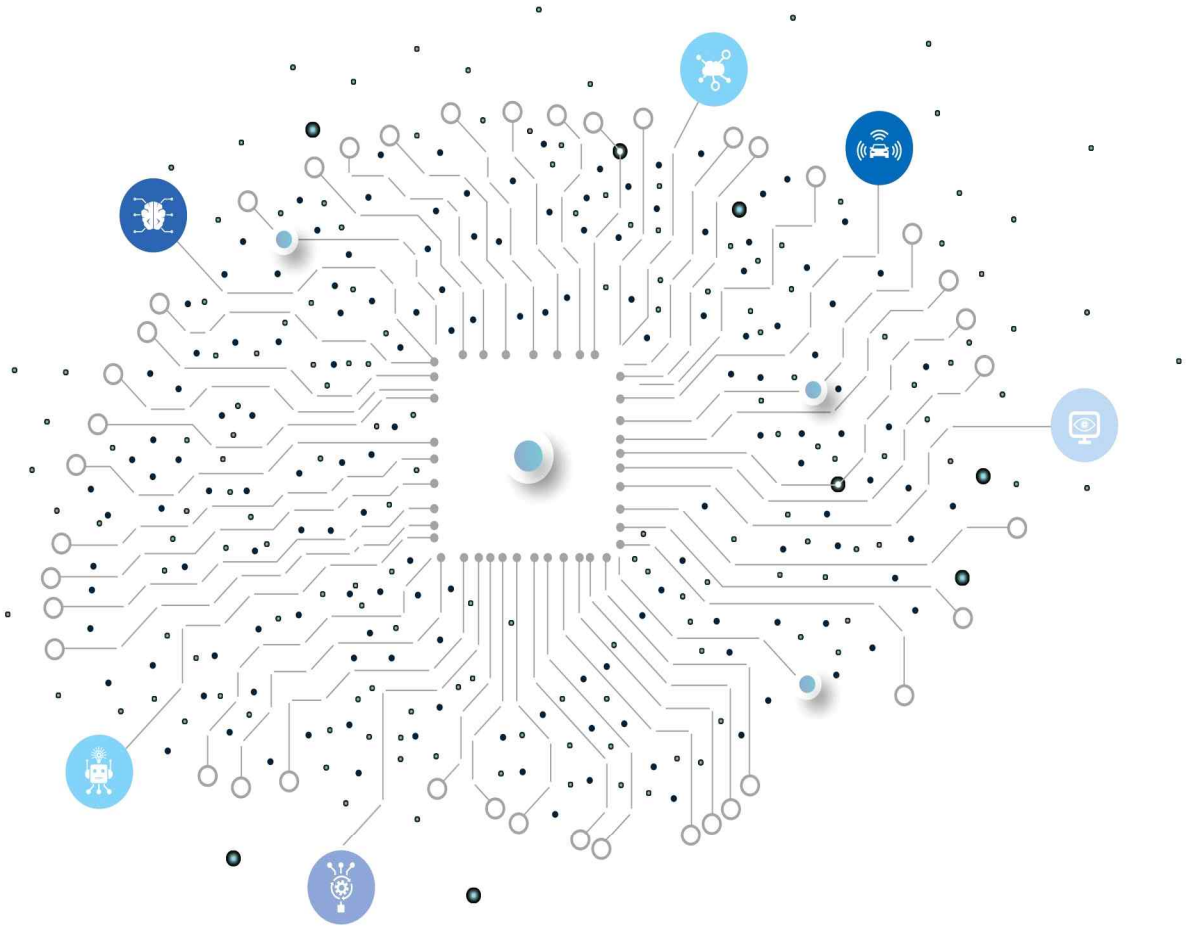
AI Network Lab
INSIGHT
Vol.7
(2022.07)



2022 이슈리포트

Zero Trust Architecture

| 작 성 | 제주대학교 송왕철 (philo@jejunu.ac.kr)

NIA 한국지능정보사회진흥원
NATIONAL INFORMATION SOCIETY AGENCY

o 『AI Network Lab 인사이트』는 인공지능, 클라우드, 5G 등 4차 산업혁명의 핵심인 지능정보기술과 네트워크 신기술에 대한 동향을 간략하고 심도 있게 분석한 보고서입니다.

o 본 연구보고서는 과학기술정보통신부의 방송통신발전기금조성사업, 한국지능정보사회진흥원의 초연결지능형 연구개발망 구축·운영사업의 연구과제 결과이며, 한국지능정보사회진흥원/한국능률협회와 공동 기획하였습니다.

o 본 보고서의 내용은 한국지능정보사회진흥원의 공식 견해와 다를 수 있습니다.

발 행 처 한국지능정보사회진흥원

발 행 인 문용식

기 획 한국지능정보사회진흥원 지능형인프라본부 공공인프라팀

보 고 서 온라인 서비스 www.nia.or.kr

Contents

보고서 주요 내용

(1) 서론 ····· 4
(2) 기술 및 서비스 현황 ····· 5
(3) Zero Trust Architecture ····· 6
(4) 관련 플랫폼 ····· 11
(5) 클라우드 서비스 ····· 16
(6) 결론 ····· 17

참고문헌 ····· 18

Zero Trust Architecture

주 요 내 용

(1) 서론

정보화 사회가 진전되어가면서, 기업이나 사회의 여러 조직들은 더 이상 폐쇄된 네트워크만으로 업무를 관리하기 어려워졌으며, 동시에 최근의 COVID-19 바이러스로 인한 사회적 문제들로 인해 사람들이 사무실에서 원격 근무로 전환하여 근무하는 사례가 빈번해졌다. 또한, 기업과 조직에서는 다양한 장치와 네트워크를 지원하는 클라우드 플랫폼의 사용을 증가시켜왔다. 이러한 변화는 또한 현장 작업은 물론이고 온라인 작업과 관련된 갑작스런 패러다임 변화가 생기게 됨에 따라 잠재적 보안 위험을 악용할 수 있는 기회가 노출되게 되었다. 데이터는 점점 더 많은 서비스, 장치, 애플리케이션 및 인력으로 분산되고 있고, 암호 또는 경계 방화벽과 같은 기존의 보안 조치는 악의적인 작업을 차단하기에 불충분한 것으로 입증되었다. 다시 말해, 현재의 디지털 혁신 시대에는 경계선이 존재하지 않으며 보안에 대한 오래된 접근 방식은 오늘날의 위협에는 충분한 대응이 되지 못하는 상황인 것이다.

레거시 보안은 클라우드 보안을 다루는 기능에 한계가 있다. 레거시 보안은 모든 응용이 동일한 네트워크 위치에서 제공되고 모든 사용자가 동일한 진입점에서 해당 애플리케이션에 액세스한다고 가정하는 폐쇄 경계 보안 모델에 의존하기 때문이다. 이와는 대조적으로 근래에 제시된 Zero Trust 아키텍처는 경계 내 또는 경계 밖의 어떤 것도 본질적으로 신뢰하지 않는 IT 보안 패러다임이다. 이 접근법의 핵심 철학은 네트워크 경계선 내외에서 사설 네트워크의 서비스에 접속하려는 사용자나 컴퓨터는 보안 관점에서 동일하게 취급된다는 것이다. 이러한 추가 보호 계층은 사이버 공격의 범위를 억제하는 것으로 입증되었다.

Zero Trust가 제공하는 추가 보안 계층은, 기업이 네트워크 내의 종단점 및 서비스 수를 늘리고 클라우드 기반 애플리케이션 및 서버를 포함하도록 인프라를 확장함에 따라 매우 중요하다. 이러한 경향은 전통적인 보안 방법을 사용하여 보안 경계를 설정, 모니터링 및 유지하는 것을 더욱 어렵게 만들며, 또한 직원들에게 원격으로 일할 수 있는 능력을 제공하는 글로벌 인력을 보유한 조직에는 국경 없는 보안 전략이 필수적이다.

Zero Trust는 신원 검증 및 행동 분석, 마이크로 세분화, 종단점 보안 및 최소 특권 제어를 포함하여 광범위한 예방 기법을 결합하여 공격 희망자를 억제하고 위반 시에

이들의 액세스를 제한하는 방식이다. 방화벽 규칙을 설정하고 패킷 분석에 의해 차단하는 것만으로는 충분하지 않다. 예를 들어 네트워크 경계 장치에서 인증 프로토콜을 통과하는 손상된 계정은 액세스를 시도하는 각 후속 세션 또는 종단점에 대해 다시 검증받을 수 있어야 한다. 정상적인 동작과 비정상적인 동작을 인식하는 기술을 보유할 수 있다면, 그 기관은 VPN이나 소프트웨어 게이트웨이를 통해 연결하지 않더라도 인증 제어 및 정책을 강화할 수 있으므로 연결이 완전히 안전하고 신뢰할 수 있다.

따라서 본고에서는 Zero Trust 아키텍쳐에 대하여 살펴보면서 새로운 보안 체계에 대한 논의를 하고자 한다.

(2) 기술 및 서비스 현황

Zero Trust 전략은 엔터프라이즈 IT 생태계 유지 관리 목표를 달성하기 위해 기존의 여러 기술과 거버넌스 메커니즘에 의존한다. 예를 들어, MFA(Multi-factor Authentication)는 Zero Trust 모델의 핵심 기능이다. MFA는 단순히 사용자를 인증하기 위해 둘 이상의 증거를 요구하는 것을 의미하며, 단지 암호를 입력하는 것만으로는 접근을 얻을 수 없다. 일반적으로 볼 수 있는 MFA의 애플리케이션은 구글과 페이스북과 같은 서비스들이 구현한 2단계(two factor) 인증이다. 즉, 비밀번호와 함께 등록된 모바일 번호로 전송되는 OTP가 로그인에 사용된다. 설정한 비밀번호는 '당신이 알고 있는 것'이며, OTP는 당신이 가지고 있는 어떤 것이 된다. 따라서 '당신이 알고 있는 것' 요소가 손상되더라도, 당신의 계정을 보호할 '있는 것' 요소는 여전히 존재한다.

그림 1. 2단계 인증

방화벽을 사용하여 경계 보안을 적용하는 것은 애플리케이션과 사용자가 동일한 물리적 경계(perimeter)에 독점적으로 존재하는 한 충분히 잘 작동하는 모델이다. 그러

나 모바일 인력의 증가, 리소스 액세스에 사용되는 다양한 장치의 급증, 디지털 전환을 지원하기 위한 아키텍처의 변화 및 퍼블릭, 프라이빗 및 하이브리드 클라우드의 폭발적인 성장으로 인해 기존의 경계 원칙은 거의 폐기될 시점에 처해있다. 경계는 더 이상 기업의 물리적 위치만이 아니며, 기존 경계선이 뚫리면 공격자는 조직의 권한이 있는 내부 네트워크에 비교적 쉽게 액세스할 수 있으며, 이는 경계선 안에 있는 것이 더 이상 안전한 장소가 아니라는 것을 의미한다. 그 결과 기업들은 MPLS와 같은 전통적인 네트워킹 방법을 포기하고 NetFoundry의 OpenZiti처럼 그림 2과 같이 Software Defined Perimeter (SDP)를 구현하고 있다. SDP는 ID를 기반으로 리소스 액세스를 제어한다. SDP를 사용하면 보호된 리소스에 대한 액세스가 허용된 엔티티는 네트워크 또는 위치에 관계없이 연결 전에 완전히 인증될 수 있다.

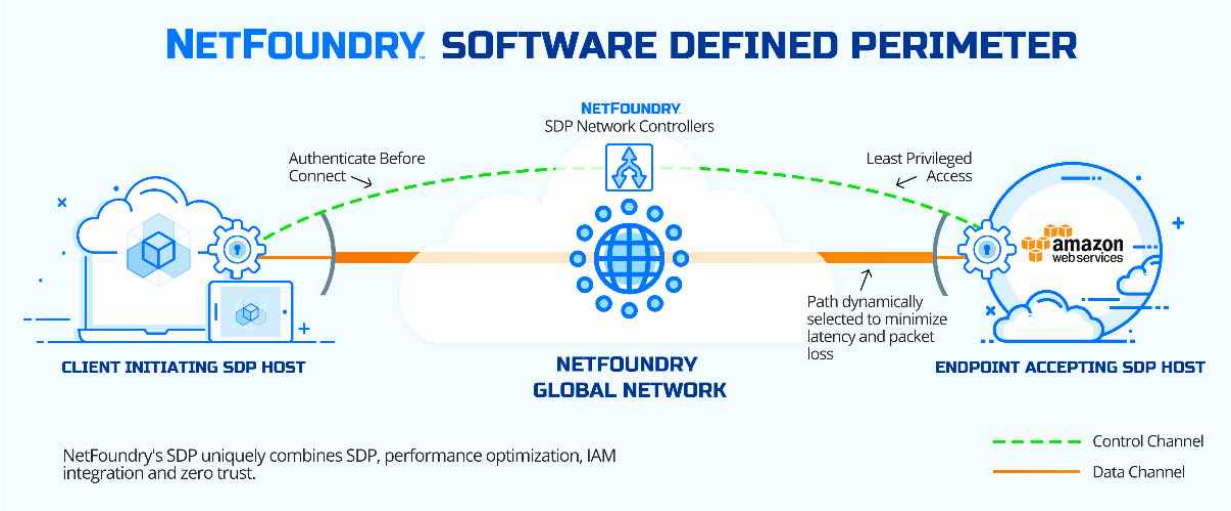


그림 2. SDP(Software Defined Perimeter), 출처: Netfoundry

(3) Zero Trust Architecture

(가) NIST 표준안

NIST(National Institute of Standards and Technology)는 2020년 8월에 Zero Trust의 표준 아키텍처를 상세히 기술한 완전한 문서를 발표했다. Zero trust와 관련된 작업을 제안할 때 많은 연구 논문들이 이 문서에 연결되며, 우리도 또한 이 표준을 제안된 보안 프로젝트의 기반으로 삼았다. 이 문서에서 고려한 두 가지 주요 고려 사항이 있다. 첫 번째는 Zero Trust 아키텍처의 core components이고, 두 번째는 Zero Trust를 위한 SDP 구현에 대한 것이다.

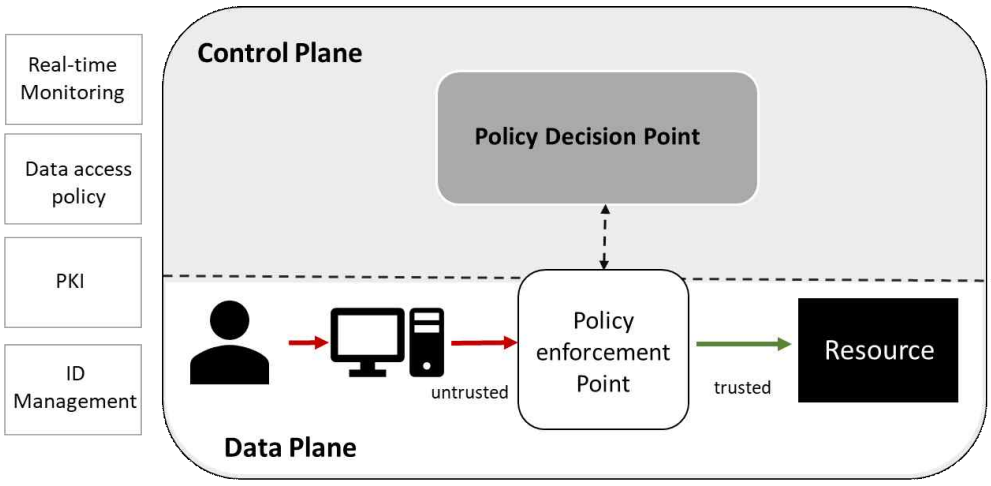


그림 3. Components of Zero Trust in the ZTA Architecture Standard, 출처: NIST

ZTA 아키텍처의 두 가지 주요 구성 요소는 Policy Decision Point (PDP)과 Policy Enforcement Point (PEP)이다.

☞ PDP: 이 구성 요소는 주어진 주제에 대한 리소스에 대해 액세스 권한을 부여하는 결정을 담당한다. 리소스에 대한 액세스를 허용, 거부 또는 취소한다. 또한 사용자(장치)와 리소스(정책에 따라) 간의 통신 경로를 설정 및/또는 종료할 책임이 있다. 세션별 인증 및 인증 토큰 또는 엔터프라이즈 리소스에 액세스하는 데 클라이언트가 사용하는 자격 증명을 생성한다.

☞ PEP: 이 구성 요소는 사용자와 리소스 간의 연결을 직접 활성화, 모니터링 및 종료하는 역할을 한다. 이것은 두 가지 다른 방법으로 표현될 수 있는 ZTA의 논리적 구성 요소이다.

- ✓ 클라이언트(예: 랩톱의 에이전트) 및 리소스 측(예: 액세스를 제어하는 리소스 앞의 게이트웨이 구성 요소)
- ✓ 통신 경로에 대한 게이트키퍼 역할을 하는 단일 구성 요소

(나) Zero Trust를 위한 SDP 구현

NIST에 따르면 ZTA(Zero Trust Architecture)를 구성하고 달성하는 방법은 대체로 다음의 세 가지로 분류된다.

☞ Enhanced Identity Governance에 기반한 ZTA

☞ Micro-Segmentation에 기반한 ZTA

☞ Network Infrastructure and Software Defined Perimeters에 기반한 ZTA

이들 중에 마지막 방식이 SDP(Software Defined Perimeter)방식으로 언급되며,

SDN(Software Defined Networks)와 IBN(Intent based Networking)으로부터의 개념을 포함하고 있어서[1], 본고에서는 이를 위주로 설명하고자 한다.

NIST의 말을 인용하면, 네트워크 인프라 및 Software Defined Perimeter를 사용하는 ZTA는 Software Defined Network(SDN) 개념을 포함하는 접근 방식이다 [2]. 이 접근 방식에서 컨트롤러는 Policy Decision Point가 내린 결정에 따라 네트워크를 설정하고 재구성한다. 클라이언트는 컨트롤러 구성 요소에 의해 관리되는 정책 시행 지점을 통해 액세스를 계속 요청한다. 이 구현은 Policy Enforcement Point를 Device Agent/Gateway 모델로 구분한다. [3]

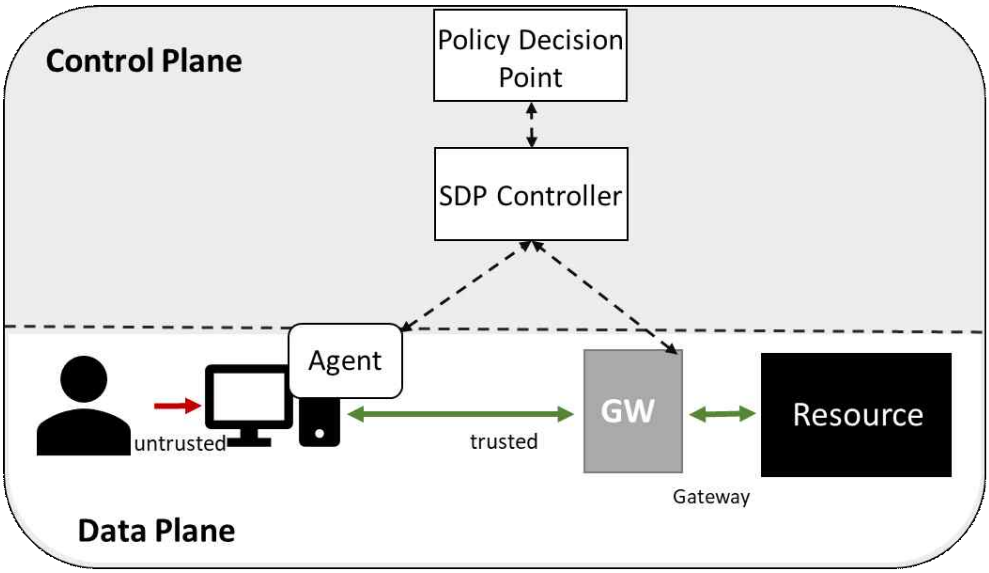


그림 4. SDP envision in a device agent/gateway model, 출처: NIST

위의 그림 4에서 볼 수 있듯이 에이전트는, 사용자에게서 시작된 요청이 평가받도록 트래픽을 SDP 컨트롤러로 전송하는 소프트웨어 구성 요소이다. 컨트롤러는 SDP 게이트웨이와 통신하고 에이전트와 리소스 간에 구성된 승인된 통신 경로만 허용한다.

SDP 개념 모델을 따르는 간단한 시나리오는 다음과 같다.

※ 엔터프라이즈 제공 장치를 가진 사용자가 엔터프라이즈 리소스(엔터프라이즈 앱)에 연결하려는 경우

1. 액세스 요청은 소프트웨어 에이전트에 의해 수행되고 요청은 컨트롤 플레인 통신을 통해 컨트롤러로 전달된다.
2. SDP 컨트롤러는 평가를 위해 정책 결정 지점으로 요청을 전달한다.
3. 요청이 승인되면 컨트롤러는 control plane을 통해 장치 에이전트와 관련 리소스 게이트웨이 간의 통신 채널을 구성한다. 여기에는 인터넷 프로토콜(IP) 주소, 포

트 정보, 세션 키 또는 유사한 보안 세부 정보와 같은 정보가 포함될 수 있다.

4. Device 에이전트와 게이트웨이가 연결되고 암호화된 서비스 데이터 flow가 시작된다.
5. Device 에이전트와 리소스 게이트웨이 간의 연결은 워크플로가 완료되거나 보안 이벤트(예: 세션 시간 초과, 재인증 실패 등)로 인해 컨트롤러에 의해 트리거 될 때 종료된다.

에이전트는 모든 장치에 설치해야 하는 소프트웨어다. 또한 클라우드 서비스가 필요한 경우에는 클라이언트-서버 모델을 적용할 수 있다. 이 사용 사례에서 엔터프라이즈는 로컬 네트워크를 가지고 있지만 클라우드 서비스 공급자를 사용하여 애플리케이션/서비스 및 데이터를 호스팅 한다. 게이트웨이는 리소스를 호스팅 하는 퍼블릭 / 프라이빗 클라우드(서버) 내부의 가상화된 장비이다. 개념적 배치는 그림 5에서 확인할 수 있다. 제로 트러스트 절차는 위에 나열된 Device Agent/Gateway모델을 따른다.

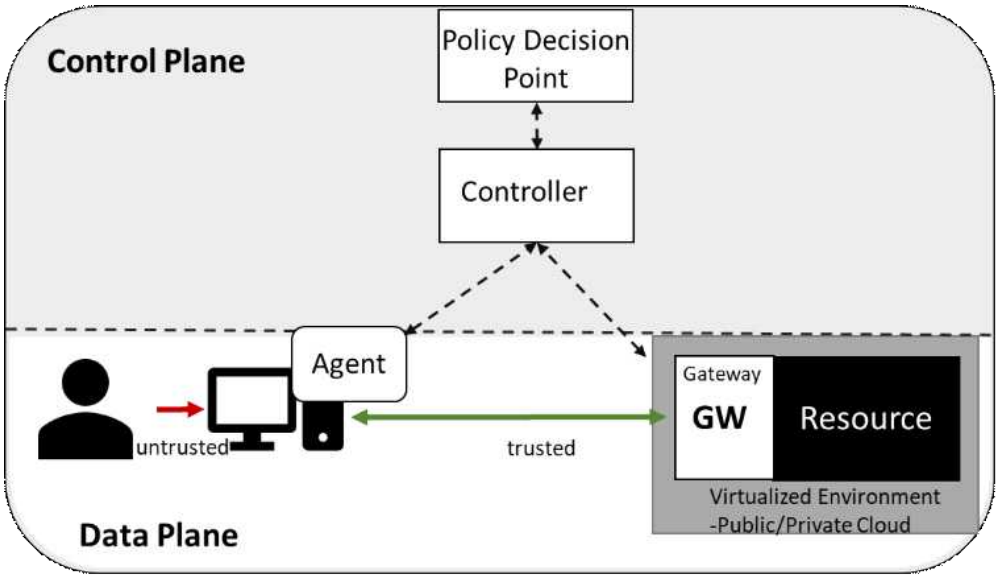


그림 5. Client-Server model for SDP, 출처: NIST

NIST가 Zero-Trust 아키텍처 표준에서 제안한 SDP 아키텍처 모델은 Cloud Security Alliance SDP 규격(CSA-SDP)을 기반으로 한다 [4]. CSA는 SDP를 위한 아키텍처를 제안했으며, 이는 많은 Zero-Trust 제안의 기초로 사용되어 왔다. CSA에 따르면, SDP의 주요 구성 요소에는 클라이언트(요청자), 호스트(서비스 제공자), 클라이언트와 서비스 제공자를 연결하는 SDP 컨트롤러가 포함된다.

연결은 컨트롤 플레인을 통해 SDP 컨트롤러와의 상호 작용에 의해 관리된다. SDP 아키텍처의 예는 그림 6에 나와 있다. 이러한 구성 요소는 보안 연결을 달성하기 위해 ZTA가 요구하는 것과 관련이 있다. 그것이 두 개념(SDP와 ZT)이 연관성이 있는 이

유이며, 대부분의 연구는 SDP를 ZT에 대한 좋은 접근법으로 간주한다.

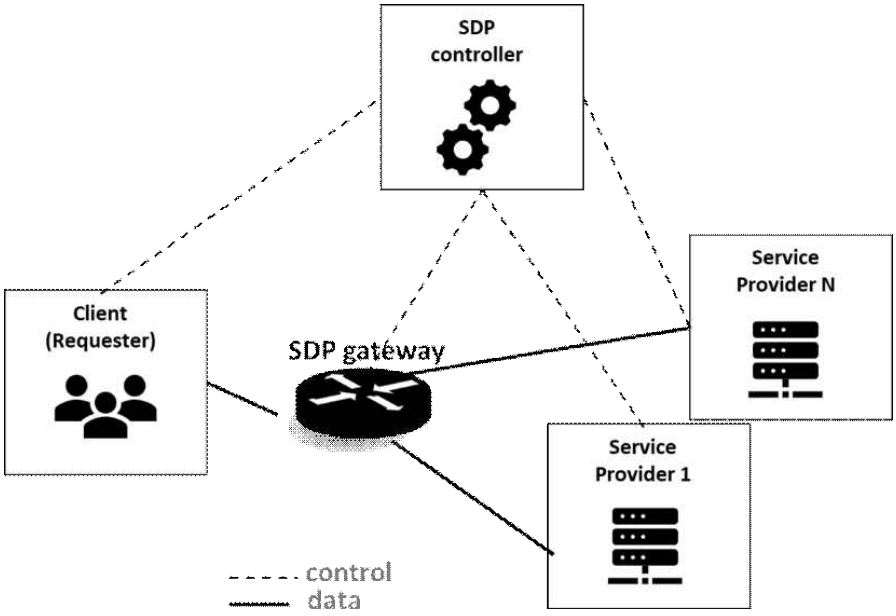


그림 6. Basic SDP architecture, 출처: NIST

그림 6에서와 같이 일반적인 SDP 시나리오에는 다음과 같은 구성 요소가 있다:

① SDP 클라이언트 소프트웨어는 SDP 네트워크에 대한 연결을 시작한다. 이는 ZTA의 에이전트/게이트웨이 접근 방식과 유사하다. SDP 소프트웨어(에이전트)는 클라이언트 장치 자체에서 실행된다. 이 요청은 SDP를 운영하는 기업의 통제 영역 밖에서 부터 올 수 있다.

② Service Provider 장치는 클라이언트의 연결을 허용하고 SDP에 의해 안전하게 보호되는 일련의 서비스를 제공한다. 서비스 공급자는 일반적으로 기업의 통제(및/또는 직접 대표자) 아래 네트워크에 상주한다.

③ SDP 게이트웨이는 인증된 사용자와 장치에 보호된 프로세스 및 서비스에 대한 액세스를 제공한다. 게이트웨이는 또한 이러한 연결에 대한 모니터링, 로깅 및 보고를 제정할 수 있다.

④ SDP 컨트롤러는 사용자가 인증 및 인증되었는지, 장치가 검증되었는지, 보안 통신이 설정되었는지 등을 점검하며, 네트워크의 사용자 및 관리 트래픽이 별도로 유지되도록 하여 격리된 서비스에 대한 액세스를 보호한다.

SDP 환경의 일반적인 워크플로우는 다음과 같다.

1. SDP 컨트롤러와 하나 이상의 SDP 게이트웨이가 활성화되고 PKI 서비스, 다중 요소 인증, 아이덴티티 연합 및 기타 유사한 서비스와 같은 인증 및 권한 부여 서비스에 연결된다.

2. 하나 이상의 서비스 제공자가 SDP 내에서 추가되고 활성화된다. SDP 컨트롤러에 연결하고 안전한 방식으로 인증한다. 기본적으로 서비스 공급자는 엔드포인트로부터의 통신을 승인하지 않으며 프로비저닝 되지 않은 요청에 응답하지 않다.
3. SDP 내에서 연결하려는 각 클라이언트는 SDP 컨트롤러에 의해 인증되어야 한다.
4. 클라이언트를 인증한 후 SDP 컨트롤러는 클라이언트가 통신할 수 있는 서비스 공급자 목록을 결정한다(정책 및 인증/인가 정보에 기반).
5. SDP 컨트롤러는 서비스 공급자에 직접 연결된 SDP 게이트웨이에 클라이언트의 통신을 수락하도록 지시하고 암호화된 통신에 필요한 선택적 정책을 시작한다.
6. 클라이언트와 서비스 공급자는 상호 암호화된 데이터 채널을 통해 통신한다.

(4) 관련 플랫폼

Zero Trust Architecture(ZTA)는 많은 관심을 갖는 새로운 패러다임의 보안 메커니즘이므로, OpenZiti[5], OpenVPN[6], Pritunl[7], Panther SDP[8] 등과 같은 많은 개발 프로젝트들이 있다고 알려져 있다. 본 절에서는 OpenZiti, OpenVPN에 대하여 간략히 소개한다.

(가) OpenZiti

OpenZiti는 Apache 2.0 license로 license를 갖는 오픈 소스 코드로서, NETFOUNDRY[9] 회사에 의해 개발되고 있는 ZTA를 위한 차세대 보안 오픈 소스 네트워킹 솔루션이며, 다음의 몇 가지 요소를 갖추고 있다.

☞ Ziti 패브릭은 스마트 라우팅이 내장된 확장 가능하고 플러그형 네트워킹 메시를 제공함
☞ Ziti 에지 구성 요소는 네트워크에 대한 안전한 제로 트러스트 진입점을 제공함
☞ Ziti SDK를 사용하면 Ziti를 애플리케이션에 직접 통합할 수 있음
☞ Ziti tunnelers 및 프록시를 사용하면 기존 애플리케이션 및 네트워크에서 Ziti 배포를 활용할 수 있음

주요 보안 기능은 다음과 같다.

☞ 제로 트러스트 및 응용 Segmentation

- ✓ 제로 트러스트 솔루션을 통해 네트워크에 대한 액세스뿐만 아니라 해당 네트워크 내의 개별 애플리케이션에 대한 액세스를 강제할 수 있게 한다.
- ✓ Ziti 시스템의 모든 클라이언트에는 프로비저닝 된 인증서가 있는 ID가 있어야 하고, 인증서는 보안 통신 채널을 설정하고 연결된 ID의 인증 및 권한 부여에 사용된다. 클라이언트가 네트워크 애플리케이션에 액세스를 시도할 때마다 Ziti는 먼저 ID가 애플리케이션에 액세스할 수 있는지 확인하며, 액세스가 취소되면 열린 네트워크 연결이 닫히게 된다. 이 모델을 통해 Ziti 시스템은 여러 애플리케이션에 대한 액세스를 제공하는 동시에 클라이언트가 액세스 권한이 부여된 애플리케이션에만 액세스할 수 있도록 한다. 또한, 클라이언트에 대한 인증서 기반 인증을 요구하는 것 외에도 Ziti는 인증서를 사용하여 Ziti 구성 요소 간의 통신을 승인하는 기능을 갖추고 있다.

☞ 다크 서비스 및 라우터

- ✓ 서비스를 어둡게 만들 수 있다. 즉, 누구도 시도하고 연결할 수 있게 하는 포트가 열려 있는 것이 아니다. 무언가를 어둡게 만드는 것은 몇 가지 방법으로 수행할 수 있지만 일반적으로 Ziti에서 처리되는 방식은 서비스가 Ziti 네트워크 패브릭에 도달하여 하나 이상의 연결을 설정하고, 패브릭으로 들어오는 클라이언트는 인증 및 권한 부여 후 이러한 연결을 통해 서비스에 연결할 수 있게 한다.
- ✓ 패브릭을 구성하는 Ziti 라우터도 어두울 수 있다. 사설 네트워크에 위치한 라우터는 일반적으로 어둡게 만든다. 이러한 라우터는 컨트롤러와 통신하고 네트워크 패브릭 메시에 연결하기 위해 사설 네트워크 밖으로 연결되게 될 수 있다. 이러면 사설 네트워크의 서비스와 라우터가 아웃바운드 연결만 만들 수 있으므로 인바운드 트래픽에 대해 구멍이 열리지 않게 할 수 있다.

☞ 종단 간 암호화

- ✓ Ziti의 개발자 SDK를 활용하고 클라이언트 및 서버 응용 프로그램에 Ziti를 내장하면 클라이언트 응용 프로그램에서 서버 응용 프로그램으로 원활하게 암호화되도록 트래픽을 구성할 수 있다. 터tunnelers 또는 프록시 응용 프로그램을 사용하려는 경우 컴퓨터에서 컴퓨터로 또는 사설 네트워크에서 사설 네트워크로 트래픽을 암호화할 수 있습니다. 이를 통해, 종단 간 암호화는 클라이언트와 서버 간의 시스템이 손상되더라도 트래픽을 해독하거나 변조할 수 없다.

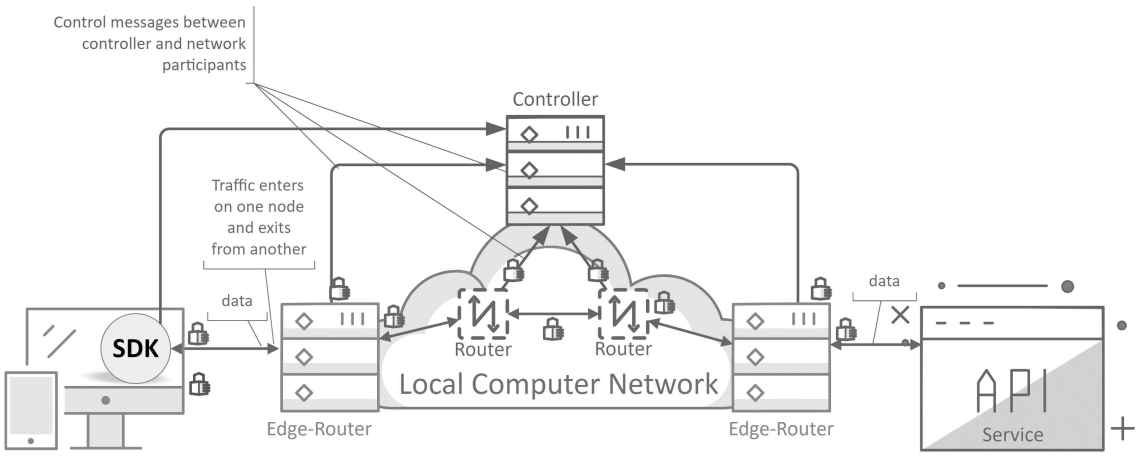


그림 7. OpenZiti framework by NetFoundry, 출처: NetFoundary

OpenZiti의 구성은 다음과 같다. Ziti Controller, Ziti Router/Edge Router 및 Ziti Edge Client로 구성된다. 이러한 구성 요소들은 클라이언트에서 서버로의 두 지점 간에 보안 연결을 제공하기 위해 사용된다. 이러한 유형의 네트워크는 기존 네트워킹 인프라 위에 안전한 연결을 제공하므로 오버레이 네트워크로 간주된다.

Ziti Controller는 configuration plane을 제공한다. Ziti controller는 Ziti 서비스를 configure하는 데 책임을 지며Ziti 네트워크를 구성하는 사용자, 장치 및 노드에서 사용되는 아이덴티티들을 관리하는 중앙 지점이 된다. Ziti controller는 상호 인증된 TLS(mTLS)를 기반으로 Ziti 네트워크의 모든 연결에 대한 인증 및 인증을 담당한다. 컨트롤러는 Ziti 네트워크의 일부인 엔티티의 확인 및 서명 요청을 처리하기 위해 "self-signed certificate"를 사용한다.

Ziti Routers/Edge Routers는 하나의 Ziti 네트워크 노드에서 트래픽의 목적지로 트래픽을 안전하고 안정적으로 전송하는 역할을 한다. 또한 Edge 라우터는 Ziti 인프라의 일부가 아닌 end-to-end 장치에 대한 입구 및 출구 지점을 제공한다.

router/edge-router의 주요 기능은 다음과 같다:

☞ Edge-Router: 네트워크에 대한 안전한 Zero Trust entry point (아이덴티티 기반 인증, 인증, 암호화)

  ✓ 아이덴티티, 역할 및 서비스를 매핑 하는 모든 서비스 정책을 이 Edge-Router에서 적용하고 강제되도록 한다.

☞ Router: 스마트 라우팅 및 동적 치유 기능을 갖춘, 확장 가능하고 플러그 가능하며 지리적 라우팅이 가능한 메시 네트워크 오버레이

  ✓ 이 유형의 라우터는 트래픽만 라우팅하며 주로 오버레이 네트워크의 확장성 사용된다.

모든 router는 기본적으로 routable mesh network overlay로 동작하며, "edge" 기능은 달성하고자 하는 네트워크 시나리오의 유형과 관련하여 추가 구성으로 전환(toggled)될 수 있다. 네트워크에서 오버레이 트래픽 흐름을 허용하려면 Ziti 배포에 Edge-Router가 하나 이상 있어야 한다. (서비스 정책을 라우터에 적용할 수 없으면 E2E 연결을 제공할 수 없다).

Ziti Edge 클라이언트는 Ziti 네트워크에 안전하게 연결하는 데 필요한 기능을 제공하는 SDK를 기반으로 하며 대상 애플리케이션에 쉽게 통합되도록 설계되었다.

Ziti의 제로 트러스트 기능에 대한 주요 개념은 다음과 같다:

☞ Services

✓ 기존 네트워크에서 클라이언트가 액세스할 수 있는 모든 리소스의 정의에 대한 개념이다. Ziti 서비스는 언더레이 개념의 표현이 아닌 identity로 정의된다(네트워크 정보가 필요 없음).

☞ Identities

✓ 연결을 설정할 수 있는 Ziti 네트워크의 개별 엔드 포인트를 나타낸다. Ziti 네트워크 내에서 이루어지는 모든 연결은 X.509 인증서를 사용하여 상호 인증된다. 모든 Identities는 지정된 인증서의 서명에 매핑 된다. Ziti Edge 클라이언트는 Ziti 네트워크에 대한 연결을 시작할 때 이 인증서를 제공한다.

☞ Policies

✓ Identities와 Services가 상호 작용하는 방법을 제어한다. 서비스를 사용하려면 Identities에 서비스에 대한 액세스 권한이 부여되어야 한다. 또한 서비스에 대한 모든 액세스는 하나 이상의 에지 라우터를 통과하므로 해당 에지 라우터에 액세스하려면 서비스와 Identities가 모두 지정되어야 한다.

(나) Open VPN

Open VPN은 전통적인 VPN이라는 기능을 구현한 open source 프로젝트로서, 라우팅 또는 브리지 구성 및 원격 액세스 시설에서 안전한 지점 간 또는 사이트 간 연결을 생성하는 기술을 구현하는 VPN(가상 사설망) 시스템이며, 클라이언트 및 서버 응용 프로그램을 모두 제공하고 있다.

Zero Trust Access를 적용하는 것은 안정적인 보안 프로그램의 중요한 계층으로, ZTA를 반영하여 개발된 Open VPN Cloud는 모든 규모의 기업에 안전한 가상화 네트

워크를 생성할 수 있는 기능을 제공한다. 이 네트워크는 네트워크 경계 외부에서 가정 및 공용 Wi_Fi 네트워크와 SaaS 애플리케이션을 사용하는 작업자를 보호하는 보안 액세스를 확장하며, 강력한 Zero Trust Network를 구축하여 공격을 차단하거나 크게 완화하는 데 필요한 모든 도구와 기능을 제공하고 있다.

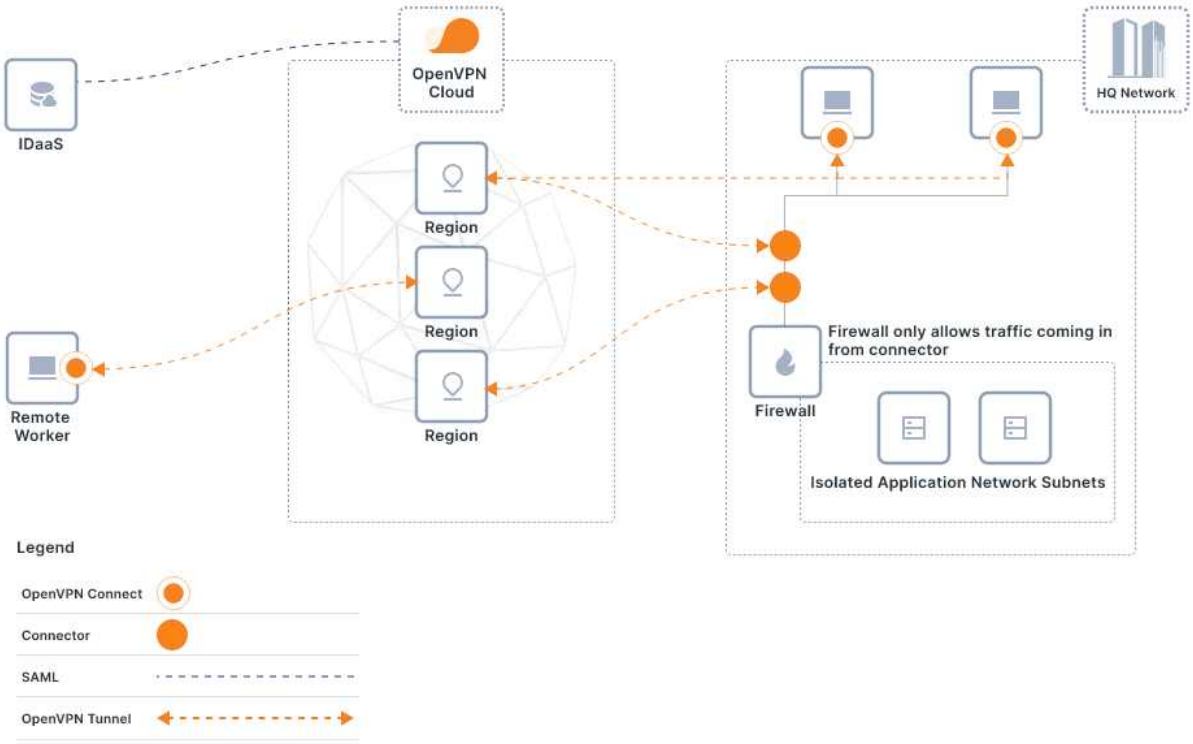


그림 8. OpenVPN solution, 출처: OpenVPN

- ✓ perimeter defense에만 기반 하여 connection을 신뢰하지 않는다. ID 기반 인증 정책을 정의한 다음 특정 애플리케이션 리소스에 대한 보안 연결을 적용한다.
- ✓ 특정 애플리케이션 리소스를 분류하고 격리하여, 위치에 관계없이 안전한 사설 네트워크를 통해서만 액세스할 수 있도록 한다.
- ✓ 서비스 액세스에 대한 강력한 ID 인증 및 네트워크 수준 권한 부여로 네트워크에서 lateral movement를 방지한다. 이는 Connect Auth 기능을 사용하여 모든 연결에 인증을 적용하고, 주요 SAML ID 플랫폼과 통합하고, 사설 및 공공 서비스들의 도메인 이름에 대한 유연한 그룹 수준 액세스 제어를 사용함으로써 가능하게 한다.
- ✓ 사용자 그룹을 기반으로 액세스 제어를 정의한다. 모든 그룹에 필요한 리소스

에만 액세스를 제한하는 ACL(액세스 제어 목록)을 만들고, 역할과 부서를 ACL에 매핑하고 네트워크 수준에서 시행하도록 한다.

✓ 도메인 이름으로 신뢰할 수 있는 인터넷 대상에만 액세스를 제한한다.

(5) 클라우드 서비스

클라우드 기술은 전 세계의 비즈니스 운영 방식을 혁신해왔고 클라우드 서버를 사용하면 장소에 상관없이 더 큰 유연성을 얻을 수 있으며 민감한 데이터의 저장을 가능하게 하며 재택근무를 가능하게 하는 클라우드는 모든 비즈니스의 미래에 핵심이다. 이는 사무실의 경계 기반 사이버 보안 시스템 외부로 시스템을 확장하여 다양한 진입 지점을 여는 것으로, 클라우드는 어디에나 있기 때문에, 그만큼 기존의 perimeter에 기반 하는 보안모델이 아니라, ZTA에 기반 한 보안 모델의 적용은 클라우드에 있어서는 필수적이다.

많은 ZTA 솔루션들이 클라우드에서의 연동을 내세우고 있듯이, 그림 9의 예와 같이, 아마존 AWS 및 마이크로소프트의 Azure 등과 같은 많은 클라우드 서비스들을 보면, 자체적인 솔루션으로 ZTA를 지원하고 있으며, 기본의 보안 모델을 보강하여 제시하고 있다.

마이크로소프트는 Zero Trust 원칙으로 '명확한 검증', '최소한의 권한 액세스', '침

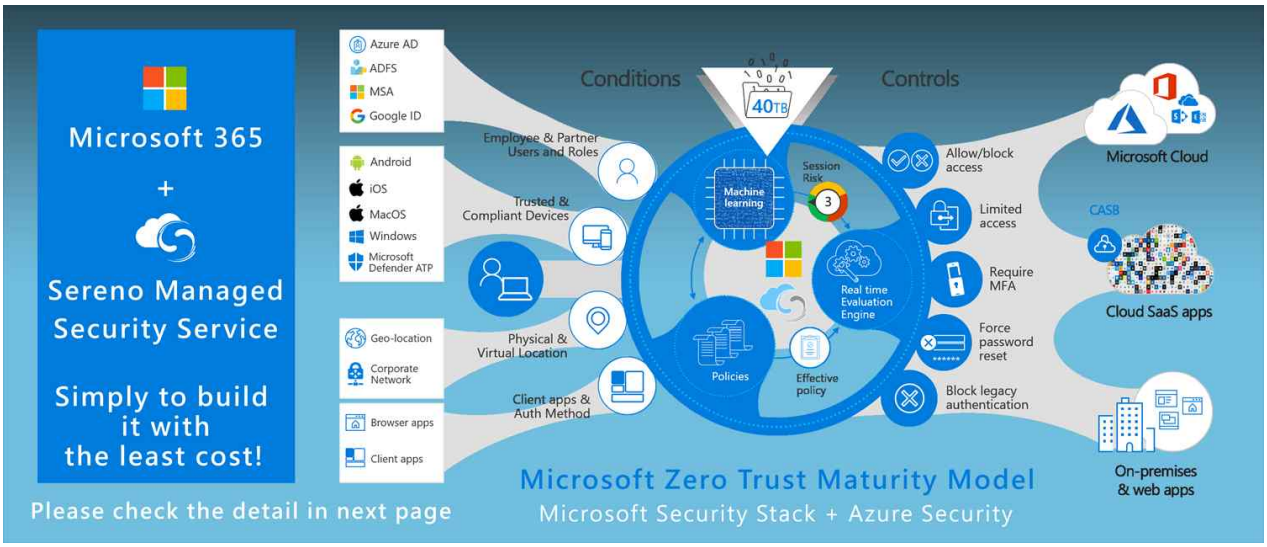


그림 9. Zero Trust Archtecture for K12
(출처: https://www.serenoclouds.com/microsoft-zero-trust-security/)

해 가정' 3가지를 정하고 이에 따라 Azure Active Directory를 구축해서 ZTA를 구축하고 있다. 구글은 Beyond Corp Enterprise를 이용해 구글의 핵심인프라 및 기업 리소스용 사용자 기반 및 기기 기반 인증과 승인을 제공한다. AWS는 Zero Trust 솔루

션을 제공하고 있지 않으나, Zero Trust 구현을 위한 클라우드 권장 보안 아키텍처를 제시하고 있다.

(6) 결론

2014년도 말에 구글이 Beyond Corp이라는 프로젝트를 통하여, 사용자의 네트워크 위치에 따라 네트워크를 통한 자원에 대한 접속을 결정하는 것이 아닌 사용자와 그 context에 따라 안전하게 접속을 결정하는 시스템을 개발하고 발표한 이후로, 또한 2018년도 Forrester가 발표한 ZTX(Zero Trust eXtended)를 통해 경계선에 의한 보안이 아닌 데이터와 아이덴티티 중심으로 전환해서 비즈니스의 보안 요구사항을 충족시킬 수 있을 보여준 이후로, 도입부에서 얘기한 바 있지만, 최근 COVID-19로 인한 재택근무의 급속한 확산과 클라우드 의존도의 급속한 증가를 통해 Zero Trust Architecture를 구현하는 솔루션은 현대의 ICT를 기반으로 하는 비즈니스에 필수불가결한 모델이 된 듯하다.

이미 상당수 기업 ICT 스토어에서는 제로 트러스트 모델을 적용하고 있고, 다중 인증, IAM, 그리고 접속 허가제도 등을 시행하고 있는 것을 생활 속의 다양한 서비스를 접하면서 느낄 수 있다. 하지만, ZTA는 지속해서 다양한 사물인터넷의 도입과 인공지능 기술의 도입을 겪으면서, 지속적으로 발전적인 모델을 보이게 될 것으로 보인다. 비즈니스 영역의 보안과 개인 보안이 모두 안전한 서비스가 이뤄질 수 있는 지속적 발전을 기대해 본다.

참 고 문 헌

[1] Cohen R, Barabash K, Rochwerger B, Schour L, Crisan D, Birke R, Minkenberg C, Gusat M, Recio R, Jain V (2013) An Intent-based Approach for Network Virtualization. 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013). (IEEE, Ghent, Belgium), pp 42-50. Available at https://ieeexplore.ieee.org/document/6572968

[2] Stafford, V. A. "Zero trust architecture." NIST Special Publication 800 (2020): 3.1.3 pp 13

[3] Stafford, V. A. "Zero trust architecture." NIST Special Publication 800 (2020): 3.2.1 pp 13

[4] Stafford, V. A. "Zero trust architecture." NIST Special Publication 800 (2020): 3.2.1 pp 14

[5] https://openziti.github.io/

[6] https://openvpn.net/

[7] https://pritunl.com/

[8]https://www.waverleylabs.com/services/software-defined-perimeter-panther-sdp-implementation/

[9] https://netfoundry.io/