정 보 보 호 학 회 지
제27권 제1호, 2017. 2

NFV 기반 네트워크 보안 서비스 시스템

현 상 원*

요 약

네트워크 기능 가상화(Network Function Virtualization, NFV) 기술은 기존에 물리적인 장비 형태로 제공되던 네트워크 기능들을 소프트웨어로 구현하여 가상의 인스턴스 형태로 제공하는 것을 말한다. 이런 NFV 기술을 통해 가용한 네트워크 자원들의 효율적인 활용과 가변적인 시스템 상황에 대한 유연한 대응이 가능하다. 이러한 NFV 기술이 점차 발전하면서 네트워크 보안 분야에서도 보안 서비스 벤더들이 자신들의 클라우드 시스템을 통해 소프트웨어 기반 다양한 네트워크 보안 기능들을 제공하는 시스템 형태가 점차 나타나고 있다. 본 논문에서는 NFV 기반 네트워크 보안 서비스 제공 시스템을 위한 참고 아키텍처로서 국제 인터넷 기술 표준화 단체인 IETF의 Interface to Network Security Functions (I2NSF) working group에서 제안한 I2NSF 시스템을 소개한다. 그리고 이러한 시스템 모델을 기반으로 NFV 기반 네트워크 보안 서비스 제공 시스템 설계 및 개발 시 고려해야 할 주요 연구이슈들에 관해 논의한다.

Ⅰ. 서 론

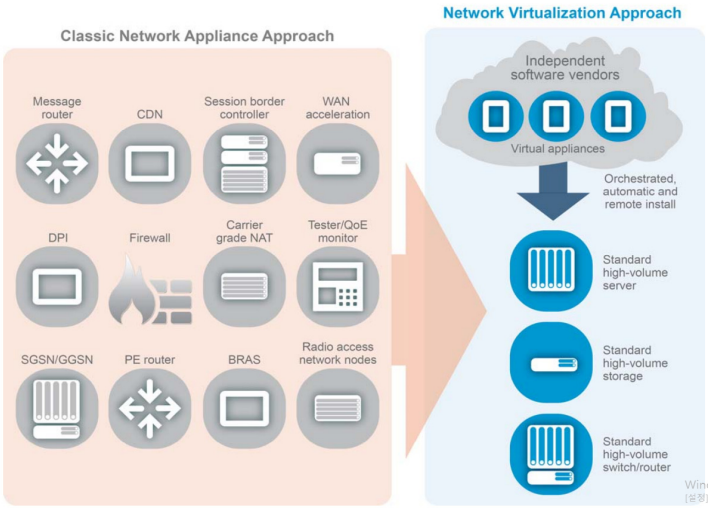
이동 통신 사업자나 엔터프라이즈 네트워크 시스템 등 다양한 네트워크 시스템에서 비용 절감과 네트워크 자원의 효율적이고 유연한 활용을 위해 네트워크 기능 가상화(Network Function Virtualization, NFV) 기술이 널리 적용되고 있는 추세이다 [3] (그림 1). 또한 이러한 소프트웨어 기반 가상화 기술과 함께 클라우드 시스템 기술의 발달로 외부 서비스 공급 업체의 클라우드 시스템을 통해 제공되는 기능 및 자원을 활용하는 것이 점차 보편화 되고 있다.

이는 네트워크 보안 서비스 영역에서도 마찬가지로서 기업체는 자신의 네트워크 시스템 및 정보 자산 보호를 위해 직접 네트워크 보안 장비를 구입해서 운영하는 대신 외부 보안 솔루션 벤더의 클라우드 시스템을 통해 제공되는 소프트웨어 기반 다양한 네트워크 보안 기능(Network Security Function, NSF)들을 이용료를 지불하고 사용하는 서비스 형태가 나타나고 있다 [1]. 이러한 NFV 기반 보안 서비스 시스템을 통해 보안 서비스를 필요로 하는 기업체는 고가의 네트워크 보안 장비 구매를 위한 비용을 지불하지 않아도 되기 때문에 비용을 줄일 수 있다. 뿐만 아니라 네트워크 보안 기능에서 핵심 요소인 다양한 공격들에 대한 데이터베이스를 직접 관리할 필요 없이 보안 서비스 업체의 전문가를 통해 관리되기 때문에 다양한 최신 공격들에 대해서도 신속한 대응이 가능하다.

NFV 기반 네트워크 보안 서비스 시스템의 주요 요구사항들로는 다음과 같은 것들이 있다. 첫 번째로는 일반적으로 여러 보안 벤더들로부터의 다양한 NSF들이 존재하게 된다. 일례로 보안 서비스를 필요로 하는 기업체의 요구에 따라서는 단일 보안 벤더가 아닌 각 NSF 별 서로 다른 벤더의 솔루션을 필요로 할 수 있다. 뿐만 아니라 특정 NSF에 대해서도 상호 보완적인 효과를 위해 여러 벤더들로부터의 NSF들을 동시에 필요로 할 수 있다. 그런데 서로 다른 벤더들에 의해 개발된 NSF들의 경우 그들을 제어 관리하기 위한 인터페이스 또한 각 벤더마다 상이하게 된다. 그리고 이러한 다양성은 필연적으로 제어 및 관리에 관한 비용과 복잡도의 증가로 이어지게 된다. 이러한 비효율성, 문제점을 해결하기 위해서는 다양한 NSF들에 대한 통일된 제어 및 관리를 가능하게 하기 위한 표준화된 인터페이스를 정의하는 것이 본질적으로 필요하다.

두 번째로는 NFV 기반 네트워크 보안 서비스 시스템의 사용자에게 간편한 보안 정책 설정을 지원하는 것이 필요하다. 여기서 사용자는 NFV 기반 네트워크 보안 서비스 시스템을 통해 보안 서비스를 제공 받고자

* 성균관대학교 소프트웨어대학 소프트웨어학과 (swhyun77@skku.edu)



〔그림 1〕 네트워크 기능 가상화 기본 컨셉 (〔8〕로부터 인용)

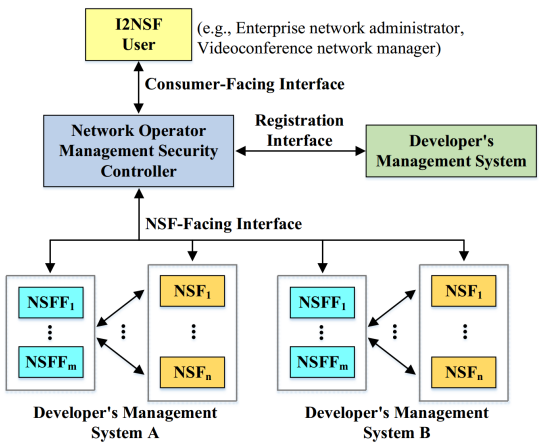
하는 네트워크 시스템의 관리자를 말한다. 사용자는 자신의 네트워크 시스템 보호를 위해 적용되어야 할 보안 정책을 명시해서 요청하게 되는데 이때 시스템에서 운영 중인 다양한 NSF들에 관한 세부사항들까지 고려해야 한다면 상당히 번거로운 작업이 될 것이다. 때문에 사용자 친화적인 고수준 보안 정책 설정에 대한 지원이 필요하다. 이를 위해서는 사용자와 NSF들 간을 매개할 수 있는 관리 모듈이 필요하며, 사용자는 이 관리 모듈에게 고수준을 보안 정책을 통해 요청하며, 이러한 사용자 요청을 받은 관리 모듈은 그러한 고수준의 보안 정책을 실현하기 위한 NSF들에 대한 저수준의 보안 정책을 생성 적용할 수 있어야 한다.

세 번째로 가변적인 네트워크 상황이나 보안 요구사항에 따라 유연한 대응이 가능한 시스템 설계가 필요하다. 주어진 네트워크 자원의 효율적인 활용을 위해서는 네트워크 트래픽 처리량에 맞게 NSF 인스턴스들이 동적으로 생성 및 폐기될 수 있어 한다. 뿐만 아니라 병목현상 발생으로 인한 서비스 지연을 피하기 위해 주어진 네트워크 패킷들을 여러 가용한 NSF 인스턴스들로 고르게 분배하여 처리할 수 있는 부하분배 또한 필요하다.

본 논문의 나머지 부분에서는 NFV 기반 네트워크 보안 서비스 제공에 관한 레퍼런스 시스템으로서 I2NSF 시스템을 소개한다. 그리고 이러한 시스템 모델을 기반으로 NFV 기반 네트워크 보안 서비스 시스템에서 핵심이 되는 연구이슈들에 관해 논의한다.

Ⅱ. NFV 기반 네트워크 보안 서비스 시스템: I2NSF 프레임워크

이 장에서는 NFV 기반 네트워크 보안 서비스 제공에 관한 레퍼런스 아키텍처로서 국제 인터넷 기술 표준화 단체인 IETF의 Interface to Network Security Functions (I2NSF) working group [4]에서 제안한 I2NSF(Interface to Network Security Functions) 시스템[2]에 대해 소개한다. 그림 2는 전체적인 I2NSF 시스템 아키텍처를 표현한 그림으로서 주요 시스템 구성요소들과 그들 간을 서로 연결하는 주요 인터페이스들을 보여준다.



〔그림 2〕 I2NSF 시스템 아키텍처: 구성요소 및 인터페이스

2.1. 시스템 구성요소

여기서는 I2NSF 시스템을 구성하는 주요 컴포넌트들인 I2NSF 사용자, 보안 컨트롤러, 보안 서비스 제공자 시스템 컨트롤러, 네트워크 보안 기능 각각에 대해 설명한다.

2.1.1. I2NSF 사용자

I2NSF 사용자는 다양한 외부 보안 서비스 제공자들로부터 NFV 기반의 네트워크 보안 기능(NSF)들을 이용하고자 하는 네트워크 시스템 관리자로서, 제공받은 네트워크 보안 기능들을 통해 자신이 관리하는 네트워크 시스템 및 트래픽을 보호하고자 한다. 기본적으로 사용자는 자신의 네트워크 시스템 및 트래픽 보호를 위한 사용자 친화적인 고수준의 보안 정책 명세를 작성하여 보안 컨트롤러에게 요청한다. 그림 2에서 보듯이 시스템에서 실행중인 세부 네트워크 보안 기능들은 사용자로부터 감춰지는 구조이기 때문에 고수준 보안 정책 명세 작성 시 사용자는 자신이 원하는 보안 정책 실현을 위해 궁극적으로 어떤 네트워크 보안 기능들이 필요한지 그리고 그들 각각에 대한 보안 정책 룰 등의 세부사항들에 대해서는 신경 쓸 필요가 없다.

실행중인 네트워크 보안 기능에서 악의적인 공격이나 의심스러운 네트워크 트래픽이 관찰된 경우 이는 보안 컨트롤러를 통해 사용자에게 보고된다. 사용자는 이러한 다양한 보안 이벤트들을 수집 분석함으로서 새로운 유형의 공격을 찾아낼 수 있을 뿐만 아니라 그러한 공격에 신속한 대응을 위해 보안 정책 명세를 수정하거나 새로 생성하여 요청할 수 있다[7].

2.1.2. 보안 컨트롤러

보안 컨트롤러는 I2NSF 시스템에서 사용자가 요청한 보안 정책이 적용될 수 있도록 네트워크 보안 기능들에 대한 다양한 제어 및 관리를 담당하는 핵심 구성요소이다. 보안 컨트롤러의 주요 역할 중 하나는 사용자로부터의 고수준 보안 정책을 네트워크 보안 기능들에 대한 저수준 보안 정책으로 변환하는 것이다. 세부적으로는 사용자로부터의 고수준 보안 정책을 실현하기 위해 어떤 종류의 네트워크 보안 기능들이 유기적으로 작용해야 하는지를 우선 결정한다. 그리고 나서는 선택된 네트워크 보안 기능들 각각에 대해서 고수준 보안 정책을 위해 필요한 저수준 보안 정책을 생성하여 해당 보안 기능들에게 전달 및 적용한다. 결과적으로 선택된 다양한 보안 기능들을 통해 새로운 저수준 보안 정책들이 유기적으로 작용함으로서 궁극적으로는 사용자가 요청한 보안 정책들이 네트워크 트래픽에 적용된다.

이와 더불어서 보안 컨트롤러는 시스템에서 운용중인 NSF들 각각에 대한 다양한 정보(예: IP주소, 지원되는 전송 프로토콜 타입, 작업 부하 상태)를 유지 관리하고, NSF들 상태에 대한 주기적인 모니터링을 수행한다. 또한 보안 서비스 제공자 시스템 컨트롤러와의 상호 작용을 통해 NSF 인스턴스들의 생명주기를 동적으로 관리한다.

2.1.3. 보안 기능 벤더 시스템 컨트롤러

이것은 I2NSF 시스템에 NFV 기반으로 네트워크 보안 기능들을 제공하는 외부 보안 서비스 벤더 시스템을 말하며, I2NSF 시스템의 필요에 따라 여러 보안 기능 벤더 시스템 컨트롤러들이 있을 수 있다. 이것은 보안 컨트롤러의 요청에 따라 새로운 NSF 인스턴스를 생성하여 제공하거나 더 이상 사용되지 않는 기존 NSF 인스턴스를 폐기하는 역할을 수행한다.

2.1.4. 네트워크 보안 기능(NSF) 및 보안 기능 전달자 (NSFF)

방화벽, DPI(Deep Packet Inspection), IDS (Intrusion Detection System) 등이 네트워크 보안 기능에 해당되며, 보안 컨트롤러에 의해 설정된 저수준 보안 정책에 따라 실제 네트워크 트래픽에 대한 보안 검사를 수행한다. 각각의 NSF의 독립적인 보안 검사와 더불어서 주어진 네트워크 트래픽에 대해 다양한 종류의 NSF들을 통한 복합적인 보안 검사 또한 가능하다. 이를 위해 NSF는 트래픽에 대한 자체 보안 검사 결과에 따라 추가적으로 필요한 다른 NSF를 호출하게 된다. 예를 들면 방화벽에서 패킷헤더 검사를 통해 알려지지 않은 의심스러운 트래픽이 관찰된 경우 이를 DPI로 전달하여 패킷 페이로드에 대한 보다 면밀한 분석을 수행하게 된다. 이를 지원하기 위해 NSF 전달자가 존재하며 첫 번째 NSF(방화벽)로부터 호출된 NSF(DPI)로 트래픽을 전달하는 역할을 수행한다.

2.2. 인터페이스

여기서는 I2NSF 시스템을 구성하는 주요 인터페이스들인 Consumer-Facing 인터페이스, NSF-Facing 인터페이스, Registration 인터페이스 각각에 대해 설명한다.

2.2.1. Consumer-Facing 인터페이스

Consumer-Facing 인터페이스는 I2NSF 사용자와 보안 컨트롤러 간을 연결하는 인터페이스이다. 그리고 이 인터페이스는 사용자 관점에서 I2NSF 시스템에 대한 유일한 인터페이스를 제공하며, 이러한 설계는 각각의 네트워크 보안 기능들에 대한 세부 사항(각 벤더 고유의 특징)을 숨김으로서 네트워크 보안 기능들에 대한 추상화된 관점을 사용자에게 제공한다.

이 인터페이스의 주요 목적은 사용자의 고수준 보안 정책을 보안 컨트롤러에게 전달함으로서 사용자가 원하는 보안 서비스/정책을 I2NSF 시스템에 요청하는 것이다. 또한 보안 컨트롤러는 NSF들로부터 보고 받은 보안 경고 및 이벤트들을 이 인터페이스를 통해 사용자에게 전달한다. 사용자는 이렇게 수집된 보안 경고 및 이벤트들을 분석함으로서 새로운 유형의 공격을 찾아낼 수 있으며, 그러한 공격에 신속한 대응을 위해 보안 정책 명세를 수정하거나 새로 생성하여 요청할 수 있다.

2.2.2. NSF-Facing 인터페이스

NSF-Facing 인터페이스의 주요 목적은 다양한 보안 솔루션 공급 업체들로부터의 네트워크 보안 기능들을 보다 효율적으로 제어 관리하기 위한 표준화된 인터페이스를 제공하는 것이다. 이를 위해 이 인터페이스는 각각의 네트워크 보안 기능들의 세부 사항들로부터는 독립적이며, 따라서 NSF에 대한 보안 정책 룰 설정 시 보안 컨트롤러는 그 NSF 고유의 보안 정책 룰 체계 또는 폼 팩터 등을 신경 쓸 필요가 없다.

기본적으로 이 인터페이스를 통해 보안 컨트롤러는 각각의 NSF에 대한 저수준 보안 정책 룰 설정 및 관리를 수행한다. 이러한 룰 설정을 통해 결과적으로 사용자가 원하는 고수준 보안 정책이 시스템에 적용되는 것이다. 뿐만 아니라 NSF에 대한 원격 제어 관리를 위해 보안 컨트롤러는 이 인터페이스를 통해 NSF에 대한 제어 명령을 호출할 수도 있다.

각각의 NSF는 이 인터페이스를 통해 보안 컨트롤러에게 자신의 현재 상태(예: 작업 부하 수준, 과부하 여부 등)를 주기적으로 알린다. 또한 보안 이벤트나 경고가 발생할 때마다 NSF는 이 인터페이스를 통해 그 사실을 보안 컨트롤러에게 보고한다.

NSFF는 이 인터페이스를 통해 보안 컨트롤러로부터 NSF들에 대한 네트워크 포워딩 정보를 전달 받으며, 이 정보를 기반으로 NSF 간 트래픽 포워딩을 수행한다. 만약 NSFF가 주어진 트래픽을 전달할 대상 NSF의 네트워크 포워딩 정보를 가지고 있지 않을 경우에는 이 인터페이스를 통해 보안 컨틀로러에게 해당 정보를 질의하게 된다.

2.2.3. Registration 인터페이스

그림 2에서 보는 바와 같이 Registration 인터페이스는 보안 컨트롤러와 보안 기능 벤더 시스템 컨트롤러 간을 연결한다. 이 인터페이스의 주된 목적은 시스템에서 운용중인 NSF 인스턴스들의 생명주기를 동적으로 관리하고 보안 기능 벤더 시스템 컨트롤러에 의해 새로 생성된 NSF 인스턴스를 보안 컨트롤러를 통해 I2NSF 시스템에 등록하기 위함이다.

현재 시스템에 새로운 NSF 인스턴스가 필요한 경우 보안 컨트롤러는 등록 인터페이스를 통해 벤더 시스템 컨트롤러에게 해당 NSF 인스턴스의 생성을 요청한다. 이때 보안 컨트롤러의 요청에는 생성될 NSF 인스턴스가 어떤 종류의 보안 기능을 제공해야 하는지, 얼마만큼의 서비스 처리 용량을 가져야 하는지 등에 대한 정보를 명시한다. 이러한 요청을 수신 시 벤더 시스템 컨트롤러는 수신된 요청에 명시된 보안 기능과 서비스 처리 용량을 제공하는 NSF 인스턴스를 새로 생성한 다음 생성된 인스턴스에 대한 네트워크 접근 정보를 보안 컨트롤러에게 알린다. 이 네트워크 접근 정보는 시스템에서 NSF 인스턴스에 대한 고유 식별자로 활용된다.

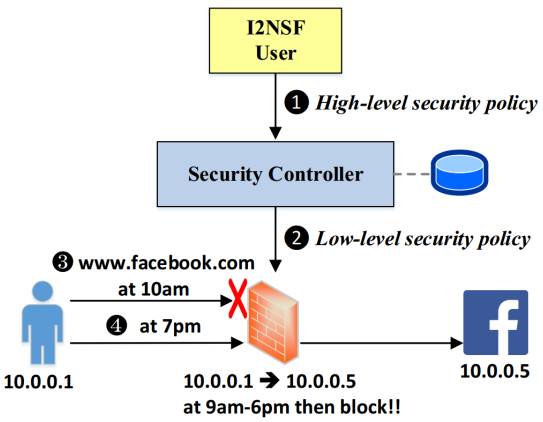
반대로 기존에 운용중인 NSF 인스턴스들 중 활용도가 낮아서 더 이상 필요하지 않다고 판단되는 인스턴스가 있을 경우 보안 컨트롤러는 등록 인터페이스를 통해 보안 기능 벤더 시스템 컨트롤러에게 해당 인스턴스의 폐기를 요청한다. 폐기 요청의 경우 폐기할 NSF 인스턴스의 고유 식별자인 네트워크 접근 정보가 포함된다.

2.3. I2NSF 시스템을 이용한 보안 서비스 예

본 절에서는 보안 서비스를 필요로 하는 회사 네트워크 시스템을 예로 I2NSF 시스템을 통한 보안 정책 적용 예를 설명한다. 이 시나리오에 회사 네트워크 시스템에서는 업무 시간 중 직원들의 소셜 네트워킹 사이트 접속이 차단되어야 한다고 가정한다. 그림 3은 이 시나리오에 대해서 I2NSF 시스템을 통한 보안 정책 적용 예를 묘사한다.

이 보안 정책을 적용하기 위해 우선 I2NSF 사용자에 해당하는 회사 네트워크 관리자는 보안 컨트롤러에게 요청할 고수준 보안 정책을 작성한다. 고수준 보안 정책의 예는 다음과 같다: "오전9시~오후6시까지 회사 직원들의 소셜 네트워킹 사이트에 대한 모든 접속을 차단한다." 사용자는 작성된 고수준 보안 정책을 Consumer-Facing 인터페이스를 통해 보안 컨트롤러에게 전달한다.

사용자로부터 고수준 보안 정책을 전달 받은 보안 컨트롤러는 그에 대응되는 NSF에 대한 저수준 보안 정책을 생성한다. 이를 위해 보안 컨트롤러는 먼저 회사 네트워크 시스템의 IP 주소 매핑 테이블을 참조하여 각 직원이 사용하는 IP 주소 리스트 만든다. 또한 모든 소셜 네트워킹 사이트들의 URL 혹은 IP 주소 리스트를 만든다. 이렇게 생성된 정보를 이용해서 오전9시~오후6시 중에 직원 IP로부터 소셜 네트워크 사이트 URL 혹은 IP로의 패킷을 차단하는 방화벽 룰을 생성한다. 그리고 나서 보안 컨트롤러는 생성된 룰을 NSF-Facing 인터페이스를 통해 방화벽에 해당하는 NSF에게 전달하여 적용한다.



〔그림 3〕 I2NSF 시스템을 이용한 보안 정책 적용 예: 회사 네트워크 시스템에서 업무 시간 중 소셜 네트워킹 사이트 접속 차단

룰이 설정된 방화벽은 수신된 모든 패킷들에 대해서 패킷 헤더에 소스 IP와 목적지 IP 확인을 통해 직원 컴퓨터로부터 페이스북 사이트로의 패킷인지를 확인한다. 또한 현재 시간을 체크하여 해당 패킷이 업무 시간 중에 발생된 것인지를 확인한다. 만약 두 조건이 모두 만족될 경우 그 패킷은 위에서 생성된 방화벽 룰에 매칭되고 결과적으로 차단된다.

Ⅲ. 연구 이슈/과제

여기서는 I2NSF 시스템 아키텍처에 관한 논의를 바탕으로 NFV 기반 네트워크 보안 서비스 제공 시스템 설계 및 개발 시 고려해야 할 주요 연구이슈들에 관해 논의한다.

〔표 1〕 NFV 기반 네트워크 보안 서비스 시스템에서 주요 연구이슈

카테고리	주요 연구이슈
사용성	사용자 친화적인 고수준 보안 정책 설정 지원
	다양한 보안 벤더들로부터의 NSF들에 대한 표준 인터페이스
	보안 정책 룰들 간 충돌 문제
보안	불법적인 트래픽 감청
	불법적인 트래픽 변조
성능/효율성	네트워크 상황과 보안 요구사항에 맞게 NSF 인스턴스들의 동적 생성 및 폐기
	NSF 인스턴스들에 대한 효율적인 부하 분배

3.1. 사용성 이슈

NFV 기반 네트워크 보안 서비스 시스템의 사용성을 높이기 위해서는 사용자에게 간편한 보안 정책 설정을 지원하는 것이 중요하다. 이를 위해 보안 컨트롤러는 사용자와 네트워크 보안 기능들 중간에서 이들 간을 매개하는 역할을 하며, 이를 통해 실제 네트워크 보안 기능들의 세부사항들은 사용자로부터 숨겨진다. 이러한 아키텍처에서 보안 컨트롤러의 중요한 역할은 사용자로부터 받은 고수준 보안 정책으로부터 필요한 네트워크 보

안 기능들에 대한 저수준 보안 정책들을 생성하는 것이다. 이를 위해서는 우선 사용자의 고수준 보안 정책을 실현하기 위해서는 어떤 네트워크 보안 기능들이 필요한지를 결정해야 한다. 그리고 나서 선택된 네트워크 보안 기능들이 유기적으로 동작함으로서 궁극적으로 사용자의 보안 정책 집행되도록 하기 위한 네트워크 보안 기능들에 대한 저수준 보안 정책을 생성해야 한다.

시스템에 다양한 보안 정책 룰들이 존재하는 상황에서는 필연적으로 룰들 간 충돌이 발생할 수 있다. 그리고 이러한 보안 정책 룰 간 충돌이 발생한 상황에서 사용자의 직접 개입을 최소화 하면서 이러한 충돌을 해결하는 것이 시스템 사용성 면에서 중요하다. 이를 위해서는 우선 잠재적인 충들을 미연에 방지할 수 있도록 저수준 보안 정책 생성 시 주의 깊게 설계되어야 한다. 또한 다양한 네트워크 보안 기능들이 동작하고 있는 상황에서 보안 컨트롤러는 이들에 대한 지속적인 모니터링을 통해 충돌 발생을 신속하게 감지하고 해결해야 한다.

다양한 보안 서비스 벤더들로부터의 네트워크 보안 기능들이 운영되고 있는 상황에서 그들에 대한 제어 관리 작업의 복잡도를 줄이는 것이 시스템 사용성 면에서 중요하다. 이러한 목적을 위해서 다양한 네트워크 보안 기능들에 대해 일관성 있는 제어 및 관리를 가능하게 하기 위한 표준화된 인터페이스가 정의되어야 한다.

3.2. 보안 이슈

NFV 기반 네트워크 보안 서비스 시스템에서 실질적으로 네트워크 트래픽에 대한 사용자의 보안 정책이 적용되려면 대상 트래픽이 외부 보안 벤더의 클라우드 시스템에서 실행되고 있는 네트워크 보안 기능(NSF)로 전달되어야 한다. 그런데 만약 외부 보안 벤더의 클라우드 시스템이 악의적인 공격자의 제어 하에 놓인 상황이라면 그 네트워크 트래픽은 다양한 유형의 공격에 노출되게 된다. 한 가지 가능한 공격은 트래픽이 전달될 NSF 소프트웨어를 불법적으로 변경하여 사용자 몰래 트래픽에 포함된 민감한 데이터를 감청하는 것이다. 또 다른 유형의 공격으로는 공격자가 악의적인 의도를 가지고 트래픽에 포함된 데이터를 불법적으로 변경하는 것이다. 예를 들면 특정 보안 정책을 우회하기 위한 목적으로 패킷에 주요 부분을 불법적으로 변경하는 것이다. 또한 공격자는 NSF의 보안 정책 설정을 불법적으로 변경함으로서 시스템에서 실행중인 보안 서비스 자체를 무력화 시킬 수 있다. 이러한 다양한 유형의 공격들로부터 시스템 및 네트워크 데이터를 보호하는 것이 NFV 기반 네트워크 보안 서비스 시스템 성공을 위해 반드시 필요하다.

3.3. 성능/효율성 이슈

시스템이 운영되는 동안 네트워크 상황이나 사용자의 보안 요구사항이 동적으로 변동될 수 있다. 그리고 NFV 기술의 가장 큰 장점 중 하나는 이러한 가변적인 상황에 신속하고 유연한 대처가 가능하다는 것이다. 예를 들면 사용자의 시스템이 DDoS 공격을 받고 있는 상황에서 IDS를 통해 유입되는 트래픽을 검사하고 공격일 경우 필터링 해야 하는 상황이라면 IDS 인스턴스를 늘림으로서 대량의 트래픽에 효과적으로 대처할 수 있어야 한다. 뿐만 아니라 충분한 수의 NSF 인스턴스들이 가용하다고 하더라도 일부 특정 인스턴스로만 트래픽이 몰리게 된다면 병목 현상으로 인한 서비스 지연이 발생하게 된다. 따라서 효율적인 부하분배 또한 중요한 이슈이다.

Ⅳ. 결 론

다양한 네트워크 시스템 보호를 위해 외부 보안 솔루션 벤더들로부터 제공되는 가상화 기반 네트워크 보안 기능들을 활용하는 시스템 형태가 점차 나타나고 있다. 본 논문에서는 이러한 NFV 기반 네트워크 보안 서비스 제공에 관한 레퍼런스 아키텍처로서 I2NSF 시스템을 소개하고, 이러한 시스템 환경에서 고려해야 할 주요 연구이슈들에 대해 논의했다. NFV 기반 네트워크 보안 서비스 시스템에서는 일반적으로 다양한 보안 벤더들로부터의 NSF들이 공존하는 상황이기 때문에 이런 다양한 NSF들에 대한 효율적이고 통일된 제어 및 관리를 제공하기 위한 표준 인터페이스가 반드시 필요하다. 뿐만 아니라 보안 서비스 사용자의 편의를 위해 다양한 NSF들에 대한 세부사항들까지 신경 쓸 필요 없이 보다 사용자에게 친숙한 보안 정책 설정을 지원해야 한다. 또한 가변적인 네트워크 상황 및 보안 요구 사항들에 효과적으로 대응하기 위한 유연한 아키텍처의 설계 또한 중요한 이슈이다.

참 고 문 헌

[1] A Trend Micro Technical White Paper, "Advanced Security Services with Trend Micro Deep Security and VMware NSX Platforms", June 2015.

[2] J. Strassner, L. Dunbar, D. Lopez, E. Lopez, and R. Kumar, “Framework for Interface to Network Security Functions”, Internet Engineering Task Force, Internet-Draft,draft-ietf-i2nsframework-04, Oct. 2016, work in Progress.

[3] N. ETSI, "GS NFV-MAN 001 v1. 1.1 Network Function Virtualisation (NFV); management and orchestration", 2014.

[4] Interface to Network Security Functions (I2NSF) Working Group", Oct. 2014, https://datatracker.ietf.org/wg/i2nsf/charter/

[5] Susan Hares, Diego R. Lopex, Myo Zarny, Christian Jacquenet, Rakesh Kumar, Jaehoon Paul Jeong, “I2NSF Problem Statement and Use cases”, Internet Engineering Task Force, Internet-Draft, draft-ietf-i2nsf-problem-and-use-cases-06, Jan. 2017.

[6] Jaehoon (Paul) Jeong, "I2NSF Technology and Standardization Trend", OSIA Standards & Technology Review Journal, Vol. 28, No. 4, December 2015.

[7] Sanghak Oh, Eunsoo Kim, Jaehoon Jeong, Hoon Ko and Hyoungshick Kim, “A Flexible Architecture for Orchestrating Network Security Functions to Support High-Level Security Policies”, ACM IMCOM(ICUIMC), Jan. 2017.

[8] Jeff Wilson, “Delivering Security Virtually Everywhere with SDN and NFV”, IHS INFONETICS WHITE PAPER, Jul. 2015.

〈저 자 소 개〉

현 상 원 (Sangwon Hyun)

2002년 2월 : 성균관대학교 전기전자컴퓨터공학부 졸업

2004년 2월 : 서울대학교 컴퓨터공학과 석사

2011년 12월 : North Carolina State University 전산학 박사

관심분야 : 정보보호