https://doi.org/10.5392/JKCA.2019.19.12.407

소프트웨어 정의 경계의 단일 패킷 인증 및 네트워크 접근통제 보안관리 개선

Improved Single Packet Authentication and Network Access Control Security Management in Software Defined Perimeter

정진교*, 이상구**, 김용민*
전남대학교 정보보안협동과정대학원*, ㈜안랩**

Jin-kyo Jung(jinkyo@gmail.com)*, Sang-ku Lee(kkamanstar@gmail.com)**,
Young-Min Kim(ymkim@chonnam.ac.kr)*

요약

클라우드 컴퓨팅, 스마트워크 등으로 IT 환경 변화가 진행됨에 따라 기존의 경계 보안 모델이 한계를 보이고 있으며, 소프트웨어 정의 경계(Software Defined Perimeter)가 그 대안으로 논의되고 있다. 하지만, SDP Spec 1.0에서는 장치등록 절차와 정책 배포 과정 및 인증 키의 생성과 공유 과정이 명시되어 있지 않다. 이에 본 논문에서는 단일패킷인증(Single Packet Authentication)의 동작 절차를 개선하여 기존의 SDP 접근통제의 문제점을 보완하는 방법을 제안한다. 개선된 제안 방법을 통하여 기존 접근통제 방법에 비하여 일관되고 자동화된 통합 접근 통제 정책을 구현할 수 있음을 보이고자 한다.

■ 중심어 : | 제로트러스트 | SDP | SPA | 접근통제 | 접근정책관리 |

Abstract

As the IT environment changes with cloud computing and smart work, the existing perimeter security model is showing its limitations and Software Defined Perimeter is being discussed as an alternative. However, SDP Spec 1.0 does not specify the device registration procedure, policy distribution process and authentication key generation and sharing process.In this paper, we propose a method to solve the problem of SDP access control by improving the operation procedure of Single Packet Authentication. This paper suggests that the proposed method can implement a consistent and automated integrated access control policy compared to the existing access control methods.

■ keyword : | Zero-Trust | SDP | SPA | Access Control | Access Policy Management |

I. 서 론

최근 클라우드 및 스마트워크 등 새로운 기술의 적용이 확산됨에 따라 새로운 형태의 보안과 개인정보보호 문제가 대두되고 있다. 보안을 위한 망 분리 및 하이브리드 클라우드의 도입 등으로 인하여 네트워크 구성은 더욱 복잡해지고 있으며 이로 인해 보안 관리의 난이도가 증가하고 있다. 그동안 업계 보안 표준으로 알려진 경계보안모델은 변화된 네트워크 환경에 대한 적용과 경계 보안을 위한 다수의 보안 장비의 통합 및 관리의 어려움이 존재한다. 보안 담당자들은 방화벽 정책의 복잡성, 이기종 장비 관리, 정책 변경 등에 대한 어려움을

접수일자 : 2019년 11월 13일
수정일자 : 2019년 11월 25일
심사완료일 : 2019년 11월 25일
교신저자 : 이상구, e-mail : kkamanstar@gmail.com

호소하고 있다. 이러한 문제에 대응하기 위해서 소프트웨어 정의 경계(Software Defined Perimeter)가 새로운 보안 프레임워크로 제안되고 있다[1].

본 논문에서는 스마트워크, 클라우드 확산 등 변화하는 기업의 IT 환경에서 보안성과 편의성을 제공할 수 있는 SDP의 개선된 네트워크 접근통제 방법을 제안하는 것을 목표로 한다. 이를 위하여 CSA(Cloud Security Alliance)에서 발표한 SDP Spec 1.0의 구성요소와 동작 원리를 분석하여 장치의 등록 방법을 보완하고, 장치인증 단계의 핵심 기술인 단일 패킷 인증(Single Packet Authorization, 이하 SDP)방법에 있어서의 키의 생성 및 공유방법과 동적 방화벽 기술[2]을 활용하여 기존 접근통제 방식의 문제점을 개선하기 위한 방법을 제안한다. 주요기업의 해킹사례에 제안하는 방법과 기존 연구의 비교를 통하여 보안 안정성 및 정책관리 효율성에서 효과가 있음을 보이고자 한다.

본 논문 II장에서는 주요 해킹사례와 클라우드 환경에서의 접근통제 문제점을 보이고, SDP의 개요와 문제점에 대해 설명한다. III장에서는 개선된 SDP 접근통제 방법을 제안하고, 접근 통제 관리업무의 효율성과 보안 안전성을 분석한다. 마지막으로 IV장에서 결론과 향후 연구에 대하여 제시한다.

II. 관련 연구

본 연구에서는 현행 접근통제 관련 기술과 연구 사례 및 한계를 분석하고, 클라우드 및 기업 내부 주요 인프라에 대한 접근통제 기술로 최근 많은 관심을 받고 있는 SDP 구성요소와 동작 원리, 특징 등을 살펴본다.

1. 기업 네트워크 접근통제 취약성 사례

KISA는 2017년 주요 기업의 해킹사례로 3건의 분석 결과를 제시했다[3]. 그 중 2개의 사례가 접근통제 취약점과 연관이 되어 있는데, 두 가지 모두 기업 내부망에 침투한 후 추가적인 공격대상을 식별하고 침해를 확산한 사례로 내부 망에서의 접근통제 취약성의 대표적인 사례로 볼 수 있다.

클라우드의 경우에도 맥아피가 발표한 클라우드 활용과 위협 보고서(Cloud Adoption and Risk Report)[4]에 따르면 클라우드 도입 기업 가운데 80%는 한 달에 한 번 이상 계정탈취 공격 받은 것으로 나타났다. 취약 계정, 권한 있는 사용자, 내부자 위협 등 클라우드 보안위협은 전년 대비 27.7% 증가했고, 이들 공격은 주로 클라우드에 저장된 고객 데이터, 패스워드, 카드사용 내역 등 탈취를 노렸다[4].

2. 기업 네트워크를 위한 주요 접근통제 기술

2.1 기존 네트워크 접근통제 기술과 한계

새로운 IT 기술이 적용됨에 따라 NAC, 방화벽, VPN 등 오랜 기간 활용된 네트워크 접근통제 방식이 한계점을 노출하고 있다.

첫 번째로 NAC(Network Access Control) 인증 후 네트워크의 접속을 강제함으로써 보안성을 높일 수 있지만[16], 기업 외부에서의 접근 요구가 증가하는 최근의 기업 환경에서는 효과성이 떨어지고 있고, 특히 클라우드 환경에는 NAC 기술이 불가하다.

두 번째로 네트워크 방화벽의 경우 네트워크 접점 증가, 망 구성의 복잡성 증가, 이기종 장비의 증가 등으로 인한 통합 정책 관리의 난해함으로 사용자 접근정책 관리에 큰 어려움을 겪고 있다[5]. 또한 사용 장치의 증가 및 모바일 요구는 기존 IP, Port 기반 접근 정책의 어려움을 증폭시키고 있다.

마지막으로 VPN의 경우 외부에서 내부망에 접속 시 활용되고 있으나, 외부에 VPN 서버가 노출될 수밖에 없고 사용자의 인증 정보(아이디/패스워드)가 노출되면 외부 해커의 접속을 위한 경유지로 활용될 수 있는 위험성을 가지고 있다.

2.2 클라우드 서비스의 접근통제 방식

기업 내부의 데이터센터가 클라우드로 이전함에 따라 가상 네트워크 및 컴퓨팅 인스턴스들을 보호하기 위하여 클라우드 플랫폼 사업자가 제공하는 ACL, Security Group, VPN, 상호인증 기술 등을 사용한 접근통제 방식을 활용되고 있다[6][17].

하지만, 클라우드 사업자가 제공하는 보안 서비스도 대부분 IP 주소 및 서비스 포트 기반의 접근통제 방식을 활용하고 있어, 앞서 언급했던 기존 네트워크 접근

통제의 문제점과 한계를 그대로 가지고 있다[6]. 특히, 기업 내부 사용자만 접속을 허용하면서, 사용자의 위치가 동적으로 변경되는 모바일을 통해 접속하는 경우 접근 정책은 매우 난해해 진다.

3. 제로트러스트와 소프트웨어 정의 경계

제로트러스트 보안 모델은 IT 시장 조사 기관인 포레스터 리서치의 보고서에서 2010년 처음 언급되었다[7]. 2000년대 수많은 보안 사고와 보안 비효율성의 근본 원인을 경계부 보안 모델이 신뢰구간과 비신뢰 구간으로 나누고 네트워크에 임의의 권한을 암묵적으로 부여하였기 때문이라고 진단하였다.

이에 대한 해법으로 제로트러스트 보안 모델 다음 세 가지의 방법을 제안했다. 첫째, 모든 자원 접근에 대한 검증 및 보호. 둘째, 최소 권한 부여 전략의 적용 및 엄격한 접근통제 정책. 셋째, 모든 트래픽에 대한 모니터링과 로깅을 실시하는 것이다.

3.1 SDP 개요 및 구성 요소

이러한 개념에 따라 Cloud Security Alliance는 소프트웨어 정의 경계(Software Defined Perimeter, SDP) Spec 1.0[8]을 발표하였다.

SDP는 다음의 네가지 목적으로 설계 되었다.

- 서비스를 네트워크로 부터 격리
- 어플리케이션 오너에게 논리적 접근 통제 권한 제공
- 장치 및 사용자에 대한 신원 확인 후 네트워크 접근
- 모든 트래픽의 암호화

표 1. SDP 구성요소

구성요소	역할
SDP Controller (SC)	- SDP 호스트 간의 통신 여부 결정 - 다양한 데이터 참조를 통한 의사결정 수립
Initiating SDP Host (IH)	- 통신을 요청하는 호스트 - Controller에게 통신 가능한 AH 목록을 요청
Accepting SDP Host (AH)	- 서비스를 제공하는 호스트 - Controller의 지시에 따라 IH의 요청을 수락

SDP는 [표 1]과 같이 SDP 클라이언트, SDP 컨트롤러, SDP 게이트웨이로 구성된다.

SDP의 구성 요소간 동작 흐름은 [그림 1]과 같은데, SDP 워크플로우[9]는 기존의 네트워크 접근 통제 방법과 완전히 다른 방식을 취하고 있다. CSA의 SDP Spec 1.0을 기준으로 세부적인 워크플로우 절차는 [그림 1]과 같이 7단계로 진행된다. SDP는 장치의 인증을 수행 후에 자원에 대한 네트워크 연결을 허용함으로써 공격자에게 네트워크의 공격 대상을 감춘다는 점에서 기존의 보안 방법과 근본적인 차이를 보이고 있다[10][15].

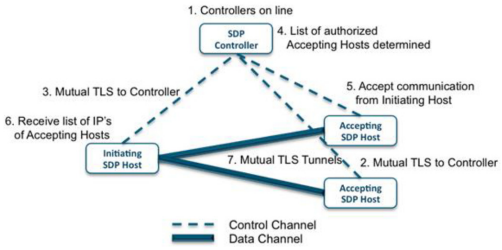

그림 1. SDP 동작 흐름

3.2 SPA 접근통제 기술

단일 패킷 인증(SPA, Single Packet Authorization)은 SDP의 중요한 핵심 기술 중 하나로 장치에 대한 인증 기능을 제공한다. IH, AH, 컨트롤러 간의 모든 통신은 먼저 인증 단계를 거치게 되는데, SDP의 인증은 SPA 방식을 사용하여 수행된다[8][9][11].

SPA 프로토콜은 RFC 4226에 정의된 HOTP (HMAC-Based One-Time Password Algorithm) 프로토콜을 기반으로 한다. SPA에서 통신 당사자는 비밀 시드를 공유하게 되는데, 비밀 시드는 카운터와 함께 일회용 암호(OTP)를 만드는 데 사용된다. 접속을 원하는 SPA 클라이언트는 SPA 서버와 통신하기를 필요할 때마다 카운터, OTP을 패킷에 포함하여 단일 패킷으로 전송한다[10]. SPA 서버는 전송된 OTP를 검증하고 성공적이면 응답한다. SDP에서도 SPA 패킷의 동작 원리는 앞서와 동일하며, SPA 패킷은 클라이언트에서 컨트롤러 또는 AH로 전송되는데 패킷 포맷은 [그림 2]와 같다[11].

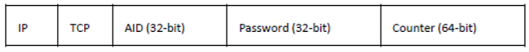

그림 2. SPA 패킷 포맷

SPA는 SDP 아키텍처에 다음과 같은 이점을 제공한

다[8][9].

- 컨트롤러나 AH는 유효한 SPA 패킷을 수신하는 경우를 제외하고 모든 연결 시도에 응답하지 않기 때문에 서버 스캐닝, 비인가 접근 등으로부터 안전하다.
- 유효하지 않은 패킷은 기본차단 되므로 DoS 공격을 완화하는 데 도움이 된다.
- SPA 패킷으로 시작하지 않는 연결 시도는 비정상 접근이라 판단하여 보안 위협 탐지에 도움이 된다.

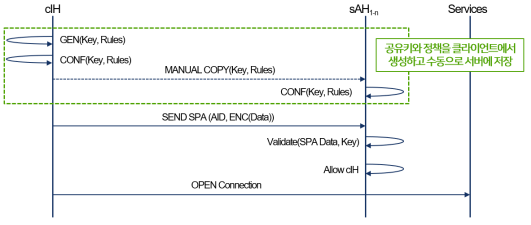

그림 3. SPA 프로토콜의 동작 방식과 문제점

하지만, SPA 프로토콜을 기반으로 한 fwknop 프로젝트[12]의 경우 [그림 3]과 같이 SPA 패킷 암호화 및 검증에 활용하는 키를 SPA 클라이언트(cIH)에서 생성하도록 되어 있고, 해당 키와 서비스 접근 정책을 SPA 서버(sAH)의 접근통제 설정에 수작업으로 저장하는 방식으로 되어 있어, 키 생성 및 공유와 접근정책 통합 관리 측면에서 문제점을 가지고 있다[13]. 이로 인해 기존 SPA를 활용한 접근통제 기술은 기업 환경에서 활용하기에는 적합하지 않다고 볼 수 있다.

[표 2]는 SPA의 문제점을 분석[14]한 것으로 SDP를 기업 환경에 적용하기 위해서는 핵심 기술인 SPA의 문제점을 해결하여야 한다.

표 2. SPA 접근통제 방식의 문제점

구분	특징	문제점
구조 관점	동적 정책 생성 시 Timeout 반영	통신이 단절될 수 있음
적용 관점	AH / AH 그룹 상단 게이트웨이에 적용	게이트웨이만 적용 시 내부의 East-West 구간 위협 노출
관리 관점	클라이언트에서 접근 정책 생성	정책을 클라이언트에서 생성, 신뢰성 문제 발생 가능

Ⅲ. SDP 기반의 접근통제 보안관리

1. 개선된 SDP 기반 접근통제 방법

기존의 SDP Spec 1.0의 절차는 다음과 같다.

- SDP 컨트롤러에 SDP 게이트웨이 등록
- AH(서버)의 어플리케이션 정보 등록 후 온보딩(On-Boarding) 상태 전환
- SPA 인증을 통해 장치 인증 수행
- 필요시 사용자 인증 진행
- 접근하고자 하는 SDP 게이트웨이와 상호인증 후 접근경로 오픈.

여기에서의 문제점은 관련연구에서 언급한 바와 같이 장치 등록을 하는 사전 등록 절차와, 인증 후 실제 정책이 어떻게 관리되고 배포되는지가 분명하게 설명되어 있지 않다는 점이다. 또한, [그림 4]와 같이 기존 SPA의 문제점으로 언급했던 SPA 패킷 암호화 및 인증을 위해 사용되는 키를 누가 어떤 절차를 통해 생성하는지와 SDP 클라이언트(cIH)와 SDP 컨트롤러(sCTL)가 어떤 방식으로 최초 공유하는지도 세부적으로 정의 및 명시되어 있지 않다.

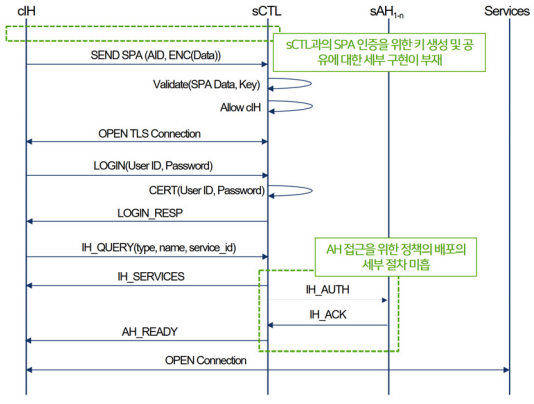

그림 4. SDP 오픈 프로젝트의 동작방식과 문제점

제안하는 접근통제 방법은 사용자의 접근 위치에 상관없이 대상 서비스 접근을 위한 장치(클라이언트)를 사전에 등록하고, 접근 시 장치와 사용자 인증을 거친 후, 사용자 역할 및 요청에 맞는 접근 정책을 각 게이트웨이에 동적으로 배포하고, 접근 기록을 로깅하고 모니터링 함으로써 일관되고 자동화된 통합 접근제어 정책을 관리하기 위한 방법이다.

[그림 5]은 전체 구성 및 흐름을 요약한 그림이다. 제

안하는 방법의 전체적인 절차에 대한 기본 설명은 다음과 같다.

- 장치 등록 요청: 서비스에 접속하려는 장치의 속성 정보(PC명, MAC, OS 등)를 추출하여 컨트롤러 서버에 등록 요청(등록 시 1회)
- 장치 등록/사용자 매핑: 사용자 인증 후 장치를 등록, 사용자 매핑 후 컨트롤러 서버 정보를 장치에 배포(등록 시 1회)
- 접근 프로파일 요청: SPA인증 후 접근 가능한 대상 서비스의 프로파일을 요청
- 접근 프로파일 배포: 사용자 역할에 따라 사전 생성되어 있는 프로파일을 사용자 장치에 배포
- 대상 서비스 접근 요청: SPA인증 후 대상 서비스에 대한 접근을 요청하고 사용자에게 접근 게이트웨이 정보를 제공

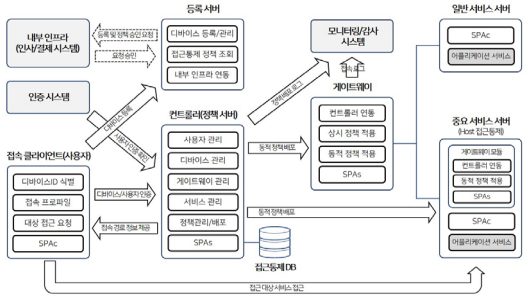

그림 5. SDP를 활용한 네트워크 접근통제 흐름

세부적인 방안으로 먼저 장치 등록 과정을 시스템화하기 위하여 [그림 6]과 같이 전체 구성요소에 장치 등록(REG) 서버를 추가하고, 등록 서버와 cIH 및 sCTL 사이의 역할 및 동작 절차를 개선하였다.

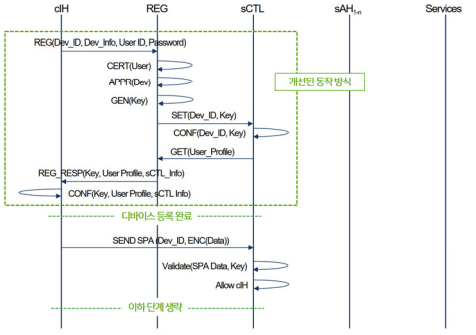

그림 6. 장치 등록 시스템화 및 동작방식 개선

- cIH와 REG 사이의 장치를 등록하는 절차 추가
- cIH와 sCTL 사이의 SPA 인증을 위한 키 생성을 기존 cIH가 생성하는 방식에서 REG 서버가 자동 생성하고 cIH와 sCTL에 공유하는 방식으로 변경
- 기업 내의 승인 워크플로우 적용을 위하여 승인 절차를 추가
- 장치 등록이 승인된 이후에만 사전에 정의된 사용자 프로파일과 sCTL 정보가 cIH에 전달되도록 하여 장치 등록이 안 된 경우 불필요하게 정보가 노출되지 않도록 개선

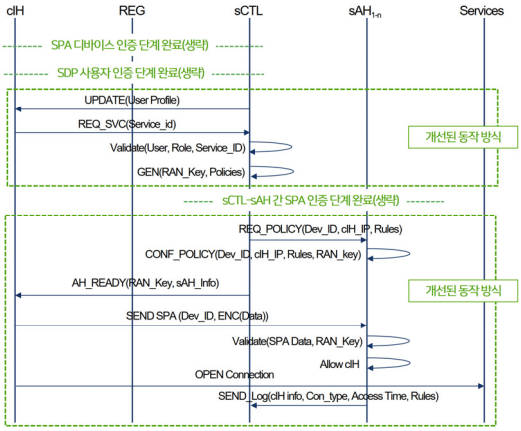

그림 7. 접근정책 통합관리 및 동작방식 개선

그리고, 통합 정책관리를 위하여 [그림 7]과 같이 sCTL와 sAH 간의 정책 적용을 요청, 배포하는 동작 절차를 구체화 하였다. 참고로, sAH가 sCRL에 등록하는 과정은 생략하였으며, 정책을 요청하고 관리하는 프로세스는 기존 기업의 워크플로우를 활용하는 것으로 가정하였다.

- cIH와 sCTL간의 SPA 장치 및 SDP 사용자 인증이 완료된 후에 사용자 프로파일을 자동으로 업데이트 하도록 개선
- cIH에서 Services 접근 시 sAH와의 인증을 위한 임시 키를 랜덤하게 생성 후 cIH와 sAH에게 자동 공유하는 방식을 추가
- Services 접근에 필요한 정책이 사용자 역할 기반으로 다수의 sAH1-n에 자동 배포되는 방식으로 변경
- 모니터링 및 감사를 위하여 모든 접근 요청 및 접속

이력을 로깅 할 수 있는 동작 절차 추가

[표 3]은 [그림 6]과 [그림 7]에서 사용하는 용어에 대한 설명을 나타낸 것이다.

표 3. 장치 등록 및 접근정책 통합관리의 동작방식 용어

용어	설명
UPDATE(User Profile)	SPA장치 인증 및 사용자 인증 후에 사용자의 최신 프로파일을 갱신
REQ_SVC(Service_id)	프로파일에 정의 된 서비스 접근 요청
Validate(User, Role, Service_ID)	요청된 서비스 아이디가 사용자의 역할에 적합한지 검증
GEN(RAN_Key, Policies)	AH로 접근 요청을 위한 임시 키(RAN_key) 생성
REQ_POLICY(Dev_ID, cIH_IP, Rules)	cIH의 장치 아이디 정보, IP, 접근 정책을 sAH에 요청
CONF(Dev_ID, cIH_IP, Rules, RAN_Key)	sCTL로부터 전달받은 정보를 기반으로 SPA 인증을 위한 설정 저장
AH_READY(RAN_Key, sAH_Info)	AH 접근을 위한 임시 키와 접근을 위한 네트워크 정보 전달
SEND_Log	접근을 요청한 사용자, 접근정책, 접근 일시 등 모니터링을 위한 로그 저장

개선된 방식을 통해 앞서 언급한 SPA의 인증 키 관리 문제와 IH(클라이언트)수, Host의 수, 개별 정책 수가 증가 될 때마다 접근 정책이 급격하게 증가하는 문제를 해결함으로써, 컨트롤러(통합 정책 관리)에서 전체 정책을 통합 관리하게 하고, 필요한 경우 AH에 자동 배포할 수 있게 하였다.

2. 제안 방법의 관리업무 개선 효과 분석

기존 방화벽 접근통제 방식의 절차는 [그림 8]와 같이 사용자가 장치의 출발지(Source) IP를 기준으로 목적지(Destination)의 IP 및 포트에 대한 정책을 요청하고, 보안담당자는 해당 정책을 검증 후 방화벽에 정책을 적용한다. 이 후 사용자는 접속 하고자 하는 대상 서비스 또는 서버에 접근하여 개별적인 사용자 인증 과정을 거친 후 필요한 업무를 수행하게 된다. 또한 대부분의 기업은 한번 적용된 정책은 별도의 만료일이 없는 한 그대로 유지가 되어 정책의 숫자가 늘어나는 경향을 보인다.

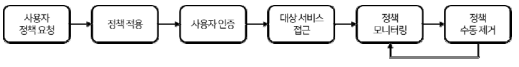

그림 8. 기존 방화벽 접근통제 절차

또한, 일반적으로 사용자 장치의 IP로 사용자를 식별하고 있어 사용자의 신규 장치 추가, 업무가 변경, 동일 역할의 신규 사용자가 추가 등의 정책 변경이 필요한 경우에는 앞서의 절차를 반복적으로 진행하기 위한 관리 비용이 증가한다.

VPN 의 경우에도 접근 IP에 대한 통제 대신 아이디/패스워드 기반의 사용자 인증 부분만 상이하고 방화벽과 유사한 절차로 진행 하는데, 사용자 역할에 따른 대상 서비스 접근 정책은 기존 방화벽 신청 절차와 마찬가지여서, 신규 또는 변경사항이 발생할 때마다 역시 많은 수작업을 진행해야 한다.

반면 본 논문에서 제안한 접근통제 방식의 경우에는 [그림 9]과 같은 절차로 진행되게 된다. 내부의 대상 서비스에 접근하기 위해서 사용자의 장치를 등록 서버를 통해 등록하는 과정을 거친다.

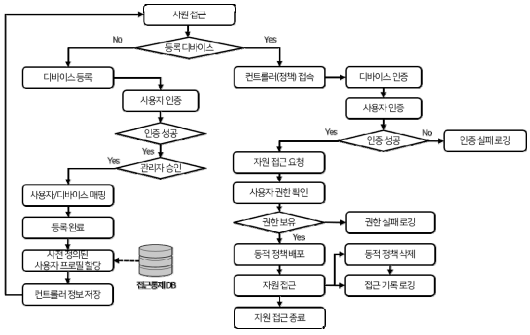

그림 9. 통합 정책관리 기반의 개선된 접근통제 절차

이 때 사용자 인증 과정을 통해 장치 사용자를 특정(매핑)하게 된다. 이후 사전에 정의된 사용자의 역할에 따라 접근 프로파일을 장치의 에이전트에 전송/저장하고, 서비스 접근 시도 시 해당 업무 목적에 맞는 프로파일을 선택하여 접근을 요청하게 된다. 서비스 접근 요청을 받게 되면 장치 등록 여부, 적법한 사용자 여부를 인증 과정을 통해 확인하고, 정상으로 확인된 경우에는 각 게이트웨이 또는 서버에 정책을 배포하여 사용자가 대상 서비스에 접속할 수 있게 한다. 만약, 사용자의 장치가 추가되거나 변경이 되더라도 정책을 변경하는 것이 아니라 장치 정보만 신규 등록 또는 변경하면 되기 때문에 관리자가 별도로 작업을 해야 하는 부담을 줄일 수 있다.

더불어, 접근 위치에 따른 적절한 게이트웨이 경로만 사용자에게 전달하고, 해당 게이트웨이에 정책만 배포하기 때문에 VPN이나 방화벽 정책을 따로 관리하지 않고 통합하여 정책을 관리할 수 있는 편의성을 제공한다.

3. 제안 방법의 보안 안정성 분석

앞서 설명한 제안하는 접근통제 방식을 적용하여 앞서 II. 관련연구에서 언급한 기업의 주요 침해사고 사례를 방어할 수 있다. 제안한 방법은 SDP의 보안 특징을 상속하므로 포트스캐닝, DDoS 공격, 스니핑 공격, 중간자 공격, 무차별 대입 공격, 제로데이 공격 및 탈치된 계정 정보의 활용 한 비인가 접근에 대해 효과적인 대응을 할 수 있다.

내부 사용자의 PC에 악성코드에 감염되었을 경우에도 사용자 인증 없이 어떠한 대상 서비스로 접근이 되지 않으며, 설사 인증 후 허용된 서비스도 허용된 짧은 시간 이후에는 접근이 다시 차단되기 때문에 추가적인 공격이 어렵다. 단, 인증된 사용자의 장치가 장악된 상태에서 사용자 계정 정보도 탈취된 경우에는 비인가자의 접근이 성공할 수 있는 위험이 존재한다.

표 4. 기존 기술, 관련 연구, 제안 방식에 대한 비교

구분	방화벽	VPN	SDP 1.0	제안 방식
네트워크 포트 스캐닝	X	△	O	O
서비스 거부 공격	X	△	O	O
스니핑 공격	N/A	O	O	O
중간자 공격	N/A	O	O	O
무차별 대입 공격	X	N/A	O	O
취약 서버 공격 (Zero-day Attack)	X	X (내부망)	O	O
탈취된 계정 정보를 활용한 비인가 접근	X	O	O	O
관리자 PC 장악 후 우회 비인가 접근	X	X	△	△
설정 오류로 인한 비인가 접근 허용	X	X	N/D	O
통합 정책 관리 (On-Premise, Cloud)	X	X	N/D	O
접근 이력 로깅/감사	△ (IP)	O (IP,USER)	N/D	O

SPA를 이용한 장치 인증 및 사용자 인증 후 정책이 배포되고, 실제 접근이 이루어졌는지가 기록되어 언제(When), 어디서(접속IP), 어디로(Where) 등의 활동로그를 추적할 수 있다. 반대로, 인증되지 않은 장치에서 컨트롤러 서버로 패킷이 전송되면 공격자로 인식하여 공격 대상 스캐닝 시도 시부터 탐지가 가능하다.

[표 4]는 보안 안정성 요소 기준에 운영 및 침해사고 대응을 위해 요구되는 기능을 추가하여, II. 관련연구에서 언급한 기존 접근통제 방식 및 연구 사례를 제안하는 방식과 세부적으로 비교하여 나타낸 표이다.

비교 분석 결과 제안한 접근통제 방법은 VPN과 방화벽을 동시에 사용한 경우보다도 더욱 높은 수준의 보안성을 제공할 수 있음을 알 수 있다. 또한, 통합관리 및 추적성 관점에서는 기존 SDP 방법보다 개선되었기 때문에 침해사고 대응 및 예방에 보다 효율적인 모습을 보여주고 있다.

Ⅳ. 결론 및 향후 연구

디지털 변혁의 시대는 IT 기술 및 환경 변화에 맞추어 보안 리스크를 감소시키면서도 업무 혁신을 장려하고 생산성을 높일 수 있는 대책이 필요하다. 특히, 수작업 비중이 높은 네트워크 접근정책 변경 작업을 중앙에서 통합 관리하고 자동화를 통한 보안 위협과 보안 담당자의 업무 부담을 최소화할 수 있는 개선된 접근통제 방법이 필요하다. 이를 위하여 본 논문에서는 SDP의 핵심 기술인 SPA의 정책관리 방식의 문제점과 SDP Spec 1.0의 세부 동작 방식 및 절차를 개선함으로써 기업 환경에 적용 가능한 통합 정책 관리 방법을 제시하였다.

이를 통해 등록된 장치에서 사용자 인증 후 접근을 원하는 대상 서비스로의 정책이 서비스 상단의 게이트웨이나 개별 서버에 동적으로 반영되게 함으로써 사용자의 역할에 따라 필요할 때 접근을 허용하고 사용 목적이 완료된 경우에는 자동으로 정책을 삭제하도록 하였다. 제안하는 기법을 통해 해커가 대상 서비스로 공격할 수 있는 접점을 줄일 수 있으며, 기업에서 발생되는 주요한 침해사고 사례에서 관련 연구나 기존 접근통제 방식보다 높은 보안성을 제공할 수 있음을 확인하였다. 또한, 네트워크 접근정책 관리가 통합되어 정책 예외나 정책 변경 등 정책관리 작업의 업무 부담을 크게

낮출 수 있을 것으로 예상된다. 특히, 제 4차 산업혁명을 이끄는 여러 기술 중 클라우드 컴퓨팅의 확산을 저해하는 요소로 보안 문제가 대두되고 있는데, 제안하는 방법은 기존 네트워크 환경 뿐만 아니라 클라우드 환경을 포함하는 네트워크 접근통제를 제공하여 그 유용성이 더욱 크다고 할 수 있다.

다만, 본 연구에서는 사용자의 역할을 기준으로 접근 프로파일을 제공하는 역할기반접근통제(RBAC)을 기준 모델로 삼았다. 최근의 기업 사업 환경과 외부 위협은 더욱 복잡해지고 동적인 성격을 띄고 있어, 정적인 접근통제 모델 보다는 실시간으로 위험도를 측정하고, 운영필요성을 판단하여 접근 결정을 내리는 동적 접근 통제 모델을 SDP 환경에 적용하기 위한 추가적인 연구가 필요하다.

참 고 문 헌

[1] Abdallah Moubayed, Ahned Refaey, and Abdallah Shami, "Software Defined Perimeter : State of the Art Secure Solution for Modern Networks," IEEE Network, Vol.33, Issue 5, pp.226-233, 2009.

[2] https://www.linuxjournal.com/article/9565

[3] https://www.zdnet.co.kr/view/?no=20180528103548

[4] McAfee, *Cloud Adoption and Risk Report*, McAfee, 2019.

[5] Firemon, *State of the Firewall*, Firemon, 2018.

[6] Jason Garbis and Puneet Thapliyal, *Software Defined Perimeter for Infrastructure as a Service*, Cloud Security Alliance, 2016.

[7] John Kindervag, *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*, Forrester Research, 2010.

[8] Brent Bilger, Alan Boehme, Bob Folres, Zvi Guterman, Mark Hoover, Michaela Iorga, Junaid Islam, Marc Kolenko, Juanita Koilpilla, Gabor Lengyel, Gram Ludlow, Ted Schroeder, and Jeff Schweitzer, *SDP Specification 1.0*, CSA, 2014.

[9] Jason Garbis and Juanita Koilpollai, *Software Defined Perimeter Architecture Guide*, CSA, 2019.

[10] 정진교, 김용민, "제로트러스트 보안모델과 접근통제 적용 연구," 정보보호학회 하계학술대회 논문집, Vol.29, No.1, 2019.

[11] Fotios-Dimitrios Tsokos, *Development of a Software Defined Security Perimeter*, University of the Thessaly, 2018.

[12] http://www.cipherdyne.org/fwknop

[13] 이상구, 정진교, 김용민, "SDP 단일 패킷 인증의 접근통제 개선 방안," 한국콘텐츠학회 종합학술대회 논문집, pp.311-312, 2019.

[14] 이상구, 김용민, *단일 패킷 인증 프로토콜을 이용한 네트워크 접근통제 방법*, 전남대학교, 석사학위논문, 2019.

[15] D. Puthal, S. P. Mohanty, P. Nanda, and U. Choppali, "Building Security Perimeters to protect network systems against cyber threats," IEEE Consumer Electronics Magazine, Vol.6, Issue 4, pp.24-27, 2017.

[16] 강남길, 권태욱, "SDN 환경에서 비인가 소프트웨어 차단 기법," 한국정보보호학회논문지, 제29권, 제2호, pp.393-399, 2019.

[17] 최상용, 정기문, "안전한 클라우드 컴퓨팅 환경을 위한 보안 아키텍처," 한국컴퓨터정보학회논문지, 제23권, 제12호, pp.81-87, 2018.

저 자 소 개

정 진 교(Jin-kyo Jung) 정회원

- 2016년 8월 : 전남대학교 정보보안협동과정(이학석사)
- 2016년 9월 ~ 현재 : 전남대학교 정보보안협동과정

〈관심분야〉 : 접근통제, SDP

이 상 구(Sang-Ku Lee) **정회원**

■ 2019년 8월 : 전남대학교 정보보안협동과정(이학석사)
■ 2003년 3월 ~ 현재 : ㈜안랩

〈관심분야〉 : SDP, 클라우드

김 용 민(Young-Min Kim) **정회원**

■ 2002년 8월 : 전남대학교 전산통계학과 박사
■ 2006년 ~ 현재 : 전남대학교 문화콘텐츠학부 전자상거래전공 / 정보보안협동과정 교수

〈관심분야〉 : 시스템 및 네트워크 보안, 전자상거래 보안, 융합보안 등