 상위 수준 보안 정책은 차단 웹 사이트 및 차단 시간이 포함된 블랙리스트를 기반으로 생성되는, 보안 관리 방법.

청구항 7

제 3 항에 있어서,

상기 상위 수준 보안 정책은 특정 SIP(Session Initiation Protocol) 장치의 IP 주소, 소스 포트, 만료 시간, 사용자 에이전트 또는 SIP URI가 포함된 불법 장치 차단 목록을 기반으로 생성되는, 보안 관리 방법.

청구항 8

제 7 항에 있어서,

상기 이벤트는 상기 불법 장치 차단 목록으로의 포함 기준을 만족하는 도메인 정보에 해당하는, 보안 관리 방법.

청구항 9

제 1 항에 있어서,

상기 보안 관리 시스템은 보안 정책 관리자, NSF 능력 관리자 또는 개발자 관리 시스템을 포함하는, 보안 관리 방법.

청구항 10

제 9 항에 있어서,

상기 개발자 관리 시스템은 등록 인터페이스를 통해 NSF 능력을 등록 및 업데이트하며,

상기 NSF 능력 관리자는 상기 개발자 관리 시스템에 등록 및 업데이트된 NSF 능력을 저장하며,

상기 보안 정책 관리자는 상기 상위 수준 보안 정책을 상기 NSF 능력 관리자에 저장된 상기 NSF 능력과 관련된 상기 하위 수준 보안 정책들과 매핑하고, 상기 하위 수준 보안 정책들을 NSF 지향 인터페이스(NSF Facing Interface)를 통해 상기 적어도 하나의 NSF로 전달하는, 보안 관리 방법.

청구항 11

보안 관리 장치에 있어서,

보안 관리 아키텍처를 구현하는 프로세서; 를 포함하되,

상기 프로세서는,

보안 공격을 차단 또는 완화하기 위한 상위 수준(high-level) 보안 정책을 생성하는 NSF(Network Security Functions) 클라이언트;

상기 NSF 클라이언트로부터 상기 상위 수준 보안 정책을 수신하고, 상기 상위 수준 보안 정책을 상기 보안 관리 시스템에 등록된 NSF 능력(capability)과 관련된 하위 수준(low-level) 보안 정책들에 매핑하는, 보안 관리 시스템; 및

상기 보안 관리 시스템으로부터 상기 하위 수준 보안 정책들을 수신하는 적어도 하나의 NSF; 를 구현하되,

상기 NSF 클라이언트는 애플리케이션 로직, 정책 업데이터 및/또는 이벤트 콜렉터를 포함하는, 보안 관리 장치.

청구항 12

삭제

청구항 13

제 11 항에 있어서,

상기 애플리케이션 로직은 상기 상위 수준 보안 정책을 생성 및 업데이트하여 상기 정책 업데이터로 전송하며,

상기 정책 업데이터는 상기 상위 수준 보안 정책을 클라이언트 지향 인터페이스(Client Facing Interface)를 통해 상기 보안 관리 시스템으로 전달하며,

상기 이벤트 콜렉터는 상기 상위 수준 보안 정책의 생성 또는 업데이트에 기초가 되는 이벤트를 수신하여 상기 애플리케이션 로직으로 전송하는, 보안 관리 장치.

청구항 14

제 13 항에 있어서,

상기 상위 수준 보안 정책은 특정 공격 호스트, 서버 및 네트워크의 IP(Internet Protocol) 주소가 포함된 블랙

리스트를 기반으로 생성되는, 보안 관리 장치.

청구항 15

제 14 항에 있어서,

상기 이벤트는 상기 블랙리스트로의 포함 기준을 만족하는 IP 주소에 해당하는, 보안 관리 장치.

청구항 16

제 13 항에 있어서,

상기 상위 수준 보안 정책은 차단 웹 사이트 및 차단 시간이 포함된 블랙리스트를 기반으로 생성되는, 보안 관리 장치.

청구항 17

제 13 항에 있어서,

상기 상위 수준 보안 정책은 특정 SIP(Session Initiation Protocol) 장치의 IP 주소, 소스 포트, 만료 시간, 사용자 에이전트 또는 SIP URI가 포함된 불법 장치 차단 목록을 기반으로 생성되는, 보안 관리 장치.

청구항 18

제 17 항에 있어서,

상기 이벤트는 상기 불법 장치 차단 목록으로의 포함 기준을 만족하는 도메인 정보에 해당하는, 보안 관리 장치.

청구항 19

제 11 항에 있어서,

상기 보안 관리 시스템은 보안 정책 관리자, NSF 능력 관리자 또는 개발자 관리 시스템을 포함하는, 보안 관리 장치.

청구항 20

제 19 항에 있어서,

상기 개발자 관리 시스템은 등록 인터페이스를 통해 NSF 능력을 등록 및 업데이트하며,

상기 NSF 능력 관리자는 상기 개발자 관리 시스템에 등록 및 업데이트된 NSF 능력을 저장하며,

상기 보안 정책 관리자는 상기 상위 수준 보안 정책을 상기 NSF 능력 관리자에 저장된 상기 NSF 능력과 관련된 상기 하위 수준 보안 정책들과 매핑하고, 상기 하위 수준 보안 정책들을 NSF 지향 인터페이스(NSF Facing Interface)를 통해 상기 적어도 하나의 NSF로 전달하는, 보안 관리 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 네트워크 기능 가상화의 보안 관리 아키텍처에 관한 것이다.

배 경 기 술

[0002] 네트워크 기능 가상화(Network Functions Virtualization; NFV)는 네트워크 산업을 위한 새로운 영역이다. NFV는 네트워크 기능을 전용 하드웨어 기기에서 분리하여 범용 제품 서버에서 실행되는 순수 소프트웨어 인스턴스로 이러한 기능을 구현함으로써 네트워크 배포 및 유지 관리 비용 절감을 보장한다. 방화벽, 침입 탐지 시스템(Intrusion Detection System; IDS) 및 침입 방지 시스템 (Intrusion Protection System; IPS)과 같은 NSF(Network Security Functions)는, 실시간 보안 요구 사항에 따라 자동으로 제공되고 동적으로 이동될 수 있는 가상 네트워크 기능으로서 제공될 수도 있다. 본 명세서에서는 일반 NFV가 아닌 NSF에 초점을 맞춰

기술한다.

[0003] NFV 기반 보안 애플리케이션을 성공적으로 배포하기 위해서는, NSF가 여러 공급 업체에서 개발하거나 다른 네트워크 운영 업체에서 관리하기 때문에 표준화가 중요하다. 최근에는 NSF를 제어하기 위한 몇 가지 기본 표준 인터페이스가 IETF(Internet Engineering Task Force)라는 국제 인터넷 표준화 기구의 일부인 I2NSF (Interface to Network Security Functions) 워킹 그룹에 의해 개발중이다. 따라서, 몇 년 내로, 다양한 NSF가 표준 인터페이스를 통해 NFV 기반 보안 서비스의 중앙 관리 엔티티인 보안 컨트롤러라는 네트워크 엔티티에 의해 원격으로 제어될 수 있다.

[0004] 그러나, 보안 컨트롤러는 네트워크 상의 보안 정책을 생성하고 관리할 수 있는 임의의 NSF 클라이언트(예를 들어, I2NSF 클라이언트)와 통신해야 하기 때문에 NF 기반 보안 애플리케이션에서 표준 개발을 위한 여지가 여전히 남아있다. 본 명세서에서는 보안 컨트롤러로 관리되는 모든 NFV 기반 보안 애플리케이션을 NFV 지원 네트워크에 심리스하게/원활하게 통합하는 계층화된 아키텍처를 제안한다. 이 아키텍처를 통해 애플리케이션 사용자는 사용자 친화적인 방법으로 상위 수준의 보안 정책을 시행할 수 있다.

발명의 내용

해결하려는 과제

[0005] 본 명세서에서는 NFV를 이용한 NSF 기반의 보안 관리를 위한 일반적인 아키텍처 제시를 목적으로 한다.

[0006] 또한, 본 명세서는 제안된 프레임 워크가 위험 도메인의 블랙리스트, 시간별 액세스 제어 정책 및 VoIP(Voice over IP)-VoLTE(Voice over LTE) 서비스에 대한 의심스러운 전화 탐지와 같은 몇 가지 실제 공격 시나리오를 완화할 수 있는 방법 제안을 목적으로 한다.

[0007] 이를 위해, 본 명세서에서는 구체적으로 제안된 아키텍처의 상세한 구현을 설명하기 위한 예제를 중심으로 설명한다. 이에 기초하여, 향후 다양한 네트워크 공격을 완화할 수 있는 가능성을 보여주기 위해 제안된 프레임 워크가 완벽하게 구현될 수 있다.

과제의 해결 수단

[0008] 본 발명의 일 실시예에 따르면, 네트워크 기능 가상화에서의 보안 관리를 위한 아키텍처는 I2NSF 프레임 워크, 애플리케이션 로직, 정책 업데이터 및 이벤트 콜렉터를 포함할 수 있다.

발명의 효과

[0009] 본 발명의 일 실시예에 따른 아키텍처를 통해, 애플리케이션 사용자는 사용자 친화적인 방법으로 상위 수준의 보안 정책을 시행할 수 있다. 보다 상세하게는, 본 발명의 일 실시예에 따른 아키텍처를 통해, 네트워크 리소스 및 프로토콜에 대한 특정 정보가 필요 없는 상위 수준의 보안 인터페이스를 사용자에게 제공함으로써, 사용자에게 친숙한 방식으로 사용자로 하여금 보안 요구 사항을 정의하도록 할 수 있다.

[0010] 또한, 본 발명의 일 실시예에 따른 아키텍처를 통해, NSF 클라이언트가 직접 상위 수준 보안 정책을 수립하고 NSF에서 발생하는 이벤트를 피드백 받음으로써 효율적인 보안 관리를 실현할 수 있다.

도면의 간단한 설명

[0011] 도 1은 NFV에 기반한 보안 관리를 위한 아키텍처를 예시한 도면이다.

도 2는 NSF 클라이언트의 사용자 인터페이스를 예시한 도면이다.

도 3은 Client Facing Interface의 데이터 모델을 예시한 도면이다.

도 4는 I2NSF의 보안 관리 아키텍처를 예시한 도면이다.

도 5는 Malware 도메인 블랙리스트 작성의 보안 관리 아키텍처를 예시한 도면이다.

도 6은 I2NSF 프레임 워크 내의 보안 관리 아키텍처를 예시한 도면이다.

도 7은 Malware 도메인 블랙리스트 작성의 보안 관리 아키텍처를 예시한 도면이다.

도 8은 본 발명의 일 실시예에 따른 보안 관리 시스템의 보안 관리 방법에 관한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0012] 본 명세서에서 사용되는 용어는 본 명세서에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어를 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도, 관례 또는 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한 특정 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 실시예의 설명 부분에서 그 의미를 기재할 것이다. 따라서 본 명세서에서 사용되는 용어는, 단순한 용어의 명칭이 아닌 그 용어가 아닌 실질적인 의미와 본 명세서의 전반에 걸친 내용을 토대로 해석되어야 함을 밝혀두고자 한다.

[0013] 더욱이, 이하 첨부 도면들 및 첨부 도면들에 기재된 내용들을 참조하여 실시예를 상세하게 설명하지만, 실시예들에 의해 제한되거나 한정되는 것은 아니다.

[0014] 이하, 첨부한 도면들을 참조하여 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다.

[0016] **[1] 제1 실시예**

[0017] 네트워크 기능 가상화 (NFV)는 네트워크 보안 서비스를 설계하고 배포하는 새로운 방법을 제공하지만, 네트워크 보안 서비스들 사이의 규격/표준화된 네트워크 인터페이스 서비스가 없는 경우, 네트워크 보안 서비스들을 완벽하게 통합하는 실용적인 에코 시스템을 구축하지 못할 수도 있다. 따라서, 본 명세서에서는 NFV를 사용하는 NSF(Network Security Functions) 기반의 보안 관리 서비스를 위한 아키텍처를 제안한다. 제안된 아키텍처는 네트워크 리소스 및 프로토콜에 대한 특정 정보가 필요 없는 상위 수준의 보안 인터페이스를 사용자에게 제공함으로써, 사용자에게 친숙한 방식으로 사용자로 하여금 보안 요구 사항을 정의하도록 할 수 있다.

[0018] 1. 도입

[0019] 제1 실시예에서는 제안된 아키텍처를 위한 기본 구성 요소(예를 들어, 보안 정책 관리자, NSF 능력 관리자, 애플리케이션 논리, 정책 업데이터 및 이벤트 수집기)와 인터페이스 설계 방식을 제안한다. 또한, 제1 실시예에서는 (1) 위험 도메인의 블랙리스트, (2) 시간별 액세스 제어 정책 및 (3) VoIP-VoLTE 서비스에 대한 의심스러운 전화 탐지, 이렇게 세 가지 케이스에 대한 본 발명의 사용예를 중심으로 살펴본다. 또한, 본 명세서에서는 제안된 아키텍처의 구현 방법에 대해 예를 들어 상세히 설명한다. 또한, 본 명세서에서는 제안된 아키텍처를 실제 네트워크 환경에 배치/적용하기 위한 몇 가지 기술적 과제에 대해 살펴본다.

[0020] 이하, 설명의 편의를 위해 주제별로 절을 나누어 설명한다. 2절에서는 NFV 기반의 보안 관리 서비스 아키텍처에 대해 제안한다. 3절에서는 제안된 아키텍처를 사용하는 세 가지 주요 사용예에 대해 설명한다. 4절에서는 실제로 제안된 아키텍처를 사례를 통해 구현하는 방법에 대해 설명한다. 5절에서는 아키텍처 구현에 대한 기술적 문제에 대해 설명한다. 6절에서는 관련 연구에 대한 요약 및 분석 내용을 설명한다. 7절에서는 결론에 대해 살펴본다.

[0021] 2. 아키텍처

[0022] 본 명세서에서는 NFV에 기반한 보안 관리 서비스를 위한 추가 구성 요소를 통합한 계층화된 아키텍처를 제안한다. 본 명세서의 도면들에서 화살표는 기능 구성 요소들 간의 통신을 나타낸다. 특히, 도면에서 양방향 화살표는 양방향으로의 두 구성 요소간 상호 작용을 나타내며, 단방향 화살표는 화살표가 가리키는 방향으로의 두 구성 요소 간 상호 작용을 나타낸다.

[0023] 도 1은 NFV에 기반한 보안 관리를 위한 아키텍처를 예시한 도면이다.

[0024] 도 1을 참조하면, 유연하고 효과적인 보안 정책 시행을 지원하기 위해 제안된 아키텍처는, (1) NSF 클라이언트(100) (2) 보안 관리 시스템(110) 및 (3) NSF 인스턴스들(120), 이렇게 세 가지 계층으로 구성될 수 있다.

[0025] 본 발명의 아키텍처는 유연하고 효과적인 보안 정책 시행을 지원하도록 설계되었다. 본 명세서에서 NSF 클라이언트(100)라는 용어는 NFV 기반의 보안 애플리케이션을 의미한다.

[0026] NSF 클라이언트(100)에서 애플리케이션 로직(100-1)은 상위 수준 보안 정책을 생성할 수 있다. 정책 업데이터(100-2)는 클라이언트 지향 인터페이스(Client Facing interface)를 통해 보안 컨트롤러(110-1)에 정책들을 배포할 수 있다. 보안 컨트롤러(110-1)에서 보안 정책 관리자(110-2)는 상위 수준 정책을 NSF 능력 관리자(110-3)에 등록된 NSF 능력과 관련된 하위 수준 보안 정책에 매핑할 수 있다. 매핑 후, 보안 정책 관리자(110-2)는 NSF 지향 인터페이스(NSF Facing Interface)를 통해 NSF(120)에 해당 정책들을 전달할 수 있다. 이하에서는, 각 네트워크 구성 요소의 동작에 대해 상세히 살펴본다.

[0027] 2.1 보안 정책 관리자(110-2)

[0028] 보안 정책 관리자(110-2)는 Client Facing Interface를 통해 정책 업데이터(100-2)로부터 상위 수준의 정책을 수신하고, 상위 수준의 정책을 NSF 능력 관리자(110-3)에 등록된 특정 NSF 능력과 관련된 여러 하위 수준의 정책들과 매핑하거나 또는 하위 수준의 정책들을 상위 수준의 정책으로 매핑하는 구성 요소이다. 또한, 보안 정책 관리자(110-2)는 이러한 정책들을 NSF Facing Interface를 통해 NSF(들)에게 전달할 수 있다.

[0029] 하위 수준 정책 변경이 필요한 이벤트가 NSF(120)에서 발생하면, NSF(120)는 NSF Facing Interface를 통해 보안 정책 관리자(110-2)에게 이벤트를 전송할 수 있다. 이후, 보안 정책 관리자(110-2)는 Client Facing Interface를 통해 해당 이벤트를 이벤트 콜렉터(100-3)로 전송할 수 있다.

[0030] 2.2 NSF 능력 관리자(110-3)

[0031] NSF 능력 관리자(110-3)는 보안 컨트롤러(110-1)에 통합된 구성일 수 있다. NSF 능력 관리자(110-3)는 등록 인터페이스를 통해 개발자 관리 시스템(110-4)에 등록된 NSF의 능력을 저장하고 이를 보안 정책 관리자(110-2)와 공유하여 보안 정책 관리자(110-2)가 특정 NSF 능력과 관련된 하위 수준 정책을 생성할 수 있도록 할 수 있다. 또한, NSF 능력 관리자(110-3)는 새로운 NSF가 등록될 때마다 등록 인터페이스를 통해 NSF 능력 관리자(110-3)의 관리 테이블에 NSF의 능력을 등록하도록 개발자의 관리 시스템에 요청할 수 있다. 기존의 NSF가 삭제되면 NSF 능력 관리자(110-3)는 관리 테이블에서 NSF의 능력을 제거할 수 있다.

[0032] 2.3 개발자 관리 시스템(110-4)

[0033] 개발자 관리 시스템(110-4)은 등록 인터페이스를 통해 NSF 능력 관리자(110-3)에 새로운 NSF 능력을 등록하는 구성 요소일 수 있다. 등록된 NSF에 업데이트가 있으면, 업데이트된 내용/정보는 개발자 관리 시스템에서 NSF 능력 관리자(110-3)에게 전달될 수 있다.

[0034] 2.4 애플리케이션 로직(100-1)

[0035] 애플리케이션 로직(100-1)은 (보안 관리 아키텍처에서) 보안 공격을 차단 또는 완화하기 위해 상위 수준의 보안 정책을 생성하는 구성일 수 있다. 애플리케이션 로직(100-1)은 이벤트 콜렉터(100-3)로부터 상위 수준의 정책을 업데이트(또는 생성)하는 이벤트를 수신하고, 수집된 이벤트를 기반으로 상위 수준의 정책을 업데이트(또는 생성)할 수 있다. 다음으로, 애플리케이션 로직(100-1)은 최근 업데이트된 정책을 전달하기 위해 상위 수준 정책을 정책 업데이터(100-2)로 전송할 수 있다. 이하의 3절에서는 세 가지 사용예를 통해 애플리케이션 로직(100-1)을 설계하는 방법에 대해 설명한다.

[0036] 2.5 정책 업데이터(100-2)

[0037] 정책 업데이터(100-2)는 애플리케이션 로직(100-1)에 의해 생성된 상위 수준의 보안 정책을 수신하고, 이를 Client Facing Interface를 통해 보안 컨트롤러(110-1)로 배포/전달하는 구성일 수 있다.

[0038] 2.6 이벤트 콜렉터(100-3)

[0039] 이벤트 콜렉터(100-3)는 애플리케이션 로직(100-1)의 상위 수준 정책 업데이트(또는 생성)에 반영되어야 하는 이벤트를 보안 컨트롤러(110-1)로부터 수신할 수 있다. NSF에서 발생하는 이벤트에 따라 하위 수준의 보안 정책이 업데이트될 수 있으므로, NSF에서 이벤트를 수신하는 절차가 필요하다. 이벤트를 수신한 후 이벤트 콜렉터(100-3)는, 이를 애플리케이션 로직(100-1)으로 전달하여 애플리케이션 로직(100-1)이 보안 컨트롤러(110-1)로부터 수신한 이벤트를 기반으로 상위 수준의 보안 정책을 업데이트(또는 생성)하도록 할 수 있다.

[0040] 3. 사용예

[0041] NFV를 기반으로 한 일반적인 아키텍처는 가능한 보안 공격에 대응하도록 설계되었다. 본 절에서는 위험한 도메인의 블랙리스트에 있는 보안 공격 방어, 시간에 따른 액세스 제어 정책 및 VoIP-VoLTE 서비스에 대한 의심스러운 전화의 탐지 절차에 대해 설명한다.

[0042] 3.1 위험한 도메인들의 블랙리스트

[0043] 위험한 도메인(예를 들어, malware 배포에 사용되는 도메인 등) 블랙리스트 작성은 악성 활동이 의심되는 공격 호스트, 서버 및 네트워크의 IP 주소에 대한 블랙리스트를 유지 및 게시하는 것을 의미한다. 위험한 도메인 블랙리스트 작성을 위한 보안 관리 아키텍처의 경우, 위험 도메인 관리자는 보안 관리를 수행하기 위해 애플리케이션 로직의 역할을 담당할 수 있다.

[0044] 위험한 도메인 블랙리스트 작성에 기초하여, 위험한 도메인 리스트는 위험한 도메인 데이터베이스에 저장되며, 애플리케이션 로직 기능을 하는 위험한 도메인 관리자에 의해 수동 또는 자동으로 업데이트될 수 있다. 또한, 위험한 도메인 관리자는 위험한 도메인 데이터 베이스로부터 위험한 도메인 리스트를 주기적으로 로드하고, 새로 추가된 위험한 도메인들과의 패킷 전달을 방지하기 위해 새로운 상위 수준의 보안 정책(예를 들어, IP 주소를 사용하여 위험한 도메인들의 리스트 차단, 블랙리스트 차단)을 생성할 수 있다. 위험한 도메인 관리자는 새로운 상위 수준 보안 정책을 정책 업데이터로 전송할 수 있으며, 정책 업데이트는 수신한 새로운 상위 수준 보안 정책을 보안 컨트롤러에 배포할 수 있다. 보안 컨트롤러는 상위 수준 정책을 하위 수준 정책들에 매핑하고, 하위 수준 보안 정책들을 NSF에 적용할 수 있다.

[0045] NSF가 새로운 위험한 도메인을 탐지하면, 탐지한 도메인에 대응하는 IP 주소를 NSF Facing Interface를 통해 보안 컨트롤러로 전송할 수 있다. 보안 컨트롤러는 이벤트 콜렉터에 해당 IP 주소를 전달할 수 있다. 이벤트 콜렉터는 IP 주소를 위험 도메인 관리자로 전달하면, 이를 기초로 위험 도메인 관리자가 위험 도메인 데이터베이스를 업데이트할 수 있다.

[0046] 3.2 시간별 액세스 제어 정책들

[0047] 시간별 액세스 제어 정책들은 특정 기간 동안 특정 웹 사이트에 대한 사용자의 액세스를 관리할 수 있다. 예를 들어, 회사에서 관리자는 직원이 업무 시간의 집중을 방해하는 Youtube 웹 사이트에 액세스하는 것을 차단할 수 있다.

[0048] NSF 클라이언트는 시간별 접근 제어를 기반으로 애플리케이션 로직에서 차단 웹 사이트 및 차단 시간이 포함된 블랙리스트를 등록할 수 있다. 애플리케이션 로직은 해당 목록을 데이터 베이스에 저장하고 상위 수준의 보안 정책을 생성할 수 있다(예를 들어, 차단 웹 사이트 및 차단 시간을 확인하여 차단 시간 동안의 차단 웹 사이트에 대한 액세스 차단).

[0049] 애플리케이션 로직은 생성한 상위 수준의 보안 정책을 정책 업데이터로 전달하면, 정책 업데이터가 이를 보안 컨트롤러로 전달할 수 있다. 보안 컨트롤러에서 보안 정책 관리자는 상위 수준 정책을 하위 수준 정책들에 매핑한 다음, 이들을 NSF에 전송 및 적용할 수 있다.

[0050] 3.3 VoIP-VoLTE 서비스에 대한 의심스러운 전화 탐지

[0051] VoIP-VoLTE 보안 관리는 불법적인 전화나 인증이 의심되는 SIP(Session Initiation Protocol) 장치의 IP 주소, 소스 포트, 만료 시간, 사용자 에이전트 및 SIP URI가 포함된 불법 장치 차단 목록을 유지 및 게시할 수 있다. 일반 보안 관리 아키텍처에서 VoIP-VoLTE 보안 관리자는 도 1에서의 VoIP-VoLTE 보안 서비스를 위한 애플리케이션 로직 역할을 담당한다.

[0052] VoIP-VoLTE 보안 관리에 기초하여, 불법 장치 정보 목록은 VoIP-VoLTE 데이터 베이스에 저장되며, VoIP-VoLTE 보안 관리자에 의해 수동 또는 자동으로 업데이트될 수 있다. 또한, VoIP-VoLTE 보안 관리자는 주기적으로 VoIP-VoLTE 데이터 베이스로부터 불법 장치 정보 목록을 로드하고, 새로 추가된 VoIP-VoLTE 공격자와의 패킷 전달을 방지하기 위해 새로운 상위 수준의 보안 정책(예를 들어, IP 주소, 소스 포트 등을 사용하는 불법 장치 차단 목록)을 생성할 수 있다. 또한, VoIP-VoLTE 보안 관리자는 생성한 새로운 상위 수준 보안 정책을 정책 업데이터로 전송할 수 있으며, 정책 업데이터는 수신한 상위 수준 보안 정책을 보안 컨트롤러로 배포할 수 있다. 보안 컨트롤러는 상위 수준 정책을 여러 하위 수준 정책들에 매핑하고 하위 수준 보안 정책을 NSF에 적용하게 된다.

[0053] NSF가 도메인으로부터 전달된 비정상적인 메시지 또는 전화를 검출하면, IP 주소, 사용자 에이전트 및 만료 시간 값과 같은 도메인의 정보가 NSF에 의해 NSF Facing Interface를 통해 보안 컨트롤러로 전송될 수 있다. 보안 컨트롤러는 이를 이벤트 콜렉터로 전달할 수 있다. 이벤트 콜렉터는 탐지된 도메인 정보를 VoIP-VoLTE 보안 관리자에게 전달하면, VoIP-VoLTE 보안 관리자는 이에 기초하여 VoIP-VoLTE 데이터베이스를 업데이트할 수 있다.

[0054] 4. 구현

[0055] 본 절에서는 제안된 아키텍처에서 각 구성 요소와 인터페이스를 구현하는 방법에 대해 제안하며, 이때 앞서 상술한 3.3 절의 사용예를 고려한다. 이러한 구현을 통해 착신호에 사기 전화 동작(예를 들어, 비정상적인 시간대에 블랙리스트에 올라있는 위치에서 통화가 이루어지는 동작 등)이 있는지 여부를 확인하여 의심스러운 VoIP-VoLTE 전화의 차단이 가능하다.

[0056] 4.1 NSF 클라이언트

[0057] 관리자에게보다 친숙하고 접근 가능한 관리 서비스를 제공하기 위해, 웹 서버 및 관리자가 상위 수준의 보안 정책을 설정할 수 있는 사용자 인터페이스를 제공하는 몇 개의 웹 페이지가 제공/생성될 수 있다.

[0058] 도 2는 NSF 클라이언트의 사용자 인터페이스를 예시한 도면이다.

[0059] 도 2를 참조하면, 관리자가 보안 정책을 관리하기 위해서는, (1) 정책 업데이터에 대한 정책 설정 페이지와 (2) 이벤트 콜렉터에 대한 로그 메시지 페이지, 이렇게 두 가지 웹 페이지가 고려될 수 있다. YANG은 YANG에서 정의된 데이터로의 HTTP를 통한 접속을 위한 프로그래밍 인터페이스를 제공하는 RESTCONF와 같은 표준 네트워크 프로토콜에 의해 조작된 구성과 상태 데이터를 모델링하는 데 널리 사용되기 때문에, NSF 클라이언트와 보안 관리 시스템 간의 통신을 위한 데이터 모델을 정의하기 위해 YANG이 고려/사용될 수 있다.

[0060] 정책 설정 페이지에서, 특정 시간 동안 블랙리스트에 포함된 국가와 같은 상위 수준의 보안 정책을 정의하기 위한 필드가 생성될 수 있다. 만일, 관리자가 새로운 상위 수준의 보안 정책을 설정하면, NSF 클라이언트의 데이터 모델 파서(parser)가 정책을 해석하고 YANG 데이터 모델에 따라 XML 파일을 생성할 수 있다.

[0061] 로그 메시지 페이지에는, 보안 관리 시스템에서 이벤트 콜렉터로 이벤트가 전달되는 경우, 보안 관리 시스템 및 NSF 인스턴스에서 보안 애플리케이션의 결과 및/또는 기능 구성 요소의 상태를 보고하는 이벤트에 대한 정보가 표시될 수 있다.

[0062] 4.2 Client Facing Interface

[0063] NSF 클라이언트와 보안 관리 시스템 간의 상호 작용을 가능하게 하기 위해 RESTCONF를 기반으로 한 통신 채널이 구현될 수 있다. 또한, NSF 클라이언트는 구현 시 웹 애플리케이션을 기반으로 하기 때문에, 네트워크 구성(NETCONF) 프로토콜 대신 RESTCONF가 선호될 수 있다.

[0064] 또한, Client Facing Interface를 위한 표준화된 데이터 모델이 아직 없기 때문에, 보안 정책 요구 사항에 기반한 데이터 모델이 설계될 필요가 있다.

[0065] 도 3은 Client Facing Interface의 데이터 모델을 예시한 도면이다.

[0066] 도 3에서는 VoIP-VoLTE 서비스에서 의심스러운 전화를 탐지하기 위한 정책 관리와 관련된 데이터 모델 설계의 일부를 보여준다.

[0067] 알려지지 않은 공격 및 조건에 정책을 적용하기 위한 일반적인 데이터 모델이 설계될 수 있다. 이러한 데이터 모델은 (1) 정책 라이프 사이클 관리, (2) 정책 규칙 및 (3) 조치로 구성될 수 있다. (1) 정책 라이프 사이클 관리 필드는 정책 자체의 수명을 결정하기 위해 만료 시간 및/또는 만료 이벤트 세트를 지정할 수 있다. (2) 정책 규칙 필드는 서비스 타입, 조건 및 유효한 시간 간격과 같은 상위 수준 정책에 대한 특정 정보를 나타낼 수 있다. (3) 조치 필드는 어떤 행동을 취해야 하는지를 지정한다. 예를 들어, 허가(permit) 및 미러(mirror) 모두 'true'인 경우, 예외 시간(유효 시간 간격에 포함)에 블랙리스트에 있는 발신자 위치의 통화 트래픽은 차단될 수 있으며, 딥 패킷 검사(Deep Packet Inspection; DPI)를 위해 사전 정의된 호스트로 순차적으로 전달 될 수 있다.

[0068] 4.3 보안 관리 시스템

[0069] 보안 관리 시스템의 주된 역할은 상위 수준의 정책을 하위 수준의 정책 집합으로 변환하는 것이다. 예를 들어, 보안 관리 시스템은 각 국가의 IP 주소를 제공하는 위치 정보 데이터베이스를 사용하여 국가 이름을 일련의 IP 주소들의 세트로 매핑할 수 있다. 상위 수준의 보안 정책을 변환한 후, 보안 관리 시스템은 네트워크 트래픽을 해당 IP 주소 및/또는 해당 IP 주소로 지정하기 위해 하위 수준 보안 정책들을 생성할 수 있다. 데이터 모델 파서는 하위 수준 보안 정책을 위한 XML 파일을 생성하여, 이를 적절한 NSF 인스턴스에 전달할 수 있다. 또한, 보안 관리 시스템은 NSF에 의해 생성된 보안 이벤트를 YANG 데이터 모델의 상위 수준 로그 메시지로 해석하여, 이를 NSF 클라이언트에게 반대 방향으로 전달할 수 있다.

[0070] 4.4 NSF Facing Interface

[0071] Client Facing Interface와 마찬가지로 NSF Facing Interface 역시, 구현 시 RESTCONF 프로토콜과 YANG 데이터 모델을 사용할 수 있다. I2NSF는 최근 NSF Facing Interface에 대한 표준 데이터 모델과 프로토콜을 정의하기 위한 작업을 진행 중에 있다.

[0072] 4.5 NSF 인스턴스들

[0073] 사용예에서는 발신자/착신자의 위치 및 전화 시간을 확인함으로써 VoIP-VoLTE 전화가 의심스러운지 여부를 결정하기 위해, NSF 인스턴스로서 방화벽 애플리케이션이 선택될 수 있다. 전화에 의심스러운 동작 패턴이 있는 경우, 해당 전화의 네트워크 트래픽은 하위 수준 보안 정책에 따라 방화벽 애플리케이션에 의해 효과적으로 차단될 수 있다. 방화벽 애플리케이션의 결과는 RESANGON 프로토콜을 통해 YANG 데이터 모델에서 보안 관리 시스템으로 전달될 수 있다.

[0074] 특정 상황에 따라 다수의 NSF 인스턴스들이 고려될 수 있다. 예를 들어, 의심스러운 발신자의 네트워크 트래픽을 분석하는 데 DPI가 추가로 사용될 수 있다.

[0075] 5. 주요 기술적 과제

[0076] 본 절에서는 본 발명을 구현하고 시스템 성능을 향상시키기 위해 추가적으로 고려해야 할 사항에 대해 살펴보며, 다음과 같다:

[0077] (1) 정책 업데이터가 보안 컨트롤러를 최근의 상위 수준 정책으로 업데이트함에 따라 업데이트 시간이 보안 컨트롤러와 달라질 수 있으며, 이 업데이트 프로세스 중에 상위 레벨 보안 정책의 불일치가 발생할 수 있다. 이러한 상위 수준 보안 정책의 불일치는 SDN 전환에서 공통적으로 볼 수 있는 업데이트 프로세스 중 구성 불일치와 유사하다.

[0078] (2) 보안 컨트롤러가 수신하는 정책 흐름으로 확장할 수 없기 때문에, 하나의 보안 컨트롤러가 증가하는 다수의 NSF 클라이언트들을 모두 처리 할 수 없게 되어 확장성 문제가 발생할 수 있다.

[0079] (3) 네트워크 엔티티들(예를 들어, NSF 클라이언트와 보안 관리 시스템) 사이에 안전하고 인증된 통신 채널이 설정되어야 한다. 이러한 통신 채널을 보장하지 않으면, 부적절한 보안 정책이 공격자에 의해 악의적으로 변경될 수 있다. 따라서, 네트워크 엔티티들에 키를 적절히 분배하기 위해서는 효율적인 키 관리가 필요하다.

[0080] (4) 보안 컨트롤러가 상위 수준 및 하위 수준 정책을 처리할 때, 처리 시퀀스들은 보안 컨트롤러와 NSF들 모두에서 동기화 문제를 일으킬 수 있다. 이 동기화 문제가 발생하지 않도록 보안 컨트롤러에 적절한 스케줄링 모델을 정의해야 한다.

[0081] (5) Client Facing Interface를 통해 전달될 높은 수준의 정책들을 생성하기 위해, 먼저 Client Facing Interface에서 일반적인 정책 데이터 모델이 정의되어야 한다. 이를 위해, 형태 및 내용과 무관하게, 정책을 쉽게 관리 할 수 있는 정책 추상화(Simplified Use of Policy Abstractions; SUPA)의 일반적인 데이터 모델이 사용될 수 있다.

[0082] 6. 관련 연구

[0083] 네트워크 서비스 가상화를 보안 서비스에 사용하는 것에 대한 관심은 네트워킹 커뮤니티에서 꾸준히 증가하고 있다. 그러나, 앞서 상술한 바와 같이, NSF에 대한 표준 인터페이스 및 스펙이 없다면, NSF를 매끄럽게 통합 및 관리하는 것이 불가능하다. 특히, 상위 수준의 보안 정책을 위한 표준 인터페이스가 없기 때문에 NSF 기반 애플리케이션을 실제 환경에 배포하기가 어렵다.

[0084] 이를 해결하기 위해, 본 명세서에서는 제1 실시예로서 클라이언트가 NSF와 관련된 세부 구현없이 NSF 인스턴스를 제어하기 위한 상위 수준의 보안 정책을 구성 및 관리 할 수 있는 아키텍처를 제시하였다.

[0085] 7. 결론

[0086] 이상으로, 제1 실시예로서 NFV를 이용한 NSF 기반의 보안 관리를 위한 일반적인 아키텍처를 제시하였다. 또한, 앞서 제1 실시예로 제안된 프레임 워크가 위험 도메인의 블랙리스트, 시간별 액세스 제어 정책 및 VoIP-VoLTE 서비스에 대한 의심스러운 전화 탐지와 같은 몇 가지 실제 공격 시나리오를 완화시킬 수 있는 방법에 대해 살펴보았다. 또한, 다양한 예제를 도입하여 구체적으로 제안된 아키텍처의 상세한 구현을 설명하였다.

[0088] **[2] 제2 실시예**

[0089] 제2 실시예는 I2NSF(Interface to Network Security Functions) 프레임 워크에서의 보안 관리 아키텍처를 제안한다. 이 보안 관리 아키텍처는 I2NSF 클라이언트, 보안 관리 시스템(즉, 보안 컨트롤러 및 개발자 관리 시스템) 및 I2NSF 프레임 워크의 NSF(Network Security Functions)를 포함할 수 있다. I2NSF 클라이언트는 애플리케이션 로직, 정책 업데이터 및 정책 콜렉터를 포함할 수 있다. 보안 컨트롤러는 보안 정책 관리자와 NSF

능력 관리자를 포함할 수 있다. 각 구성에 관한 설명은 앞서 도 1과 관련하여 상술한 설명이 동일하게 적용될 수 있으며, 중복되는 설명은 생략한다.

[0090] 또한, 제2 실시예는 상술한 구성들의 기능과 상위 수준에서의 보안 관리 처리에 대해 제안한다. 또한, 제2 실시예는 malware 도메인 리스트 보안 관리 및 VoIP-VoLTE 보안 관리와 같은 대표적인 사용 사례에 대해서도 설명한다.

[0091] 이외에, 제2 실시예에는 앞서 상술한 제1 실시예의 설명이 동일/유사하게 적용될 수 있으며, 중복되는 설명은 생략한다. 또한, 주제별로 절을 나누어 설명한다.

[0092] 1. 도입

[0093] I2NSF 프레임 워크[i2nsf-framework]에 사용자의 상위 수준 보안 정책을 적용하기 위해, I2NSF 클라이언트는 Client Facing Interface를 통해 보안 컨트롤러에 이러한 정책을 제공할 수 있다. 제2 실시예에서는 보안 관리를 위한 아키텍처가 I2NSF 프레임 워크의 주어진 상위 수준 정책에 대해 제안될 수 있다. 이 아키텍처는 I2NSF 클라이언트, 보안 관리 시스템(즉, 보안 컨트롤러 및 개발자 관리 시스템) 및 I2NSF 프레임 워크의 NSF를 포함할 수 있다. I2NSF 클라이언트에는 애플리케이션 로직, 정책 업데이터 및 정책 콜렉터가 포함될 수 있다. 보안 컨트롤러는 보안 정책 관리자 및 NSF 능력 관리자를 포함할 수 있다.

[0094] 보안 컨트롤러의 보안 정책 관리자 및 NSF 능력 관리자는 Client Facing Interface를 통해 I2NSF 클라이언트의 정책 업데이터에서 제공하는 업데이트된 보안 정책을 제어할 수 있다. 정책 업데이터는 보안 컨트롤러에 새롭거나 업데이트된 정책을 제공할 수 있다. 반면, NSF가 하위 수준 정책을 변경하는 이벤트가 발생하면, 정책 콜렉터는 이에 상응하여 보안 컨트롤러를 통해 상위 수준 정책을 수신할 수 있다. 그 후, 정책 콜렉터는 애플리케이션 로직의 현재 정책도 이에 따라 업데이트할 수 있다.

[0095] 제2 실시예에서는 보안 관리를 위한 추가 구성 요소를 I2NSF 프레임 워크에 통합하는 보안 관리 아키텍처를 제안한다. 이러한 아키텍처는 유연하고 효과적인 보안 정책을 지원하도록 설계되었다. Application Logic은 상위 수준의 정책을 생성하고, 정책 업데이터는 이를 Client Facing Interface를 통해 보안 정책 관리자로 전송할 수 있다. 보안 정책 관리자는 상위 수준 정책을 보안 컨트롤러의 여러 하위 수준 정책들에 매핑할 수 있다. 하위 정책들에 매핑한 후, 보안 정책 관리자는 이러한 정책들이 NSF에 적용될 수 있도록 NSF로 전송하게 된다.

[0096] 2. 목적

[0097] 제2 실시예는 다음과 같이 보안 관리 아키텍처에 대한 두 가지 주요 목표를 갖는다.

[0098] (1) 높은 수준의 보안 관리: NSF에서의 유연하고 효과적인 보안 정책의 시행을 지원하기 위해 일반적인 보안 관리 아키텍처의 설계를 제안한다.

[0099] (2) 보안 정책들의 자동 업데이트: 새로운 보안 공격에 대한 업데이트된 하위 수준의 보안 정책을 대응하는 상위 수준 보안 정책에 반영한다.

[0100] 3. 보안 관리를 위한 아키텍처

[0101] 본 절에서는 I2NSF의 보안 관리 아키텍처에 대해 설명하고 보안 컨트롤러와 개발자 관리 시스템을 갖춘 보안 관리 시스템에 중점을 두고 설명한다. 또한, 보안 컨트롤러의 기본 동작 및 아키텍처의 각 구성 요소에 대한 세부 정보를 설명한다.

[0102] 도 4는 I2NSF의 보안 관리 아키텍처를 예시한 도면이다.

[0103] 도 4의 보안 관리 아키텍처는 유연하고 효과적인 보안 정책의 시행을 지원하도록 설계되었다. I2NSF 클라이언트의 애플리케이션 로직은 새로운 보안 공격에 따라 상위 수준의 정책을 생성하면, I2NSF 클라이언트의 정책 업데이터가 이러한 정책을 보안 컨트롤러의 보안 정책 관리자에게 전송한다. 보안 정책 관리자는 상위 수준 정책을 NSF 능력 관리자에 등록된 NSF 능력과 관련된 몇 가지 하위 수준의 정책들에 매핑할 수 있다. 이와 같은 낮은 수준의 정책으로의 매핑이 완료된 후, 보안 정책 관리자는 이러한 정책들을 NSF Facing Interface를 통해 NSF에 전달할 수 있다. 이하에서는 각 구성에 대해 후술한다.

[0104] 2.1. 보안 정책 관리자

[0105] 보안 정책 관리자는 Client Facing Interface를 통해 정책 업데이터로부터 상위 수준의 정책을 수신하고, 상위 수준의 정책을 NSF 능력 관리자에 등록된 특정 NSF 능력과 관련된 여러 하위 수준의 정책들과 매핑하거나 또는

하위 수준의 정책들을 상위 수준의 정책으로 매핑하는 구성 요소이다. 또한, 보안 정책 관리자는 이러한 정책들을 NSF Facing Interface를 통해 NSF(들)에게 전달할 수 있다.

[0106] 하위 수준 정책 변경이 필요한 이벤트가 NSF에서 발생하면, NSF는 NSF Facing Interface를 통해 보안 정책 관리자에게 변경된 하위 수준 정책을 전송할 수 있다. 이후, 보안 정책 관리자는 Client Facing Interface를 통해 상기 변경된 하위 수준의 정책을 상위 수준의 정책에 매핑하고, 상기 변경된 하위 수준의 정책 또는 상위 수준의 정책을 정책 콜렉터로 전송할 수 있다.

[0107] 2.2 NSF 능력 관리자

[0108] NSF 능력 관리자는 보안 컨트롤러에 통합된 구성일 수 있다. NSF 능력 관리자는 등록 인터페이스를 통해 개발자 관리 시스템에 등록된 NSF의 능력을 저장하고 이를 보안 정책 관리자와 공유하여 보안 정책 관리자가 특정 NSF 능력과 관련된 하위 수준 정책을 생성할 수 있도록 할 수 있다. 또한, NSF 능력 관리자는 새로운 NSF가 등록될 때마다 등록 인터페이스를 통해 NSF 능력 관리자의 관리 테이블에 NSF의 능력을 등록하도록 개발자의 관리 시스템에 요청할 수 있다. 기존의 NSF가 삭제되면 NSF 능력 관리자는 관리 테이블에서 NSF의 능력을 제거할 수 있다.

[0109] 2.3 개발자 관리 시스템

[0110] 개발자 관리 시스템은 등록 인터페이스를 통해 NSF 능력 관리자에 새로운 NSF 능력을 등록하는 구성 요소일 수 있다. 등록된 NSF에 업데이트가 있으면, 업데이트된 내용/정보는 개발자 관리 시스템에서 NSF 능력 관리자에게 전달될 수 있다.

[0111] 2.4 애플리케이션 로직

[0112] 애플리케이션 로직은 (보안 관리 아키텍처에서) 보안 공격을 차단 또는 완화하기 위해 상위 수준의 보안 정책을 생성하는 구성일 수 있다. 애플리케이션 로직은 생성된 정책들을 정책 업데이터로 전송할 수 있다. 애플리케이션 로직의 보다 상세한 동작에 관해서는 이하의 사용예와 함께 후술한다.

[0113] 2.5 정책 업데이터

[0114] 정책 업데이터는 애플리케이션 로직에 의해 생성된 상위 수준의 보안 정책을 수신하고, 이를 Client Facing Interface를 통해 보안 정책 관리자로 배포/전달하는 구성일 수 있다.

[0115] 2.6 정책 콜렉터

[0116] 정책 콜렉터는 업데이트된 상위 수준의 보안 정책을 Client Facing Interface를 통해 보안 컨트롤러로부터 수신하고, 이를 애플리케이션 로직으로 전달할 수 있다. NSF에서 발생하는 이벤트에 따라 하위 수준의 보안 정책이 업데이트될 수 있으므로, 상기와 같은 업데이트가 필요하다. 이벤트를 수신한 후 정책 콜렉터는, 이를 애플리케이션 로직으로 전달하여 애플리케이션 로직이 보안 컨트롤러로부터 수신한 해당 상위 수준의 보안 정책을 업데이트(또는 생성)하도록 할 수 있다.

[0117] 3. 사용예

[0118] 본 아키텍처는 가능한 보안 공격에 대응하도록 설계되었다. 본 절에서는 malware 도메인 및 VoIP/VoLTE 보안 공격에서 주어진 보안 공격 리스트에 대해 I2NSF 프레임 워크[i2nsf-framework]의 보안 공격 방어를 위한 절차를 예시한다.

[0119] 3.1. Malware 도메인 리스트에 대한 보안 관리

[0120] 도 5는 Malware 도메인 블랙리스트 작성의 보안 관리 아키텍처를 예시한 도면이다.

[0121] Malware 도메인 블랙리스트 작성은 악의적인 활동이 의심되는 가능한 공격 호스트, 서버 및 네트워크들의 IP 주소들을 유지 및 게시하는 것을 말한다.

[0122] Malware 도메인 블랙리스트 작성에 기반하여, Malware 도메인 리스트는 I2NSF 클라이언트의 Malware 도메인 관리자에 의해 수동 또는 자동으로 업데이트될 수 있다. 또한, Malware 도메인 관리자는 새롭게 추가된 Malware 도메인과의 패킷 전달을 방지하고 NSF의 하위 수준 보안 정책을 시행하기 위해, 주기적으로 새로운 상위 수준의 보안 정책을 생성할 수 있다. 또한, Malware 도메인 관리자는 새로운 상위 수준 보안 정책을 Policy Updater로 전송할 수 있으며, Policy Updater는 이를 보안 컨트롤러로 전달할 수 있다.

[0123] 업데이트된 하위 수준 정책은 NSF Facing Interface를 통해 NSF에 의해 보안 컨트롤러로 전송되어, 보안 컨트롤러가 하위 수준 정책과 대응하는 상위 수준 보안 정책을 생성하도록 할 수 있다. 보안 컨트롤러는 정책 콜렉터에 상위 수준 보안 정책을 제공할 수 있다. 정책 콜렉터는 애플리케이션 로직으로서 정책을 Malware 도메인 관리자에 전달할 수 있다.

[0124] 3.2 VoIP-VoLTE를 위한 보안 관리

[0125] VoIP-VoLTE 보안 관리는 불법적인 전화 및 인증이 의심되는 SIP 장치의 IP 주소, 소스 포트, 만료 시간, 사용자 에이전트 및 SIP(Session Initiation Protocol) URI의 블랙리스트를 유지 및 게시할 수 있다. 일반적인 보안 관리 아키텍처에서 VoIP-VoLTE 보안 관리자는 도 4의 VoIP-VoLTE 보안 서비스를 위한 애플리케이션 로직에 해당할 수 있다.

[0126] VoIP-VoLTE 보안 관리를 기반으로, 애플리케이션 로직 기능을 수행하는 VoIP-VoLTE 보안 관리자는 불법 장치 정보 리스트를 수동 또는 자동으로 업데이트할 수 있다. 또한, VoIP-VoLTE 보안 관리자는 새롭게 추가된 VoIP-VoLTE 공격자와의 패킷 전달을 방지하고 NSF의 하위 수준 보안 정책을 시행하기 위해 주기적으로 새로운 상위 수준 보안 정책을 생성할 수 있다. VoIP-VoLTE 보안 관리자는 새로운 상위 수준 보안 정책을 정책 업데이터로 전송할 수 있으며, 정책 업데이터는 이를 보안 컨트롤러로 전달할 수 있다.

[0127] NSF는 VoIP-VoLTE 공격에 대해 업데이트된 하위 수준 정책을 NSF Facing Interface를 통해 보안 컨트롤러로 전송되므로, 보안 컨트롤러가 IP 주소, 사용자 에이전트 및 해당 에이전트와 같은 상기 하위 수준 정책과 대응되는 상위 수준 보안 정책을 생성하고, 보안 컨트롤러에 의해 추가될 필요가 있는 시간 값을 만료시킬 수 있다. 보안 컨트롤러는 정책 수집기에 상위 수준 보안 정책을 제공할 수 있다. 정책 콜렉터는 애플리케이션 로직으로서 VoIP-VoLTE 보안 관리자에 정책을 전달할 수 있다.

[0128] 7. 보안 고려 사항

[0129] 보안 관리 아키텍처는 I2NSF 프레임 워크[i2nsf-framework]로부터 파생되므로, I2NSF 프레임 워크의 보안 고려사항이 존재할 수 있다. 특히, 제안된 아키텍처의 구성 요소들간에 제어 메시지 또는 관리 메시지를 전달하는데 적절한 보안 통신 채널이 사용되어야 한다.

[0131] **[3] 제3 실시예**

[0132] 본 실시예에서는 I2NSF(Interface to Network Security Functions) 프레임 워크의 보안 관리 아키텍처에 대해 설명한다. 이 보안 관리 아키텍처는 I2NSF 사용자, 보안 관리 시스템(즉, 보안 컨트롤러 및 개발자 관리 시스템) 및 I2NSF 프레임 워크의 NSF(Network Security Functions)를 포함할 수 있다. I2NSF 사용자는 애플리케이션 로직, 정책 업데이터 및 이벤트 콜렉터를 포함할 수 있다. 보안 컨트롤러는 보안 정책 관리자와 NSF 능력 관리자를 포함할 수 있다. 이하에서는 앞서 상술한 구성들의 기능과 보안 관리 처리에 대해 설명한다. 또한, 이하에서는 Malware 도메인 리스트 보안 관리, VoIP-VoLTE 보안 관리 및 시간별 액세스 제어와 같은 대표적인 사용 사례에 대해 설명한다. 각 구성에 관한 설명은 앞서 제1 및 제2 실시예와 관련하여 상술한 설명이 동일하게 적용될 수 있으며, 중복되는 설명은 생략한다.

[0133] 1. 도입

[0134] I2NSF 프레임 워크 [i2nsf-framework]에 사용자의 상위 수준 보안 정책을 적용하기 위해, I2NSF 사용자는 소비자 지향 인터페이스(Consumer Facing Interface)를 통해 보안 컨트롤러에 이러한 상위 수준 보안 정책을 제공할 수 있다. 이하에서는 I2NSF 프레임 워크의 주어진 상위 수준 정책을 위한 보안 관리 아키텍처를 제안한다. 이 아키텍처는 I2NSF 사용자, 보안 관리 시스템(즉, 보안 컨트롤러 및 개발자 관리 시스템) 및 I2NSF 프레임 워크의 NSF를 포함할 수 있다. I2NSF 사용자는 애플리케이션 로직, 정책 업데이터 및 이벤트 콜렉터를 포함할 수 있다. 보안 컨트롤러는 보안 정책 관리자 및 NSF 능력 관리자를 포함한다.

[0135] 보안 컨트롤러의 보안 정책 관리자와 NSF 능력 관리자는 I2NSF 사용자의 정책 업데이터가 Consumer Facing Interface를 통해 제공하는 업데이트된 보안 정책을 제어할 수 있다. 새 정책이 생성되었거나 기존 정책이 업데이트되어야 할 필요가 있는 경우, 정책 업데이터가 새 정책 및/또는 기존 정책의 업데이트 내용을 보안 컨트롤러에 제공할 수 있다. 반면, NSF가 하위 수준 정책을 변경해야 하는 이벤트가 발생하면, NSF는 해당 이벤트를 보안 컨트롤러로 전송할 수 있다. 보안 컨트롤러는 해당 이벤트를 이벤트 콜렉터로 전달하면, 이벤트 콜렉터가 이를 애플리케이션 로직으로 전달할 수 있다. 그 후, 애플리케이션 로직은 수신한 이벤트에 따라 현재 정책을 업데이트할 수 있다.

[0136] 제3 실시예에서는 보안 관리를 위한 추가 구성 요소를 I2NSF 프레임 워크에 통합하는 보안 관리 아키텍처를 제안한다. 이러한 아키텍처는 유연하고 효과적인 보안 정책을 지원하도록 설계되었다. 애플리케이션 로직은 상위 수준 정책을 생성하고 정책 업데이터는 이를 Consumer Facing Interface를 통해 보안 정책 관리자로 전송할 수 있다. 보안 정책 관리자는 상위 수준 정책을 보안 컨트롤러의 여러 하위 수준 정책들에 매핑할 수 있다. 매핑 후, 하위 수준의 정책들은 NSF에 배포되어 NSF에 적용될 수 있다.

[0137] 2. 목표

[0138] 제3 실시예에 따른 보안 관리 아키텍처의 두 가지 주 목적은 다음과 같다.

[0139] (1) 높은 수준의 보안 관리: NSF들에서의 유연하고 효과적인 보안 정책의 시행을 지원하기 위한 보안 관리 아키텍처의 설계를 제안한다.

[0140] (2) 보안 정책의 자동 업데이트: NSF들이 새로운 보안 공격에 대해 하위 수준 정책을 변경해야 하는 이벤트가 발생한 경우, 해당 이벤트를 대응하는 상위 수준의 보안 정책들에 반영하기 위함이다.

[0141] 3. 보안 관리 아키텍처

[0142] 본 절에서는 I2NSF의 보안 관리 아키텍처에 대해 설명하고 보안 컨트롤러 및 개발자 관리 시스템이 포함된 보안 관리 시스템에 중점을 두고 설명한다. 또한, 본 절에서는 보안 컨트롤러의 기본 동작에 대해 설명하고 아키텍처에 포함되는 각 구성 요소의 세부 사항을 설명한다.

[0143] 도 6은 I2NSF 프레임 워크 내의 보안 관리 아키텍처를 예시한 도면이다.

[0144] 도 6의 아키텍처는 유연하고 효과적인 보안 정책의 시행을 지원하도록 설계되었다. I2NSF 사용자의 애플리케이션 로직은 새로운 보안 공격에 따라 상위 수준의 정책을 생성하고, I2NSF 사용자의 정책 업데이터는 상기 상위 수준의 정책을 보안 컨트롤러의 보안 정책 관리자에게 보낸다. 보안 정책 관리자는 상위 수준 정책을 NSF 능력 관리자에 등록된 NSF 능력과 관련된 몇 개의 하위 수준 정책들에 매핑할 수 있다. 매핑 후, 보안 정책 관리자는 NSF Facing Interface를 통해 하위 수준 정책들을 NSF(들)로 배포할 수 있다. 다음 절에서는 각 구성 요소의 세부 사항에 대해 설명한다.

[0145] 4.1 보안 정책 관리자

[0146] 보안 정책 관리자는 Consumer Facing Interface를 통해 정책 업데이터로부터 상위 수준 정책을 수신하고, 상위 수준 정책을 NSF 능력 관리자의 특정 NSF 능력과 관련된 몇 개의 하위 수준 정책들로 매핑하는 구성이다. 또한, 보안 정책 관리자는 이러한 하위 수준 정책들을 NSF Facing Interface를 통해 NSF(들)로 전달할 수 있다.

[0147] 한편, 하위 레벨 정책을 변경해야 하는 이벤트가 NSF에서 발생하면, NSF는 NSF Facing Interface를 통해 보안 정책 관리자에게 해당 이벤트를 전송할 수 있다. 이후, 보안 정책 관리자는 Consumer Facing Interface를 통해 해당 이벤트를 이벤트 콜렉터로 전송한다.

[0148] 4.2 NSF 능력 관리자

[0149] NSF 능력 관리자는 보안 컨트롤러에 통합된 구성이다. NSF 능력 관리자는 등록 인터페이스를 통해 개발자 관리 시스템에 등록된 NSF 능력을 저장하고, 이를 보안 정책 관리자와 공유하여 보안 정책 관리자가 NSF 능력과 관련된 하위 수준 정책을 생성하도록 할 수 있다. 또한, 새로운 NSF가 등록될 때마다, NSF 능력 관리자는 등록 인터페이스를 통해 NSF 능력 관리자의 관리 테이블에 NSF 능력을 등록하도록 개발자 관리 시스템에 요청할 수 있다. 한편, 기존의 NSF가 삭제되면, NSF 능력 관리자는 관리 테이블에서 NSF 능력을 제거한다.

[0150] 4.3 개발자 관리 시스템

[0151] 개발자 관리 시스템은 등록 인터페이스를 통해 NSF 능력 관리자에 새로운 NSF 능력을 등록하는 구성이다. 또한, 등록된 NSF에 업데이트가 있는 경우, 해당 업데이트는 개발자 관리 시스템에서 NSF 능력 관리자로 전달된다.

[0152] 4.4. 애플리케이션 로직

[0153] 애플리케이션 로직은 보안 공격을 차단 또는 완화하기 위한 상위 수준 보안 정책을 생성하고, 생성된 정책을 정책 업데이터로 전송하는 구성이다. 이러한 애플리케이션 로직에 대해서는 이하의 사용예에서 자세한 동작을 설명한다.

[0154] 4.5. 정책 업데이터

[0155] 정책 업데이터는 애플리케이션 로직에서 생성된 상위 수준 보안 정책을 수신하고, 이를 Consumer Facing Interface를 통해 보안 정책 관리자에게 전달하는 구성이다.

[0156] 4.6 이벤트 콜렉터

[0157] 이벤트 콜렉터는 애플리케이션 로직의 상위 수준 정책을 업데이트(또는 생성)할 때 반영되어야 하는 이벤트를 보안 컨트롤러로부터 수신한다. NSF에서 발생하는 특정 이벤트에 따라 하위 수준의 보안 정책이 업데이트되므로, NSF에서 이벤트를 수신하는 절차가 필요하다. 이벤트를 수신한 후, 이벤트 콜렉터는 이를 애플리케이션 로직으로 전달하여, 애플리케이션 로직이 보안 컨트롤러로부터 수신한 이벤트를 기반으로 상위 수준의 보안 정책을 업데이트(또는 생성)할 수 있도록 한다.

[0158] 5. 사용예

[0159] 본 아키텍처는 실제 환경에서 발생할 수 있는 보안 공격에 대응하도록 설계된다. 본 절에서는 Malware 도메인에서 주어진 보안 공격 리스트, VoIP/VoLTE 보안 공격 및 시간별 액세스 제어에 대한 I2NSF 프레임 워크[i2nsf-framework]의 보안 공격에 대한 방어 절차를 설명한다.

[0160] 5.1. Malware 도메인 리스트 보안 관리

[0161] Malware 도메인 차단 리스트 작성은 악의적인 활동이 의심되는 가능한 공격 호스트, 서버 및 네트워크의 IP 주소들을 유지 및 게시한다.

[0162] 도 7은 Malware 도메인 블랙리스트 작성의 보안 관리 아키텍처를 예시한 도면이다.

[0163] Malware 도메인 블랙리스트 작성에 기초하여, Malware 도메인들의 리스트는 I2NSF 사용자의 Malware 도메인 관리자에 의해 수동 또는 자동으로 업데이트될 수 있다. 또한, Malware 도메인 관리자는 새로 추가된 Malware 도메인과의 패킷 전달을 방지하고 NSF의 하위 수준 보안 정책들을 시행하기 위해 주기적으로 새로운 상위 수준 보안 정책을 생성할 수 있다. 또한, Malware 도메인 관리자는 새로운 상위 수준 보안 정책을 정책 업데이터로 전송할 수 있으며, 정책 업데이터는 보안 컨트롤러로 이를 전달할 수 있다.

[0164] NSF가 새로운 위험 도메인을 탐지하면, 해당 IP 주소를 NSF Facing Interface를 통해 보안 컨트롤러로 전송할 수 있다. 보안 컨트롤러는 이벤트 콜렉터에 IP 주소를 전달하며, 이벤트 콜렉터는 해당 IP 주소를 위험 도메인 관리자에게 전달할 수 있다. 이에 기초하여, 위험 도메인 관리자는 위험 도메인 데이터 베이스를 업데이트할 수 있다.

[0165] 5.2 VoIP-VoLTE에 대한 보안 관리

[0166] VoIP-VoLTE 보안 관리는 불법적인 전화 및 인증이 의심되는 SIP 장치의 IP 주소, 소스 포트, 만료 시간, 사용자 에이전트 및 SIP(Session Initiation Protocol) URI의 블랙리스트를 유지 관리하고 게시한다. 보안 관리 아키텍처에서 VoIP-VoLTE 보안 관리자는 도 6에서의 VoIP-VoLTE 보안 서비스를 위한 애플리케이션 로직의 역할을 수행한다.

[0167] VoIP-VoLTE 보안 관리에 기초하여, 애플리케이션 로직 기능을 수행하는 VoIP-VoLTE 보안 관리자는 불법 장치 정보의 목록를 수동 또는 자동으로 업데이트할 수 있다. 또한, VoIP-VoLTE 보안 관리자는 새롭게 추가된 VoIP-VoLTE 공격자와의 패킷 전달을 방지하고 NSF의 하위 수준 보안 정책을 시행하기 위해 주기적으로 새로운 상위 수준 보안 정책을 생성할 수 있다. 또한, VoIP-VoLTE 보안 관리자는 새로운 상위 수준 보안 정책을 정책 업데이터로 전송할 수 있으며, 정책 업데이터는 이를 보안 컨트롤러로 전달할 수 있다.

[0168] NSF가 도메인으로부터 전달된 비정상적인 메시지 또는 전화를 검출하는 경우, IP 주소, 사용자 에이전트 및 만료 시간 값과 같은 도메인 정보는 NSF acing 인터페이스를 통해 NSF에 의해 보안 컨트롤러로 전송된다. 보안 컨트롤러는 이벤트 콜렉터에 탐지된 도메인 정보를 전달하고, 이벤트 콜렉터는 탐지된 도메인 정보를 VoIP-VoLTE 보안 관리자로 전달하며, VoIP-VoLTE 보안 관리자는 탐지된 도메인 정보에 기초하여 VoIP-VoLTE 데이터 베이스를 업데이트한다.

[0169] 5.3 시간별 액세스 제어에 대한 보안 관리

[0170] 시간별 액세스 제어 정책은 특정 기간 동안 특정 웹 사이트에 대한 사용자의 액세스를 관리한다. 예를 들어, 회사에서 관리자는 직원이 근무 시간 동안 업무에 방해가 될 수 있는 Youtube에 액세스하는 것을 차단할 수 있다.

[0171] I2NSF 사용자는, 시간별 액세스 제어에 기초하여, 애플리케이션 로직에 차단된 웹 사이트 및 차단 시간의 리스

트를 등록한다. 애플리케이션 로직은 리스트를 데이터 베이스에 저장하고 상위 수준의 보안 정책(예를 들어, 리스트에서 차단된 웹 사이트 및 차단 시간을 확인하여 웹 사이트에 대한 액세스 차단)을 생성한다. 애플리케이션 로직은 이를 정책 업데이터로 전달하면, 정책 업데이터는 이를 보안 컨트롤러로 전달한다. 보안 컨트롤러에서 보안 정책 관리자는 상위 수준 정책을 하위 수준 정책들에 매핑한 다음, NSF가 하위 수준 정책들을 적용할 수 있도록 이들을 NSF로 전송한다.

[0172] 6. 보안 고려 사항

[0173] 보안 관리 아키텍처는 I2NSF 프레임 워크[i2nsf-framework]로부터 파생되므로, I2NSF 프레임 워크의 보안 고려사항이 존재할 수 있다. 특히, 제안된 아키텍처의 구성 요소들간에 제어 메시지 또는 관리 메시지를 전달하는데 적절한 보안 통신 채널이 사용되어야 한다.

[0174] 도 8은 본 발명의 일 실시예에 따른 보안 관리 시스템의 보안 관리 방법에 관한 순서도이다. 본 순서도와 관련하여 앞서 상술한 실시예들이 동일/유사하게 적용될 수 있으며, 중복되는 설명은 생략할 수 있다.

[0175] 우선, 보안 관리 시스템은 NSF 클라이언트로부터 보안 공격을 차단 또는 완화하기 위한 상위 수준 정책을 수신할 수 있다(S810).

[0176] 다음으로, 보안 관리 시스템은 상기 상위 수준 정책을 보안 관리 시스템에 등록된 NSF 능력과 관련된 하위 수준 보안 정책들에 매핑할 수 있다(S820).

[0177] 마지막으로, 보안 관리 시스템은 하위 수준 보안 정책들을 적어도 하나의 NSF에 전달할 수 있다(S830).

[0178] NSF 클라이언트는 애플리케이션 로직, 정책 업데이터 및/또는 이벤트 콜렉터를 포함할 수 있다. 여기서, 애플리케이션 로직은 상위 수준 정책을 생성 및 업데이트하여 정책 업데이터로 전송하며, 정책 업데이터는 상위 수준 정책을 클라이언트 지향 인터페이스를 통해 보안 관리 시스템으로 전달하며, 이벤트 콜렉터는 상위 수준 정책의 생성 또는 업데이트에 기초가 되는 이벤트를 수신하여 애플리케이션 로직으로 전송할 수 있다.

[0179] 상위 수준 정책은 일 실시예로서, 특정 공격 호스트, 서버 및 네트워크의 IP 주소가 포함된 블랙리스트를 기반으로 생성될 수 있다. 이 경우, 이벤트는 상기 블랙리스트로의 포함 기준을 만족하는 IP 주소에 해당할 수 있다.

[0180] 또는, 상위 수준 정책은 다른 실시예로서, 차단 웹 사이트 및 차단 시간이 포함된 블랙리스트를 기반으로 생성될 수 있다.

[0181] 또는, 상위 수준 정책은 다른 실시예로서, 특정 SIP 장치의 IP 주소, 소스 포트, 만료 시간, 사용자 에이전트 및/또는 SIP URI가 포함된 불법 장치 차단 목록을 기반으로 생성될 수 있다. 이 경우, 이벤트는 불법 장치 차단 목록으로의 포함 기준을 만족하는 도메인 정보에 해당할 수 있다.

[0182] 보안 관리 시스템은 보안 정책 관리자, NSF 능력 관리자 및/또는 개발자 관리 시스템을 포함할 수 있다. 개발자 관리 시스템은 등록 인터페이스를 통해 NSF 능력을 등록 및 업데이트하며, NSF 능력 관리자는 개발자 관리 시스템에 등록 및 업데이트된 NSF 능력을 저장할 수 있다. 보안 정책 관리자는 상위 수준 정책을 NSF 능력 관리자에 저장된 NSF 능력과 관련된 하위 수준 보안 정책들과 매핑하고, 하위 수준 보안 정책들을 NSF 지향 인터페이스(NSF Facing Interface)를 통해 적어도 하나의 NSF로 전달할 수 있다.

[0184] 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.

[0185] 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.

[0186] 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.

[0187] 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.

[0188] 설명의 편의를 위하여 각 도면을 나누어 설명하였으나, 각 도면에 서술되어 있는 실시예들을 병합하여 새로운 실시예를 구현하도록 설계하는 것도 가능하다. 또한, 본 발명은 상술한 바와 같이 설명된 실시예들의 구성과 방법이 한정되게 적용될 수 있는 것이 아니라, 상술한 실시예들은 다양한 변형이 이루어질 수 있도록 각 실시 예들의 전부 또는 일부가 선택적으로 조합되어 구성될 수도 있다.

[0189] 또한, 이상에서는 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 명세서는 상술한 특정의 실시예에 한정되지 아니하며, 청구 범위에서 청구하는 요지를 벗어남이 없이 당해 명세서가 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형 실시들은 본 명세서의 기술적 사상이나 전망으로부터 개별적으로 이해되어서는 안될 것이다.

부호의 설명

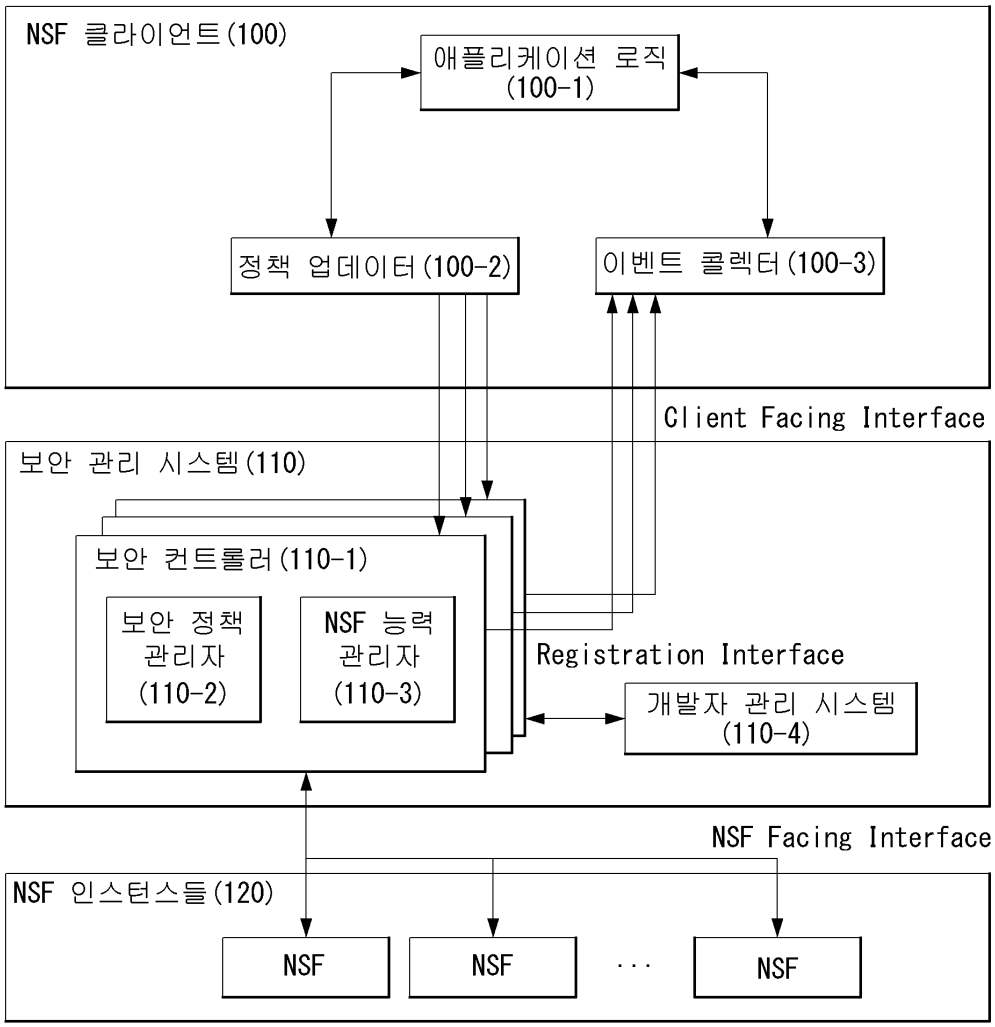
[0190] 100: NSF 클라이언트

110: 보안 관리 시스템

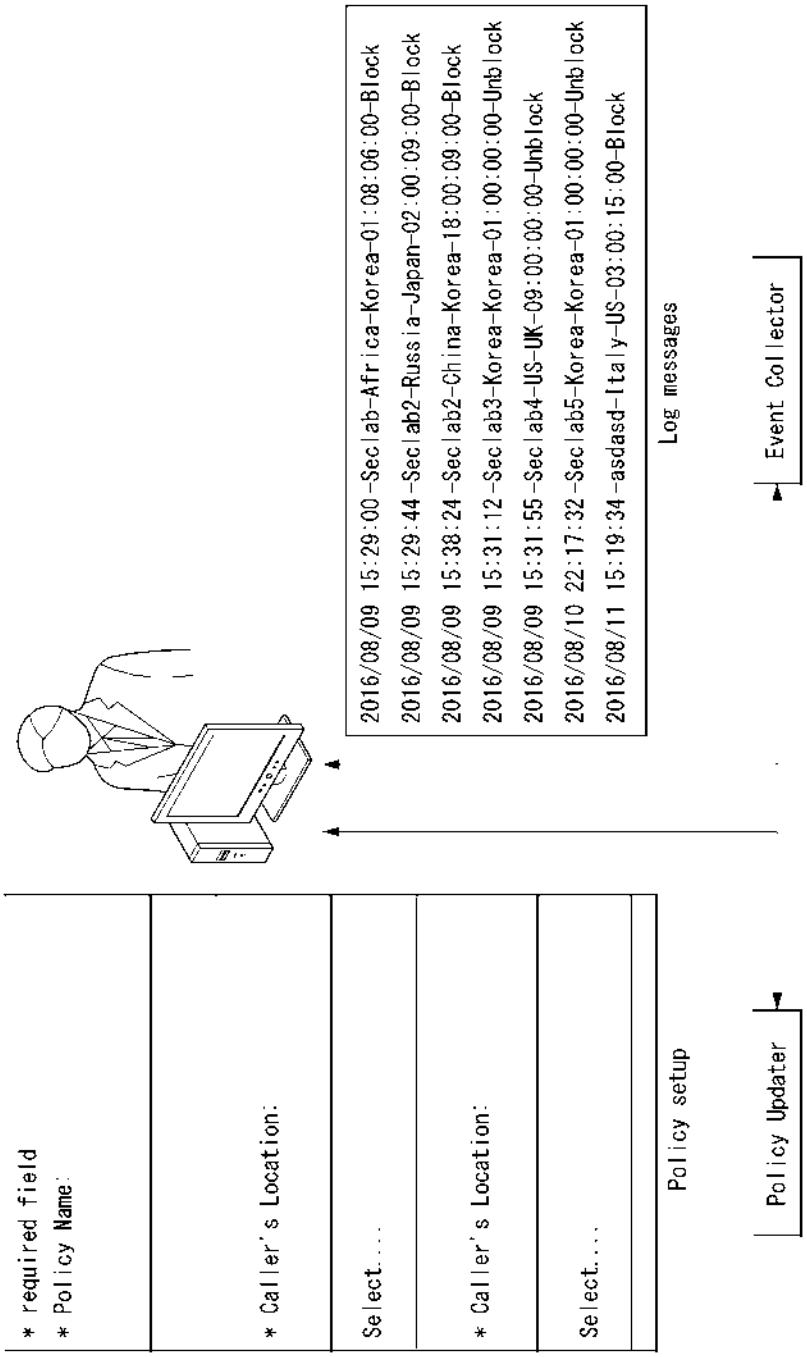
120: NSF 인스턴스들

도면

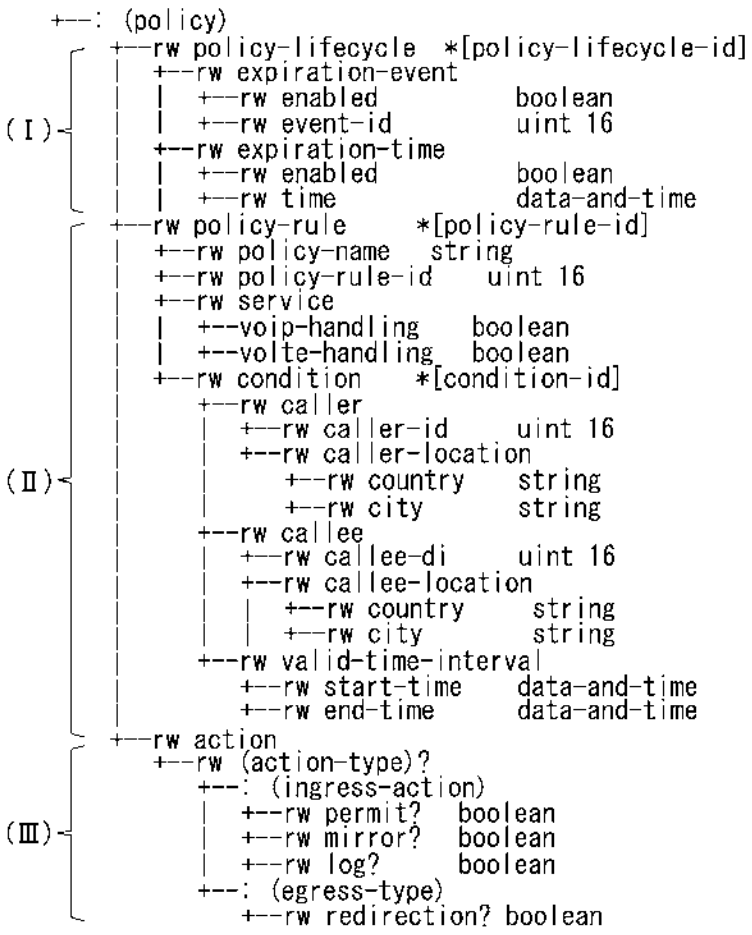
도면1


NSF 클라이언트(100)
애플리케이션 로직
(100-1)
정책 업데이터(100-2)
이벤트 콜렉터(100-3)
Client Facing Interface
보안 관리 시스템(110)
보안 컨트롤러(110-1)
보안 정책
관리자
(110-2)
NSF 능력
관리자
(110-3)
Registration Interface
개발자 관리 시스템
(110-4)
NSF Facing Interface
NSF 인스턴스들(120)
NSF
NSF
···
NSF

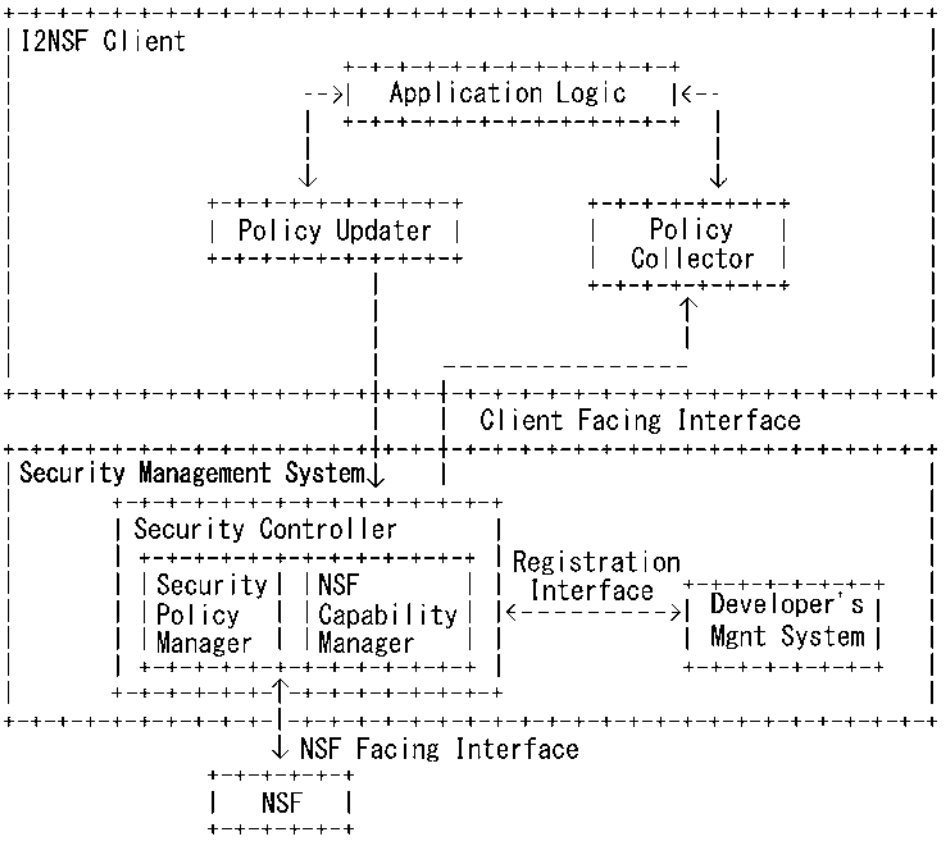
도면2


* required field
* Policy Name:
* Caller's Location:
Select....
* Caller's Location:
Select....
Policy setup
Policy Updater
2016/08/09 15:29:00-Seclab-Africa-Korea-01:08:06:00-Block
2016/08/09 15:29:44-Seclab2-Russia-Japan-02:00:09:00-Block
2016/08/09 15:38:24-Seclab2-China-Korea-18:00:09:00-Block
2016/08/09 15:31:12-Seclab3-Korea-Korea-01:00:00:00-Unblock
2016/08/09 15:31:55-Seclab4-US-UK-09:00:00:00-Unblock
2016/08/10 22:17:32-Seclab5-Korea-Korea-01:00:00:00-Unblock
2016/08/11 15:19:34-asdasd-Italy-US-03:00:15:00-Block
Log messages
Event Collector

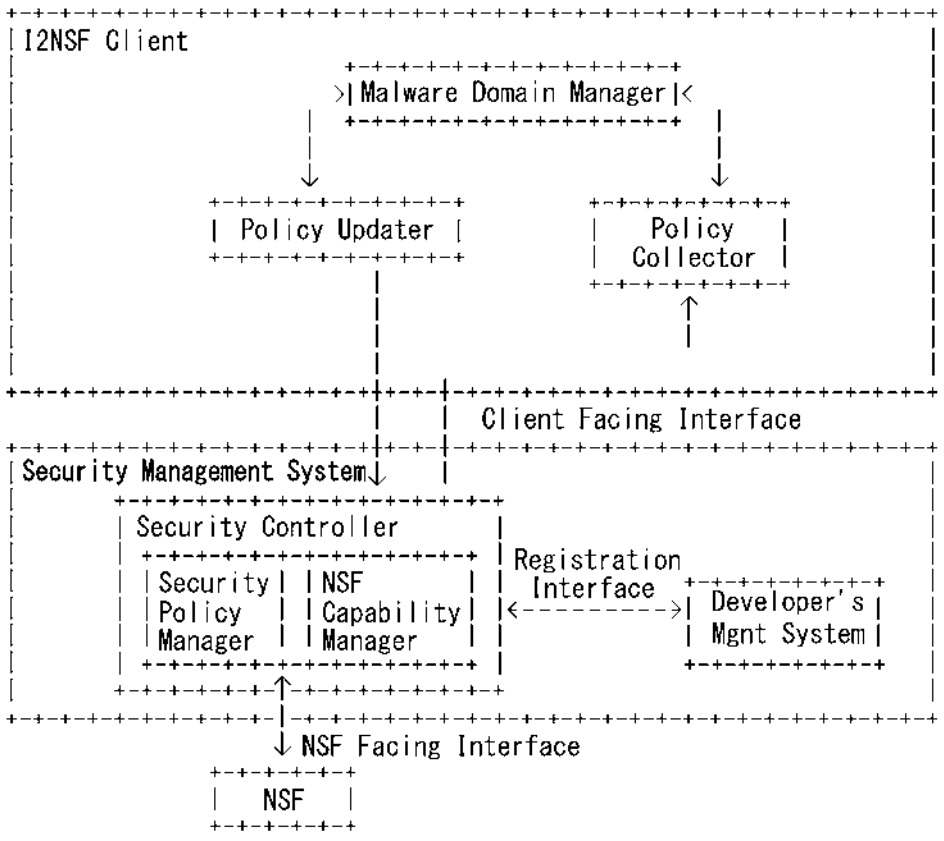
도면3


+--: (policy)
+--rw policy-lifecycle *[policy-lifecycle-id]
+--rw expiration-event
+--rw enabled boolean
+--rw event-id uint 16
+--rw expiration-time
+--rw enabled boolean
+--rw time data-and-time
(Ⅰ)
+--rw policy-rule *[policy-rule-id]
+--rw policy-name string
+--rw policy-rule-id uint 16
+--rw service
+--voip-handling boolean
+--volte-handling boolean
+--rw condition *[condition-id]
+--rw caller
+--rw caller-id uint 16
+--rw caller-location
+--rw country string
+--rw city string
+--rw callee
+--rw callee-di uint 16
+--rw callee-location
+--rw country string
+--rw city string
+--rw valid-time-interval
+--rw start-time data-and-time
+--rw end-time data-and-time
(Ⅱ)
+--rw action
+--rw (action-type)?
+--: (ingress-action)
+--rw permit? boolean
+--rw mirror? boolean
+--rw log? boolean
+--: (egress-type)
+--rw redirection? boolean
(Ⅲ)

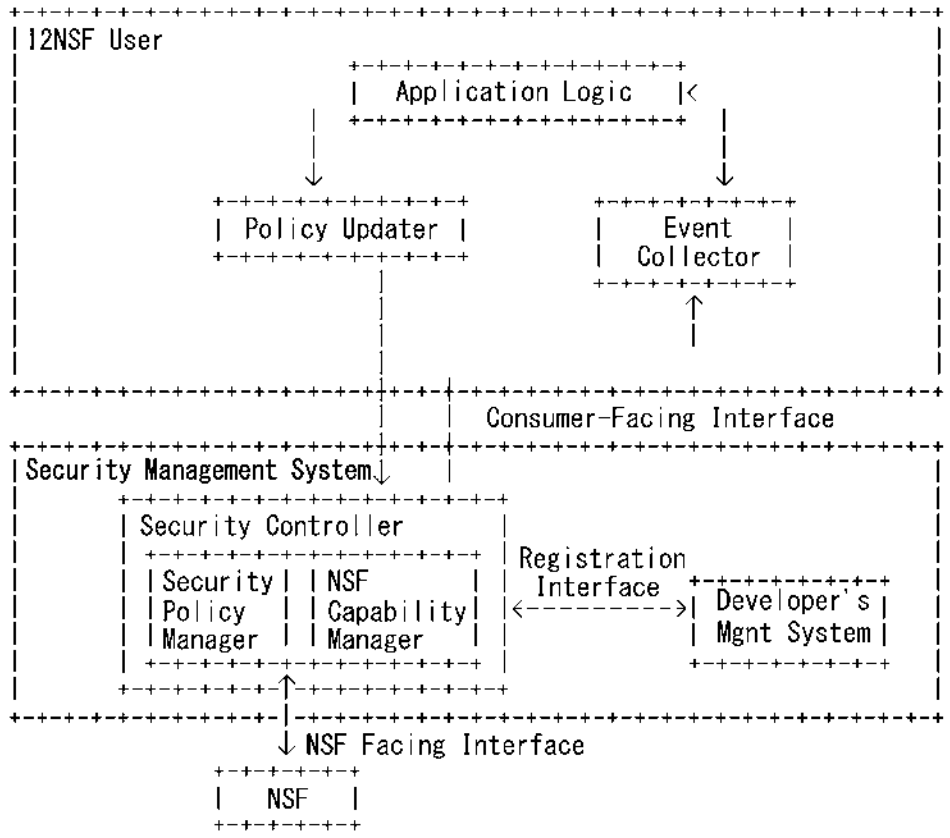
도면4


I2NSF Client
Application Logic
Policy Updater
Policy Collector
Client Facing Interface
Security Management System
Security Controller
Security Policy Manager
NSF Capability Manager
Registration Interface
Developer's Mgnt System
NSF Facing Interface
NSF

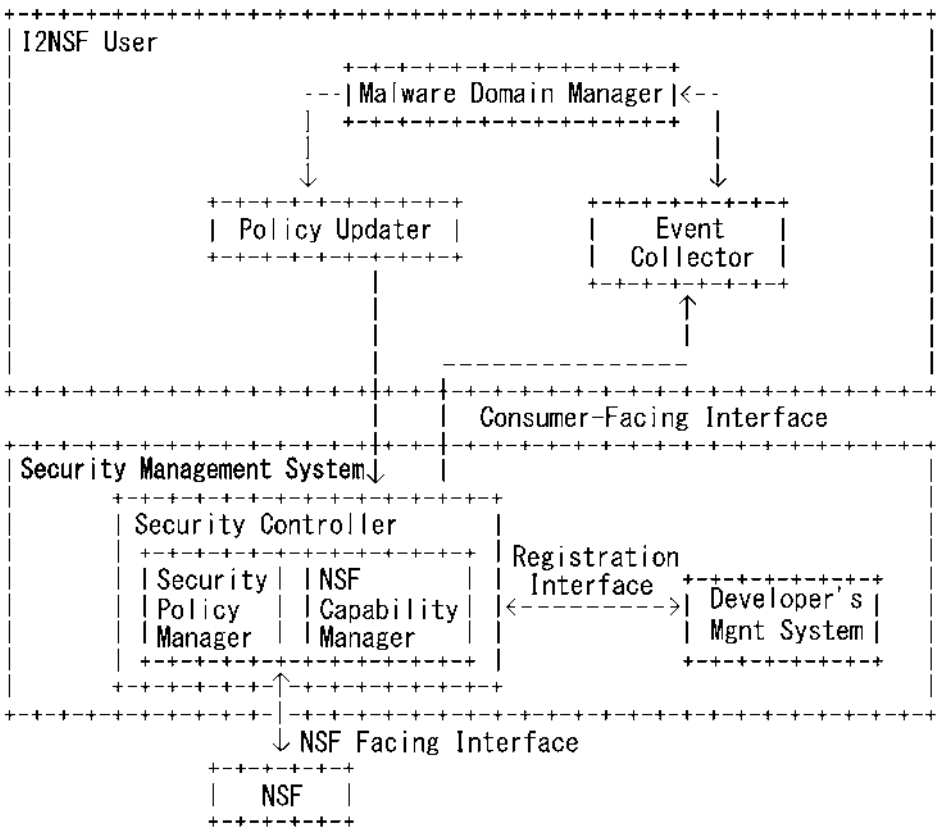
도면5


I2NSF Client
Malware Domain Manager
Policy Updater
Policy Collector
Client Facing Interface
Security Management System
Security Controller
Security Policy Manager
NSF Capability Manager
Registration Interface
Developer's Mgnt System
NSF Facing Interface
NSF

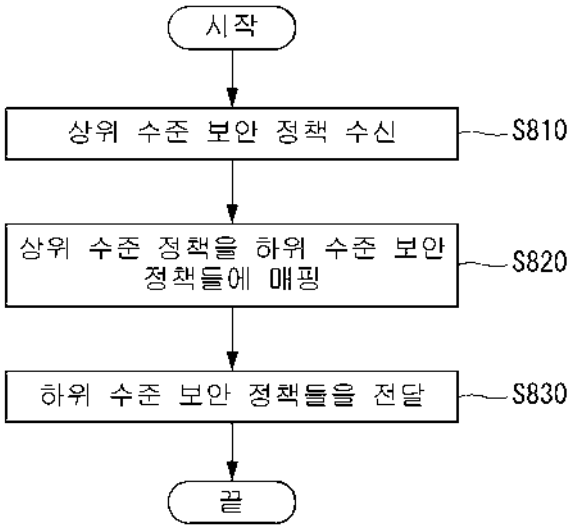
도면6


I2NSF User
Application Logic
Policy Updater
Event Collector
Consumer-Facing Interface
Security Management System
Security Controller
Security Policy Manager
NSF Capability Manager
Registration Interface
Developer's Mgnt System
NSF Facing Interface
NSF

도면7


I2NSF User
Malware Domain Manager
Policy Updater
Event Collector
Consumer-Facing Interface
Security Management System
Security Controller
Security Policy Manager
NSF Capability Manager
Registration Interface
Developer's Mgnt System
NSF Facing Interface
NSF

도면8


시작
상위 수준 보안 정책 수신
S810
상위 수준 정책을 하위 수준 보안 정책들에 매핑
S820
하위 수준 보안 정책들을 전달
S830
끝