Journal of the Korea Convergence Society
Vol. 9. No. 12, pp. 61-68, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.12.061

안전한 클라우드 환경을 위한 소프트웨어 정의 경계 기반의 네트워크 보안 솔루션 제안

차욱재[1], 신재인[1], 이동범[2], 김협[1], 이대효[3*]
[1]지니언스(주) 선임연구원, [2]지니언스(주) 대표이사, [3]지니언스(주) 연구기획실 실장

Proposal of Network Security Solution based on Software Definition Perimeter for Secure Cloud Environment

Wuk-Jae Cha[1], Jae-In Shin[1], Dong-Bum Lee[2], Hyeob Kim[1], Dae-Hyo Lee[3*]
[1]Senior researcher, Division of Research Planning Office, Genians,Inc
[2]CEO, Genians,Inc
[3]General Manager, Division of Research Planning Office, Genians,Inc

요 약 스마트폰과 모바일 환경이 발전하면서 개인의 업무 수행을 위한 시간과 공간의 제약이 사라지고 있다. 기업은 클라우드 컴퓨팅을 통하여 비용을 절감하고 사업의 범위를 빠르게 확대할 수 있게 되었다. 다양한 클라우드의 사용이 확대되면서 사용자, 데이터, 어플리케이션의 경계가 사라지고 있다. 경계(Perimeter)을 기준으로 하는 전통적인 보안 접근은 클라우드 환경에서 효용을 잃어가고 있다. 이에, 본 논문에서는 클라우드 환경에서 기존 Network Access Control(NAC)의 한계를 기술하고 이를 보완한 네트워크 보안 기술을 제안한다. 관련연구로 SDP에 대해서 설명하고, NAC의 한계를 극복하기 위해 SDP(Software Defined Perimeter)를 융합하고 동시에 클라우드 환경의 지원을 위한 새로운 프레임워크로의 역할을 설명한다. 본 논문에서 제안한 새로운 프레임워크는 물리적인 부분과 소프트웨어적인 부분에 SDP 기술을 적용하여 IP 기반이 아닌 신원 중심 접근제어 제공, 암호화된 세그먼트 관리, 동적정책관리 등을 지원하는 소프트웨어 기반의 네트워크 보안 솔루션을 제안한다.

주제어 : 소프트웨어정의, 경계, 네트워크 접근제어, 사물인터넷, 블랙 클라우드

Abstract As the smartphone and mobile environment develop, the time and space constraints for individual work performance are disappearing. Companies can reduce costs and expand their business quickly through cloud computing. As the use of various cloud expands, the boundaries of users, data, and applications are disappearing. Traditional security approaches based on boundaries (Perimeter) are losing their utility in the cloud environment. This paper describes the limitations of existing network access control (NAC) in a cloud environment and suggests network security technology that complements it. The study explains the SDP and combines SDP(Software Defined Perimeter) to overcome the limitations of NAC, while at the same time explaining its role as a new framework for supporting the cloud environment. The new framework proposed in this paper suggests a software-based network security solution that supports physical and software parts, providing identity-based access control, encrypted segment management, and dynamic policy management, not IP-based.

Key Words : SDx(Software-Defined Everything), Perimeter, Network Access Control, IoT(Internet of Things), Black Cloud

*This work was supported by the Advanced Technology Center(ATC) Program.
[No.10076453, Black-Cloud Application Technology Development based on SDP(Software-Defined Perimeter) for Access Management and Control of Unauthorized Device.]
*Corresponding Author : Dae-Hyo Lee (dado@genians.com)
Received October 9, 2018 Revised November 28, 2018
Accepted December 20, 2018 Published December 28, 2018

1. 서론

클라우드 시장은 폭발적으로 성장하고 있다. 포레스터 리서치(Rorrester Research)에 따르면 2020년 전세계 클라우드 컴퓨팅 시장규모는 2,410억 달러에 이른다고 한다. 국내의 경우 2015년 '클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률' 이 시행되면서 클라우드 발전을 위한 국가와 지방자치단체의 책무 등이 명시되었고 국가기관의 클라우드컴퓨팅 도입을 촉진하는 등 보급 및 확대에 노력하고 있다. 전문가들은 상호운영성과 데이터이동성 그리고 보안문제를 해결해야 하는 가장 중요한 문제로 지적하고 있다. 보안 문제는 기존 IT 환경에서의 문제뿐 아니라 가상인프라와 자원공유 그리고 자원집중화 등의 클라우드 아키텍처로 인한 문제까지도 고려해야 하는 매우 중요한 문제이다[1,14,15].

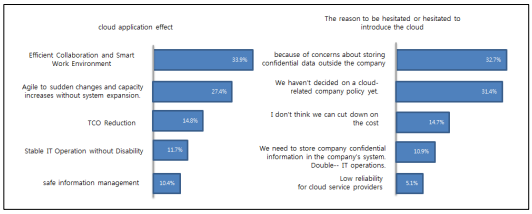

Fig. 1. Cloud Introduction Effect and Reason

클라우드 보안에 대한 우려는 이미 현실화되고 있다. 2010년 아마존(AWS) EC2 백업오류로 인해 190여개의 서비스가 11시간 동안 마비되는 사고가 발생하였다. 2012년 사회공학적 기법을 이용하여 아이클라우드(iCloud), 지메일(gmail), 트위터(Twitter)에서 계정이 탈취되고, 2013년 백도어 활동 및 C&C 서버의 수집정보 은닉을 위해 에버노트(Evernote)가 활용되는 등의 사고가 연이어 발생하였다. 이외에도 많은 회사 및 개인정보의 유출, 데이터의 소실 등 사고가 지속적으로 발생하고 있다[12,13].

2017년 CSA(Cloud Security Alliance)의 'The Treacherous 12' 보고서는 전문가 설문을 통하여 클라우드에서 발생할 수 있는 주요 보안위협 12가지를 소개하였으며, 해당 내용은 다음 장에 기술된다[4].

2. 관련 연구

2.1 NAC 솔루션과 한계

스마트폰의 확대와 함께 BYOD(Bring Your Own Device) 환경이 대중화 되면서 내부에서 빠르게 증가하는 사용자 단말을 효과적으로 관리할 수 있는 방법이 필요하다. NAC는 권한과 보안규정에 따라 사용자 및 단말에 접근제어 기능을 제공하면서 내부통제를 위한 실질적인 기능을 제공한다. 이러한 온 보딩(On-Boarding) 관리를 넘어 통합인증(IAM), IP관리(IPM), 자산관리(DMS), 패치관리(PMS)등의 다양한 부가기능을 제공하며 내부통제/관리 솔루션의 대명사로 자리매김 하였다. 그러나 클라우드 환경이 확대 및 대중화 되면서 내부 통제를 위한 NAC에도 많은 변화가 요구되고 있다[6,7].

확대된 클라우드 환경이 발생할 수 있는 주요 보안위협 12가지는 다음 표와 같이 요약하였다.

Table 1. The Treacherous 12

Major Threat (severity order)	Description
data outflow	Sensitivity information leakage by mistakes, vulnerabilities, etc.
authentication and permission	Data tapping by unauthorized access, and so on
interface	Bypass of the management interface and malicious attempts, and so on
system vulnerability	Permissions and data hijacking using vulnerabilities
account hijacking	Eavesdropping and infringement through account hijacking
malicious insider	Unethical conduct of legitimate authority holders
intelligent threat	Loss of control by APT and so on
data loss	Permanent loss of data due to disaster
insufficient due diligence	Accidental damage caused by improper use
misuse and abuse	Misuse as a stopper for spam, phishing, etc.
denial of service	Availability Infringement by the use of malicious excessive resources
shared technology vulnerability	Security concerns due to the sharing of assets (platforms, etc.)

또한, Cyxtera Technologies의 보고서는 NAC의 한계를 아래와 같이 기술하고 있다[5].

2.1.1 CLOUD 확장의 한계

내부통제를 목적으로 구축한 NAC는 클라우드를 지원하기 어렵다. 클라우드 지원을 위한 별도의 솔루션이 필요하며 이것은 네트워크 보안을 위한 또 다른 보안 계층

(Layer)의 추가를 의미 한다.

2.1.2 VLAN구성에 의존

다수의 NAC는 VLAN 구성을 요구한다. VLAN은 효과적인 네트워크 관리 기술이나 항상 최신의 상태로 유지하기 어렵고 확장에 한계가 존재한다.

2.1.3 트래픽 암호화

다수의 네트워크 어플리케이션이 암호화(encryption)를 지원하고 있다. 보고서에 따르면 약 50%이상의 네트워크 통신이 HTTPS, TLS 등을 통해 암호화 되어 전송되고 있으며 향후 더욱 증가할 것으로 예상된다. 복호화하지 않는 경우 암호화된 내용을 확인하기가 쉽지 않으며 이를 통한 보안정책의 우회가 우려되고 있다.

2.1.4 정책 수립 운용 문제

NAC의 접근제어 정책은 존재하거나 접근이 가능한 네트워크 및 네트워크 장비(방화벽, VPN 등)를 대상으로 한다. 만약 IP를 보유하고 있지 않거나 IP가 수시로 변하는 어떠한 대상이 있다면 이것에 대한 접근제어 정책을 수립 운용하기는 쉽지 않다.

2.1.5 원격지 사용자

원격지 사용자가 내부 접근을 시도하거나 원격지 간의 접근을 시도하는 행위에 대하여 NAC는 효과적인 대응방법을 제공하지 못 한다. 별도의 VPN 클라이언트 등이 필요하거나 사용자 인증 또는 NAC 에이전트 등이 요구될 수 있으며 이를 위한 복잡한 보안정책의 운용이 필요할 수 있다.

2.1.6 동적 환경 변화

매 순간 변하는 환경에 맞는 보안정책을 수립, 유지하기 위해서는 특별한 노력과 기능이 요구될 수 있다. 5 tuple(IP, Port, Protocol 등)기반의 전통적인 보안정책은 이러한 동적(dynamic)환경을 지원하기에 적절하지 않다.

2.1.7 문맥을 고려한 보안정책운용

더욱 효과적인 보안정책의 수립과 운용을 위해 더 많은 정보가 요구될 수 있다. 위치(location), 역할(role), 인증(I.A.M), 단말의 상태(Posture) 및 심지어 해킹여부(Compromised) 등도 필요할 수 있다. 전용 에이전트가 필요하거나 실시간 상태(status) 동기화 등이 요구된다.

2.2 클라우드 보안 기술

NAC의 한계를 극복하기 위한 중요한 부분으로 클라우드 환경의 확대지원과 함께 보안에 대한 확장성과 유연성이 요구된다.

산업계 전문가들은 클라우드 보안을 위한 핵심적인 기술로 가상화 인프라의 침입탐지/차단 기술, 데이터 암호화 기술, 접근제어 및 인증기술 등을 제안하고 있다.

2.2.1 가상화 인프라의 침입 탐지/차단 기술

초기 위협의 침투 및 확산을 탐지하거나 차단하는 기술이 요구된다. 다수의 클라우드 환경은 높은 효율을 위하여 가상화 기술을 사용한다. 다수의 가상머신(VM)이 단일한 물리적 호스트에서 동작하는 경우 각 가상머신의 안전한 동작은 보증되어야 하며 가상머신간의 통신 역시 보호해야 한다. 특정 가상머신이 침해(Compromised) 되거나 하이퍼바이저(hypervisor)등의 운영기반이 해킹되는 경우 피해가 전체로 확대될 수 있다.

2.2.2 데이터 암호화 기술

가장 빈번한 클라우드 보안사고는 자료유출(Data Breach & Leakage) 이다. 자원의 공유와 집중화에 따라 설정오류, 내부자 실수, 비인가 접근 등에 의해 자료유출이 발생할 수 있다. 자료유출에 따른 2차 피해를 방지하기 위해서라도 클라우드에 저장되는 데이터는 암호화 되어야 한다. 또한 서비스와 사용자, 서비스와 서비스간의 데이터 이동에도 암호화를 지원한다.

2.2.3 접근제어 및 인증기술

스마트폰과 모빌리티를 이용하여 언제 어디서나 클라우드 기반의 다양한 개인용, 업무용 서비스를 제공받는다. 모바일 기기의 클라우드 접속 시, 접근제어 및 인증기술은 단순한 IP 또는 ID/PW 기반이 아닌 단말과 사용자의 종합적인 정보를 이용하는 상황인식 기반의 통합 보안기능이다.

2.3 클라우드 보안 기술 상용화

클라우드 보안기술을 구체적으로 상용화 한 사례로 CASB 와 SDP를 들 수 있다. 특히 CASB는 앞에서 기술한 클라우드 보안 기술의 대부분을 수용하고 있어 최근 가장 주목 받고 있다.

2.3.1 CASB(Cloud Access Security Broker)

CASB는 클라우드 서비스 이용자와 클라우드 서비스 사이에 위치하여 독립적으로 보안 기능을 수행하는 솔루션이다. 에이전트, 어플라이언스(Appliance), API 등 다양한 형태로 제공되며 클라우드 서비스 이용에 대한 가시성의 확보, 접근통제, 내부정보 유출방지, 이상탐지, 로깅, 감사 등의 보안 기능을 수행한다.

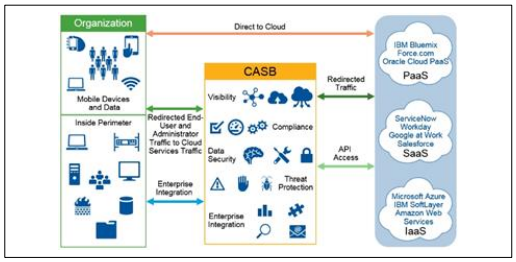

Fig. 2. Cloud Access Security Broker

2.3.2 SDP(Software Defined Perimeter)

SDP는 또 하나의 소프트웨어 정의 기술(SDX: Software Defined X)이다. CSA(Cloud Security Alliance) 가 추진하고 있는 접근제어를 위한 차세대 프레임워크이다. SDP는 컨트롤러, 게이트웨이(또는 서버), 클라이언트로 구성되어 클라우드 환경에서 모호해진 경계(perimeter)를 명확히 설정할 수 있으며, 이를 기반으로 네트워크 접근 및 통제가 가능하다[3].

3. 제안사항

3.1 클라우드 보안을 위한 표준 SDP

표준 SDP는 사용자의 상태 및 신원을 기반으로 하는 접근제어 프레임워크이다. 사용자의 신원에 따라 접근이 가능한 개별적인 세그먼트를 동적으로 생성되고 매우 정교한 접근제어 정책수립이 가능하므로(micro segmentation) 아래와 같은 효과를 기대할 수 있다.

- 클라우드 및 엔터프라이즈 네트워크 대상의 안전한 액세스 정책 운용
- SDP적용에 따른 네트워크 구성의 단순화
- 운영노력의 감소 및 하이브리드 환경에서 일관된 액세스 정책의 보장

3.1.1 표준 SDP 개요

'블랙클라우드(Black Cloud)'라고도 불리는 SDP는 2007년 전후 미국의 정부기관인 DISA(Defense Information Systems Agency)에서 수행한 컴퓨터 보안 접근방식이 발전, 변형된 형태이다.

SDP의 핵심 개념은 '(어플리케이션의) 연결이 허용되기 이전에 상태 및 ID(신원)의 승인이 필요하다' 이다. 승인된 사용자 및 어플리케이션은 접속 대상을 확인할 수 있으며 개별적이고 신뢰할 수 있는 보안연결을 제공받는다. 반대로 미 승인된 경우 접속 대상조차 확인할 수 없는 '블랙(black)'의 상태가 된다. 공격자에게 노출을 최소화여 DDoS 등으로부터 자산을 효과적으로 보호할 수 있다.

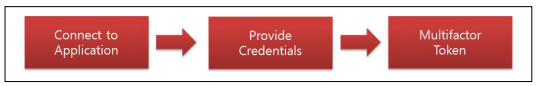

Fig. 3. Current Connected Model Based TCP/IP

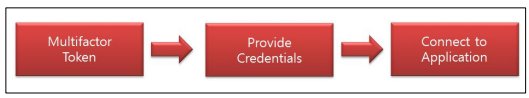

Fig. 4. Connected Model Based SDP

3.2 SDP의 특징

3.2.1 선 인증, 후 연결 방식

식별이 완료되고 권한이 부여되면 권한에 따라 접근이 가능한 자원의 목록을 확인할 수 있다. 권한이 없는 사용자 및 어플리케이션은 자원의 존재여부 자체도 확인할 수 없다.

3.2.2 IP 기반이 아닌 신원 중심 액세스 제어 제공

5 tuple이 아닌 '인증된 보안 관리자' 및 '안전한 스마트폰 단말기' 등과 같이 신원과 상태에 의한 정책의 수립 및 운용이 가능하다.

3.2.3 암호화된 세그먼트 관리를 제공

모든 사용자의 접근은 각각 개별화된 세그먼트로 관리되며 그 내용은 암호화 된다. 개별화된 세그먼트와 관련이 없는 모든 내용은 다른 사용자에게 노출되지 않는다.

3.2.4 동적정책관리 제공

새로운 자원(서버, 애플리케이션 등)이 생성되면 자동

으로 신원 및 상태에 따라 적절한 접근권한이 부여되거나 거부된다. 접근요청자 및 접근대상의 컨텍스트(시간, 위치, 장치 상태 등)에 따라 함께 변경되므로 지속적인 유지가 가능하다.

3.2.5 단순 및 일관성

접근제어 정책을 쉽게 수립할 수 있으며, 내부 네트워크부터 클라우드에 이르기까지 일관성 있게 적용할 수 있다.

3.3 표준 SDP 아키텍처와 동작(워크플로우)

아래 Fig. 5 는 SDP의 구성요소와 함께 제어 및 데이터의 흐름을 보여주고 있다.

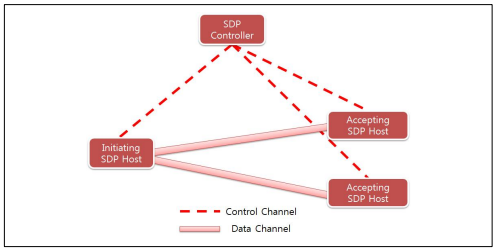

Fig. 5. SDP Specification 1.0, CSA

3.3.1 SDP Controller

SDP 컨트롤러는 모든 SDP 구성요소(SDP 게이트웨이 및 클라이언트)와 통신하며 관리자 역할을 수행한다. 가장 중요한 역할은 정책에 따른 구성요소 간의 연결가능 여부의 결정이다. 클라이언트의 접속 요청에 따라 신원 및 상태 등을 확인하고 접근제어 정책을 각 구성요소에 전달한다.

3.3.2 SDP Client (or Initiating SDP Host)

SDP 클라이언트는 컨트롤러와 통신하여 접속이 가능한 목록을 요청한다. 컨트롤러는 클라이언트에게 인증 및 상태 등의 추가정보를 요청할 수 있으며, 이 응답에 따라 접근 가능한 게이트웨이 또는 호스트의 목록을 전달 받는다.

3.3.3 SDP Gateway (or Accepting SDP Host)

SDP 게이트웨이는 컨트롤러를 제외한 모든 접속 요청을 거부(reject)한다. 컨트롤러에 의해 신원이 확인된 사용자 및 어플리케이션에 대한 연결 기능을 제공한다.

컨트롤러는 RADIUS, PKI, OpenID, OAuth, LDAP 등의 다양한 인증방법과 연동될 수 있으며 추가적인 상태정보 등을 요청할 수 있다.

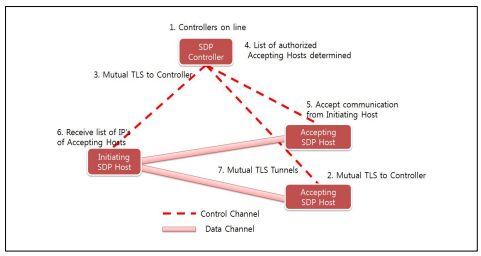

Fig. 6. SDP Specification 1.0, CSA(flow description)

3.4 기존 NAC와 SDP 기술의 비교 분석

Genian NAC는 대표적인 상용 네트워크 접근제어 솔루션으로 구성요소와 표준 SDP의 구성요소 간의 주요기능을 비교하면 아래와 같다.

Table 2. Compared to NAC and SDP components

Main Function	existing NAC components	SDP components
Access control Policy Management	policy server	SDP controller
Network Information Collection Network Control	Sensor	SDP Gateway
Terminal Information Collection	Agent	SDP Agent

3.4.1 SDP 컨트롤러(NAC 정책서버)

NAC 정책서버의 고도화를 통해 SDP 컨트롤러를 대체할 수 있다. 이미 사용자와 단말에 대한 식별과 인증기능을 제공하고 있으며 클라이언트와 센서를 위한 접근제어 정책을 관리한다. 기존의 '1:N 또는 N:1' 기반의 정적(static) 보안정책을 넘어 'M:N' 기반의 동적(dynamic) 정책 수립 및 관리가 가능하다. 클라우드 환경을 포함하여 정교하고 균일한 보안정책을 수립, 운용할 수 있다.

3.4.2 SDP 게이트웨이 (NAC 센서)

NAC 센서는 네트워크에 위치하여 네트워크 상의 자산을 식별하고 접근통제(Enforcer)기능을 수행한다. 아웃오브밴드(OOB) 와 가상화(VM) 뿐 아니라 인라인(in-line) 기반을 지원해야 한다. 이를 통해 네트워크 트래픽을 분석하고 서비스와 위협(threat) 여부 등으로 식

별의 범위를 확장하게 된다. 승인되고 권한을 보유한 클라이언트에게 암호화 통신을 제공하며 암호화 되지 않은 내용은 보안정책을 위해 또는 보안정책에 따라 분석될 수 있다.

3.4.3 SDP 클라이언트 (NAC 클라이언트)

연결을 요청하는 누구라도 SDP클라이언트가 될 수 있다. SDP 컨트롤러 및 게이트웨이와 통신을 위한 프로토콜을 지원해야 한다. 윈도우(Windows)뿐 아니라 맥(Mac OS), 리눅스(Linux) 등의 다양한 플랫폼을 지원하고 인증 및 식별을 위한 기능 역시 동일한 수준으로 지원되어야 한다. SDP 컨트롤러의 요청은 다양할 수 있다. ID/PW 등의 정적(Static)정보뿐 아니라 위치, IP, 시간 등의 동적(dynamic) 정보 그리고 OTP(One Time Password) 등의 온디맨드(On Demand) 요청 역시 포함될 수 있다. NAC와 SDP를 Table 3과 같이 비교할 수 있다. Genian SDP의 적용을 위하여 운영 중인 NAC를 포기할 이유는 없다. SDP는 NAC의 확대 발전된 형태이므로 기존의 NAC를 수용할 수 있다.

3.5 Genian SDP 제안

본 논문의 3.4에서 기존 NAC와 SDP 기술을 비교 분석한 결과 기존 NAC는 SDP와 유사한 구성요소를 제공한다. 이에, SDP의 주요 기술인 사용자 중심 접근제어, 암호화 통신, 동적 정책 관리 등을 추가 연구 개발하여 다음과 같이 SDP기술이 적용된 Genian SDP를 제안한다.

Table 3. Compare to NAC, SDP, Genian SDP

Main Technology	Genian NAC	SDP	Genian SDP
cloud support	X	O	O
multiple authentication	△	O	O
policy setting/distribution	O	O	O
dynamic policy	X	X	O
traffic encryption	X	O	O
traffic visibility	X	△	O
remote user support	X	O	O
clientless	X	X	O

아래 그림은 Genian SDP의 기본 구성을 보여준다. 아래 그림에서의 Site#는 VLAN 또는 서브네트워크와 같은 물리적인 구성 일 뿐만 아니라 특정 서비스 또는 어플리케이션의 그룹일 수도 있다. NAC 센서의 고도화를 통하여 이러한 것이 가능해 진다. 물론 클라우드 일수도 있다. 관리자는 클라이언트의 접속 요청에 대하여 매우 정교하면서 유연하게 확장 가능한 경계(Perimeter)를 정의할 수 있게 된다.

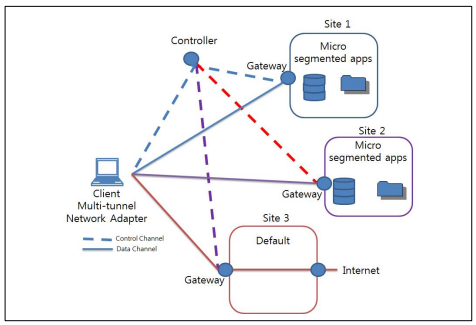

Fig. 7. Genian SDP Applicate Architecture

3.6 Genian SDP 장점

본 논문에서 제안한 Genian SDP를 적용 할 경우 다음과 같은 장점이 있다.

3.6.1 Zero-Trust Defense

신뢰할 수 있는 대상과 그렇지 못한 대상을 식별하는 것은 어려운 일이다. 구분하여도 그것들 간의 연결 정책을 유지하고 운영하는 것은 별개이다. Genian SDP를 통해 Zero-Trust 모델을 구축할 수 있다. 아무것도 신뢰하지 않는 상태(Zero-Trust)에서 출발하는 것이다. 그러나 '상태 - 식별 - 인증 - 권한' 등의 단계를 통해 신뢰를 획득하고 신뢰수준을 높일 수 있는 프로세스를 제공할 수 있다. 이것은 운용관점에서 기존의 보안 프레임워크 대비 간단하고 효과적인 방법이다.

3.6.2 RDAP(Role based Dynamic Access Policy)

역할기반의 접근제어가 가능하다. '오직 보안 관리자만 클라우드 DB에 접근할 수 있다' 와 같은 정책을 수립하고 운영하는 것이 가능하다. 모든 정책은 사용자 또는 애플리케이션 기반으로 M:N 의 형태로 수립할 수 있다.

3.6.3 하이퍼스케일링(Hyper-Scaling)

SDP 컨트롤러의 중복 구성은 물론, 하나의 세그먼트에 여러 개의 SDP 게이트웨이를 구성하는 것도 가능하다. 정책은 더 이상 IP에 국한되지 않기 때문이다. 사용

자, 어플리케이션, IP, Device를 위한 전용의 게이트웨이 구축이 가능하며 유연한 확장이 가능하다.

4. 결론

현대 시대의 네트워크 환경은 클라우드와, IoT의 도입으로 네트워크 환경이 빠르게 변화 되고 있다. 기업들은 아마존(AWS)나 애저(Azure)와 같은 IaaS(Infrastructure-as-a-Service)로 빠르게 이전하고 있으며, SaaS(Service-as-a-Service) 형태의 어플리케이션을 도입하고 있다. 이렇게 다양한 클라우드의 사용이 확대되면서 이제 사용자, 데이터, 어플리케이션의 경계가 사라지고 있다.

그러나 경계(Perimeter)을 기준으로 하는 전통적인 네트워크 접근제어 솔루션은 안타깝게도 클라우드 환경에서 더 이상 유용하지 않다. 이에, 본 논문에서는 새로운 환경에 대비하기 위한 안전한 클라우드 환경을 위한 소프트웨어 정의 경계 기반의 네트워크 보안솔루션인 Genian SDP를 제안하였다.

현재 Genian SDP는 사용자 중심 접근제어, 암호화 통신, 동적 정책 관리 기능 등을 추가 하여 SDP 기반의 네트워크 접근제어 솔루션으로 연구 및 개발을 진행하고 있다.

Genian SDP는 클라우드 및 IoT환경에서 네트워크 접근제어 솔루션으로 활용 가능하며, 원격 사용자 및 다 지점환경의 보안관리 솔루션으로 활용 가능하다. 본 논문을 통해서 클라우드 보안시장의 발전에 도움이 되었으면 한다.

REFERENCES

[1] Korea IDG Report. what makes you hesitate to be applicate cloud security?

[2] Take The Wheel: Build Your Cloud Computing Strategic Plan Now Strategic Plan: The Cloud Computing Playbook.

[3] CLOUD SECURITY ALLIANCE(April 2014), Software Defined Perimeter Working Group, SDP Specification 1.0

[4] Check Point, 2017 Global Cyber Attack Trends Report

[5] Cyxtera, How to Overcome NAC Limitations.

[6] Musa Abubakar Muhammad, Aladdin Ayesh, Pooneh Bagheri Zadeh,(2017). Developing an Intelligent Filtering Technique for Bring Your Own Device Network Access Control, the International Conference on Future Networks and Distributed System, No. 46. DOI : 10.1145/3102304.3105573.

[7] Choi Eun-bok, Lee Sang-joon (2016). MAC Policy-based Access Control Mechanism for Cloud Convergence, Journal 7 of the Korean Convergence Society, 1-8.

[8] Jung Yoon-soo, Han Gun-hee (2018). Effective access control techniques between different IoT devices in the cloud environment, Journal 9 of the[Korean Convergence Society, No. 4, 57-63.

[9] Kang Yong-hyuk, Kim Moon-jung, Han Moon-seok (2017), a study on the intrusion detection technique using software-defined networking techniques in wireless sensor networks, Journal 8 of the Korean Convergence Society, 51-57.

[10] Jung Sung-jae, Bae Yu-mi, (2013). Analysis of cloud security threats and technology trends, Journal of Security Engineering Research, No. 10, No. 2, 199-212

[11] Kim Chang-soo, Jang Bong-im, Chung Hoi-kyung (2013). Analysis of cloud security threats and technology trends, Journal of Security Engineering Research, No. 10, No. 2, 199-212.

[12] Ashish Singh & Kakali Chatterjee. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115. DOI : 10.1016/j.jnca.2016.11.027.

[13] Miss. Shakeeba S & Khan, Miss. Sakshi S. Deshmukh. (2017). Security in Cloud Computing Using Cryptographic Algorithms. Journal of Computer Science and Mobile Computing, 3, 517-525.

[14] SalmanIqbal. Miss Laiha Mat Kiah. Babak Dhaghighi. Muzammil Hussain. Suleman Khan. Muhammad Khurram Khan. Kim-Kwang Raymond Choo. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. Journal of Network and Computer Applications, 74, 98-120. DOI : 10.1016/j.jnca.2016.08.016.

[15] Won-Bon Koo, Kab-Seung Kou, Jae-In Shin, Jae-goo Jeong&Young-Gi Min. (2013). A Study on Information Security Requirements Considering the Security Technical Aspects in Cloud Service. Journal of Security Engineering, 10(3), 355-370.

차 욱 재(Cha, Wuk Jae) [정회원]

- 2005년 2월 : 서울산업대학교 컴퓨터 공학 학사
- 2011년 2월 : 성균관대학교 전자전기컴퓨터 공학 석사
- 2015년 3월 : 성균관대학교 전자전기컴퓨터공학 박사과정
- 2010년 2월 ~ 현재 : 지니언스(주)
- 2010년 2월 ~ 현재 : 한국 WG3 정보보안전문가 활동
- 관심분야 : 네트워크 보안, 암호이론, 표준화, CC, 정보보호
- E-Mail : wjcha@genians.com

신 재 인(Shin, Jae In) [정회원]

- 2009년 2월 : 한남대학교 컴퓨터공학 학사
- 2011년 8월 : 한남대학교 대학원 컴퓨터 공학 석사
- 2013년 1월 : 한국시스템보증(주)
- 2018년 9월 ~ 현재 : 지니언스(주)
- 관심분야 : 네트워크 보안, 클라우드 보안, 정보보호
- E-Mail : shinjaein@genians.com

이 동 범(Lee, Dong Bum) [정회원]

- 1995년 2월 : 성균관대학교 정보공학 학사
- 1995년 3월 : 두산정보통신(주)
- 1998년 1월 : (주)어울림정보기술
- 2005년 1월 ~ 현재 : 지니언스(주) 대표이사
- 2016년 6월 ~ 현재 : K-securitry Startup Forum 공동의장
- 2017년 2월 ~ 현재 : 정보보호산업협회(KISIA) 수석부회장
- 관심분야 : 네트워크 보안, 클라우드 보안, 정보보호
- E-Mail : dblee@genians.com

김 협(Kim, Hyeob) [정회원]

- 2010년 2월 : 연세대학교 문헌정보학 학사
- 2014년 2월 : 연세대학교 정보대학원 정보시스템학 석사
- 2018년 8월 : 연세대학교 정보대학원 정보시스템학 박사
- 2014년 3월 ~ 현재 : 지니언스(주)
- 관심분야 : 네트워크 보안, 클라우드 보안, 지식서비스 보안, 블록체인, 정보보호
- E-Mail : hyubiii@genians.com

이 대 효(Lee, Dea Hyo) [정회원]

- 2000년 2월 : 안양대학교 컴퓨터공학 학사
- 2009년 2월 : 성균관대학교 대학원 이동통신공학 석사
- 2012년 2월 : KAIST 대학원 경영학(MBA) 석사
- 1998년 8월 : ㈜어울림정보기술
- 2005년 3월 : ㈜안랩
- 2009년 3월 ~ 현재 : 지니언스(주) 연구기획실 실장
- 관심분야 : 단말 보안, 네트워크 보안, 클라우드 보안
- E-Mail : dado@genians.com