Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 6 pp. 551-555, 2023

https://doi.org/10.5762/KAIS.2023.24.6.551
ISSN 1975-4701 / eISSN 2288-4688

제로트러스트 네트워크 기반 기업 업무시스템 보안성 강화 연구

서청정
이테크시스템

A study on the Security Enhancement of Enterprise Business System based on Zero Trust Network

Cheong Jeong Seo
E-Tech System Software Engineering Division

요 약 본 연구에서는 기업이 클라우드로 업무 시스템을 전환 시 가장 문제가 되는 기업 데이터 탈취 부분에 대한 예방을 위해 제로 트러스트 네트워크 기반의 설계를 통해 보안성을 강화하는데 그 목적을 두고 있다. ISMS(Information Security Management System, 이하 ISMS)의 기본인 ISO/IEC 27017, NIST SP 800-207에서 정의한 원칙과 Framework을 활용하여 사용자의 엔드포인트를 지속적으로 모니터링하고 통합 관제를 통해 로그인 정책과 네트워크 정책을 중심으로 실제 설계 방법을 제시하여 기업이 클라우드 내에서 기업 시스템 운영을 안전하게 할 수 있는 설계 가이드를 제공하고자 한다. 설계 가이드는 인증 부분과 네트워크 보안성 2가지 관점에서 Jason Garbis와 Jerry Champman이 설계한 ZTS(Zero Trust Security, 이하 ZTS) 방법론 중 인증 부분은 Enclave-Gateway-based Model을, 네트워크 보안성 부분은 cloud-routed model을 기반으로 실제 기업 환경에 맞추어 디자인하였다.

Abstract The purpose of this study was to enhance security by implementing a zero-trust network-based design to prevent the problematic issue of corporate data breaches during transitions of corporate business systems to the cloud. This study utilized the principles and frameworks defined in ISO/IEC 27017 and NIST SP 800-207, which are basic standards for information security management systems (ISMS). Based on this, users' endpoints were continuously monitored, and design methods centered around login policies and network policies through integrated control were developed. The goal was to provide a design guide for enterprises to safely operate their business systems in the cloud. A design guide was developed by Jason Garbis and Jerry Champman for the zero-trust security (ZTS) methodology, which focuses on two aspects: authentication and network security. For the authentication part, they based their approach on an enclave-gateway-based model, while for the network security part, they used a cloud-routed model. These design choices were made to align with real-world enterprise environments.

Keywords : ZTN(Zero Trust Network), Cloud Computing, Cloud Security, ISO/IEC 271017, NIST SP 800-207

1. 서론

COVID-19로 인해 많은 기업들이 기존에 사용하던 Legacy 기반의 업무 시스템을 클라우드 환경으로 전환을 가속화 하고 있다. 기존의 대면근무 방식에서 비대면 근무 방식 전환에 따라 더 이상 On-Premise의 환경에서의 사외 접속을 통한 업무에는 한계가 있다.

예를 들어 사내망으로 대규모의 데이터 트래픽을 위한

*Corresponding Author : Cheong Jeong Seo(E-tech system Software Engineering Division)
email: seopro97@kaist.ac.kr
Received April 26, 2023 Revised May 16, 2023
Accepted June 2, 2023 Published June 30, 2023

회선의 확장과 네트워크 접속 시간 지연 등으로 업무 처리가 제대로 이루어지기 어려운 것이 전환의 주요 이유이다.

기존에 기업들이 사용하는 Legacy 시스템의 장점은 자체 구축한 데이터센터(Data Center)내에 업무용 시스템을 직접 개발 또는 외주를 통해 구현하고 그에 맞는 인프라(H/W, S/W)등을 구매하여 구축 및 운용을 하고, 보안 부분에 있어서도 사내에서만 동작하는 폐쇄적 네트워크 형태를 유지함으로써 보안성 부분이 문제가 되지 않는다. 클라우드의 장점으로는 자체 데이터센터를 운영하는 것에 비해서 비용이 절감되고 특히 부족한 컴퓨팅 자원과 스토리지, 네트워크 자원 등이 실시간으로 Scale Up/Down이 가능하다. 하지만, 클라우드 환경으로 전환이 되면, 클라우드 환경 특성상 Hacking에는 취약한 부분이 많다. 사내망과 같은 폐쇄적인 네트워크가 아닌 외부에 오픈된 네트워크 환경으로 인해 더욱더 Hacking에 쉽게 노출이 가능 하다.

최근 이러한 대표적 사례로는 삼성전자와 현대자동차 그룹의 업무 시스템 중 재택용 업무 시스템을 통해서 갤럭시 시리즈 소스코드와 제네시스 설계도 등이 탈취되어서 기업입장에서는 클라우드로의 전환에 다시 한번 고민을 하게 된다. 이러한 문제를 해결하기 위한 방법을 적용하여 클라우드 컴퓨팅 자원을 활용하기 위해서는 최소한 다음 3가지 영역을 구축 시에 고려해야 한다. 자세한 내용은 Table 1과 같다[1-5].

Table 1. Consideration of Security Items

Mandatory Field	Description
Security Authentication	Active Directory Authentication and Multi Factor Authentication(MFA)
Data Hacking	Network Security Enforcement
Administrator	Password change Policy

이러한 최소한의 요구사항을 구현하기 위해서는 본 논문을 통해 다음과 같이 기술하고자 한다. 우선 2장에서는 서론에서 제시한 요구사항 3가지를 구현하기 위해서 제로 트러스트 네트워크의 개념과 NIST SP 800-207 및 ISMS(Information Security Management System, 이하 ISMS)의 표준 프레임워크인 ISO/IEC 27017에 대한 개념을 정리한다. 3장에서는 해당 프레임 워크를 활용하여 요구사항 기반으로 시스템 설계 및 검증 방법을 제시하고자 한다. 마지막 결론에서는 본 연구의 향후 개선 과제 및 계획을 설명하고자 한다.

2. 표준 프레임워크

2.1 제로 트러스트 네트워크 개념

제로 트러스트 네트워크(ZTN : Zero Trust Network, 이하 ZTN)는 2010년에 John Kindervag가 경계보안 문제점을 해결하기 위해 제안한 솔루션으로[6]로, '아무것도 신뢰하지 않는 것'을 전제로 한 사이버 보안 모델이다. '신뢰하는 검증'에서 '신뢰하지 않고 항상 검증'하는 전략으로 사용자 또는 디바이스가 내부 네트워크 접근 요청시 철저한 검증을 수행하고 그 이후에도 최소한의 권한만을 부여해서 내부 시스템에 접근을 허용하는 방식으로 동작 한다.

가상사설망(VPN : Virtual Private Network, 이하 VPN)와의 차이점은 다음 Table 2와 같다[7].

Table 2. Difference between ZTN and VPN

Difference Factor		ZTN	VPN
Features	Trust Model	Always each authentication to connect application on the local	One time Authentication
	Access Model	Application level	Network Level
	Authentication	Via The trust broker	ID/Password
Performance	Speed	Faster than VPN	-
	Ease of Use	Don't require a separate program.	Download and Setup VPN client.

2.2 NIST SP 800-207

NIST SP 800-207은 제로 트러스트 아키텍처 구현에 대한 지침을 제공하고 있다. 이 지침의 핵심 원칙은 다음의 Table 3과 같이 정리할 수 있다[8].

Table 3. The Seven Zero Trust Pillars

Number	Principle
1	All data sources and computing services are considered resources
2	All communication is secured regardless of network location
3	Access to individual enterprise resources is granted on a per-session basis
4	Access to resource is determined by dynamic policy

5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture

NIST SP 800-207의 7가지 원칙을 적용하여 이상적인 모델을 표현하면 다음 Fig. 1과 같다[8].

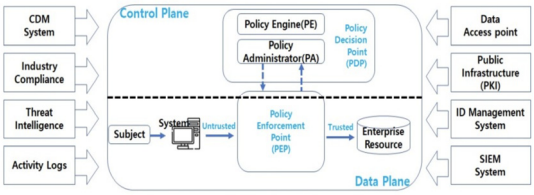

Fig. 1. Core Zero Trust logical Components (Ideal Model)

위의 Fig. 1에서 네트워크를 보호하기 위해 작동하는 요소는 Control Plane과 Data Plane 영역으로 구분이 된다. Control Plane은 네트워크 리소스에 대한 제어를 관리하는 정책과 규칙을 관리하며, 누가 어떤 리소스에 접근할 권한이 있는지 결정하고 해당 정책을 시행한다. Data Plane은 Control Plane에서 설정한 정책과 규칙을 시행하는 역할을 수행한다.

2.3 ISO/IEC 27017

ISMS의 표준인 27001:2013에서 클라우드 서비스의 정보보호 위험을 다루기 위해 추가적인 통제를 정의한 ISO/IEC 27017이 나오게 되었다. 이 중 제로 트러스트 네트워크와 연관된 콘트롤 항목을 정의하면 다음 Table 4와 같다[9,10].

Table 4. New Controls by ISO/IEC 27017:2015

Control Number	Control Item	Comment
CLD 12.1.5	Administrators's operational security	A cloud computing environment should be defined, documented, and monitored
CLD 13.1.4	Alignment of security management for virtual and physical networks	Configuration of virtual networks, consistency of configuration between virtual and physical networks

2.1-2.3에 정의 된 표준의 공통과 차이점을 비교하면 다음 Table 5와 같이 정리 할 수 있다.

Table 5. NIST SP 800-207 vs. ISO/IEC 27017

Field	NIST SP 800-207	ISO/IEC 27017
Main Role	Definition of ZTN's principle, Implement and Requirements	ZTN implement in terms of cloud environment
Focus	Security requirement	Under cloud environment

2.4 연구 전제 조건

본 연구에서는 다음과 같은 전제 조건을 두고자 한다. 첫째, 시스템의 구성은 단일 CSP(Cloud Service Provider, 이하 CSP)내에 한다고 전제한다. 다양한 CSP 내에 시스템을 분산하게 되면, 모니터링과 네트워크 구성에 있어서 복잡성이 올라가는 문제가 발생하게 된다. 둘째, 클라우드와 On-Premise 사내망의 시스템간은 Hybrid 형태로 제한을 둔다. 대부분의 기업 시스템들은 대고객 시스템이 아닌 이상 Public/Private 클라우드의 형태를 가지고 있지 않다. 셋째, 본 연구에서는 제로 트러스트 네트워크 관점에서 보안성을 강화하는데 목적이 있으므로 사용자의 인증 부분과 시스템 접속 권한을 제어하는데 중점을 두고자 한다.

3. 시스템 설계 및 검증

3.1 인증 설계

1장 Table 1에서 정의한 요구사항을 보면 인증 부분은 크게 2가지 요소로 다중인증(MFA : Multi Factor Authentication, 이하 MFA)과 Password 주기 변경 정책이 해당된다. 보통 기업에서는 기존의 전통적인 ID/Password를 이용해서 사내의 업무 시스템에 접속하는 방식보다는 간편하면서 강력한 프로세스를 활용하는데, 대표적인 기술 중의 하나가 Microsoft사의 AD(Active Directory, 이하 AD)를 많이 활용한다. 본 3장에서는 "Jason Garbis"와 "Jerry Chapman"이 저술한 Zero trust security 방법론 중 하나인 Enclave-Gateway-based Model을 활용하여 다음 Fig. 3과 같이 설계를 한다[11].

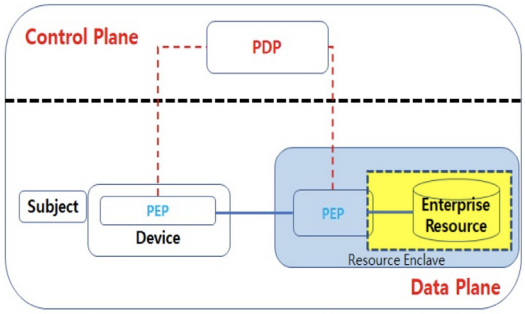

Fig. 2. Enclave-Gateway Based Model

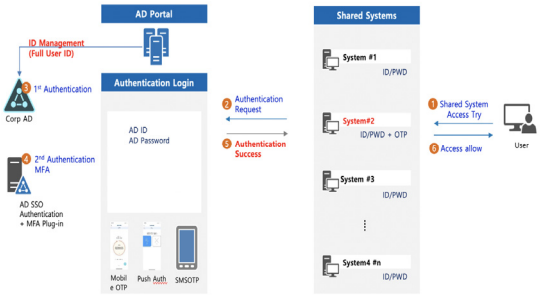

Fig. 3. Login Process Active Directory and MFA

위의 인증 프로세스 장점은 사용자가 시스템에 접속 시도 시 중앙 집중적인 Active Directory 서버를 통해 인증과 다중인증을 통해서 인증 성공 시 시스템 사용이 가능하도록 했으며, 각 시스템 별 인증 단계를 지속적으로 확인을 해서 안정성을 확보 할 수 있다. 또한 Active Directory에 정책 내에 Password 주기 변경 설정을 반영 하여 시스템 운영에 보안성을 제고할 수 있다.

위에서 나온 MFA는 보편적으로 비밀번호 및 SMS 인증번호를 사용하는 방식으로 인증번호 인식은 OTP(One Time Password, 이하 OTP)를 휴대폰에서 확인해서 인증을 강화할 수 있다. 이 외에도 최근에는 바이오인식으로 지문, 얼굴인식, 홍채인식 등의 다양한 방법을 활용하여 보안성을 높일 수 있다.

3.2 네트워크 보안성 설계

2019년 가트너에서 발표한 SASE(Secure Access Secure Edge, 이하 SASE)의 기술은 SDP(Software Defined Perimeter, 이하 SDP)와 제로 트러스트 기술을 포괄적으로 담고 있다. 기본적으로 SASE는 사용자가 각 시스템을 사용할 때에 데이터 채널과 제어 채널을 분리해서 인증 받지 못한 단말과 사용자는 접근이 불가능하도록 설계를 해야 한다. 본 연구에서는 클라우드에 기업 시스템이 전환된 상태에서 On-Premise내에 있는 기타 시스템과의 연계를 기본으로 설계를 하고 있기에 Zero Trust security 모델 중의 하나인 Cloud-routed model을 적용하여 설계를 한다[11].

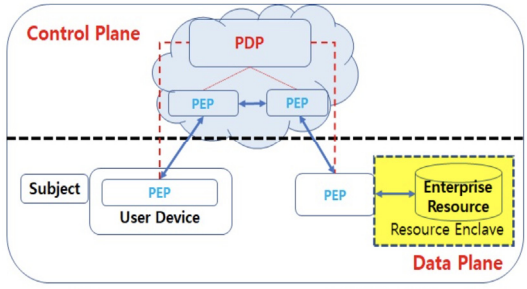

Fig. 4. Cloud-routed model

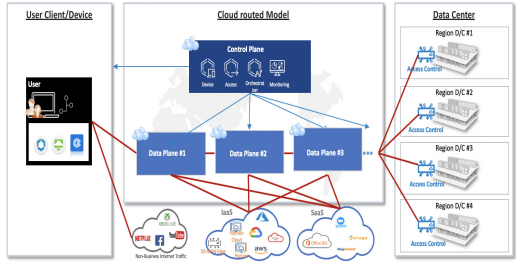

Fig. 5. SASE implement for using cloud-routed model

위의 구현 방법의 장점은 유저의 접속을 중간 Broker를 통해 목적지 정책에 맞는 지를 판단하고 해당 경로 별로 다중화 하여 원천적으로 사내의 시스템 접근 자체를 막는데 효과적이다. 3.1절에 구현한 인증 방식과 결합하여 Hacking 자체가 되지 않도록 설계하였으며, 모니터링을 24x7 감시하여 관제 시스템과의 연계가 가능한 것이 장점이다. Enclave-Gateway Based Model과의 차이를 보안성, 시스템 확장성, 운영성 등의 관점에서 비교를 하면 다음 Table 6과 같이 정리할 수 있다.

Table 6. Model difference

Item	Enclave-Gateway based model	Cloud-routed model
Security	Security Control by H/W	Security control by CSP (Cloud Service Provider)
Expansion	Enable to add Gateway but complexity high	Easy to expansion due to service by CSP
Operation	Need to special technique to operate	Easy to operate by CSP

위의 방법을 통해 자주 일어나는 Data Hacking 등의 문제점에 대한 예방책은 다음 Table 7과 같다.

Table 7. Check Items & Validation Methods

Item	Weak Point	Method
Endpoint	SPAM, Malware	Control Plane + Data Plane
Network	Contents Hacking, IP deodorization	Control Plane + Data plane + AD & MFA

4. 결론

클라우드 컴퓨팅 환경은 다양한 서비스를 제공함으로써 사용자에게 편리성을 주는 부분이 있지만, 그만큼 외부의 공격에 있어서는 On-Premise 형태의 시스템에 비해서 데이터 탈취가 쉬운 부분이 있다. 특히 대부분의 기업들이 VPN을 사용해서 사내 시스템과의 연계를 하지만, 이는 보안성 측면에서 가장 취약한 형태의 구성으로 인해 제로 트러스트 네트워크 형태의 구조에 비해서 많은 문제점을 가지고 있다. 금번 연구에서는 VPN이 아닌 ZTN기반에서의 설계를 통해 사용자 인증과 네트워크 보안성 부분에 많은 개선이 있음을 알 수 있다. 향후 이 과제를 더욱더 발전시켜 다음의 연구를 진행하고자 한다.

첫째, 다양한 CSP간의 구성을 통해 멀티클라우드 컴퓨팅 환경으로 연구를 강화하고자 한다. 기업 입장에서는 클라우드 비용을 줄이고 특정 CSP에게 Lock-in 되지 않는 장점이 있는 멀티 클라우드로의 전환이 가속화되고 있기 때문이다. 둘째, 본 연구에서는 기본적으로 업무를 위한 디바이스의 형태로 PC 기반을 중점으로 설계를 하였다. 향후에는, 다양한 디바이스의 형태와 OS지원이 가능한 확장성을 확보하도록 하고자 한다. 마지막으로는 인증 부분에 있어서 보다 강력한 통제를 위해 Enclave-Gateway based Model을 써서 설계를 했지만, 고속 처리가 가능하면서 관리자 입장에서 관리가 쉬운 모델링을 적용해서 개선해보고자 한다.

References

[1] Microsoft Corporation, MS Cloud Migration Check List, 2022, Available from: https://azure.microsoft.com/en-us/migration/cloud-migration/checklist/ (accessed May. 15, 2023)

[2] Seo Cheong Jeong, Case Study on Samsung Electronics' Untack Office Environment for Remote First, *MS Azure Everywhere*, pp. 3-6, 2021, Available from: https://www.youtube.com/watch?v=l04ad8fkens (accessed May. 15, 2023)

[3] Lee Sang Ho, Study on Cloud Computing Security Measures, *Journal of Business Convergence Society* Vol.5 No.1, pp. 31-35, 2015. https://scienceon.kisti.re.kr/srch/selectPORSrchArticle.do?cn=JAKO201524236535208&dbt=NART

[4] Kim Jong Cheol, Min Young Gi, Seo Bo Kuk, Jung Hyun Cheol, Jung Gi Bong, Result of a security vulnerability check on cloud solutions and services using cloud services and how to improve security reliability, *Journal of Korea next computing society* Vol.16 No.1, pp. 56-64, 2020.02. https://www.earticle.net/Article/A370552

[5] Park Sang-Kil, Kim Gi-Bong, Son Gyeng-Ja, e Won-Suk, Park Jae-Pyo, A study on a security model for the establishment of a non-face-to-face smart work working environment in a physical network separation environment of public, *Journal of Korea convergence society*, Vol.11, No 10, pp.37-44, 2020.10. https://www.earticle.net/Article/A383167

[6] John Kindervag "No More Chewy Centers: Introducing The Zero Trust Model of Information Security", Forrest Research. 2010.09.

[7] Techradar, ZTNA vs VPN : What are the Differences, Richard Sutherland, Available from: https://www.techradar.com/versus/ztna-vs-vpn-what-are-the-differences (access May. 15. 2023)

[8] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, Zero Trust Architecture, 2020.08.

[9] Technical Committee ISO/IEC JTC 1/SC 27, ISO/IEC 27001:2013 Annex A , 2013.10.

[10] Technical Committee ISO/IEC JTC 1/SC27, ISO/IEC 27017:2015 Annex A , 2015.12.

[11] Jason Garbis, Jerry W. Chapman, Zero trust Security : An Enterprise Guide, Apress, 2021.02.

서 청 정(Cheong Jeong Seo) [정회원]

- 2008년 2월 : 한국과학기술원 전산학과 (공학석사)
- 2021년 9월 ~ 현재 : 명지대학교 보안경영공학과 박사과정
- 1997년 1월 ~ 2021년 12월 : 삼성전자 정보전략그룹 파트장
- 2022년 1월 ~ 현재 : 이테크시스템 소프트웨어 기술사업부장
- 2022년 1월 ~ 현재 : 명지대학교 방산안보연구센터 객원연구원

〈관심분야〉
클라우드 보안, AI, 정보통신