https://doi.org/10.33778/kcsa.2024.24.1.021

보안성 강화를 위한 ZTNA운영 개선방안 연구★

유 승 재*

요약

이전의 네트워크 환경에서의 보안모델은 신뢰를 기반으로 하는 Perimeter모델을 사용하여 일단 신뢰된 사용자에게 대한 리소스 접근통제가 적절하게 이루어지지 못하는 취약점이 존재해 왔다. Zero Trust는 내부 데이터에 액세스하는 사용자와 장치가 어느 것도 신뢰할 수 있는 것이 없다고 가정하는 것을 절대적 원칙으로 한다. Zero Trust 원칙을 적용하면 조직의 공격 표면을 줄이는 데 매우 성공적이며, 또한 Zero Trust를 이용하면 세분화를 통해 침입을 하나의 작은 영역으로 제한하여 공격이 발생했을 때 피해를 최소화하고 할 수 있다는 평가를 받고 있다. ZTNA는 조직에서 Zero Trust 보안을 구현할 수 있도록 하는 주요 기술로서 소프트웨어정의경계(SDP)와 유사하게, ZTNA는 대부분의 인프라와 서비스를 숨겨서 장치와 필요한 리소스 간에 일대일로 암호화된 연결을 설정한다, 본 연구에서는 ZTNA 아키텍처의 원칙이 되는 기능과 요구사항을 검토하고, ZTNA 솔루션의 구축과 운영에 따른 보안요구사항과 검토사항에 대해 연구한다.

A Study on the Improvement of Security Enhancement for ZTNA

Seung Jae Yoo*

ABSTRACT

The security model in the previous network environment has a vulnerability in which resource access control for trusted users is not properly achieved using the Perimeter model based on trust. The Zero Trust is an absolute principle to assume that the users and devices accessing internal data have nothing to trust. Applying the Zero Trust principle is very successful in reducing the attack surface of an organization, and by using the Zero Trust, it is possible to minimize damage when an attack occurs by limiting the intrusion to one small area through segmentation. ZTNA is a major technology that enables organizations to implement Zero Trust security, and similar to Software Defined Boundary (SDP), ZTNA hides most of its infrastructure and services, establishing one-to-one encrypted connections between devices and the resources they need. In this study, we review the functions and requirements that become the principles of the ZTNA architecture, and also study the security requirements and additional considerations according to the construction and operation of the ZTNA solution.

Key words : ZTNA, SDP, Network Security

접수일(2024년 02월 22일), 수정일(2024년 03월 29일), 게재확정일(2024년 03월 30일)

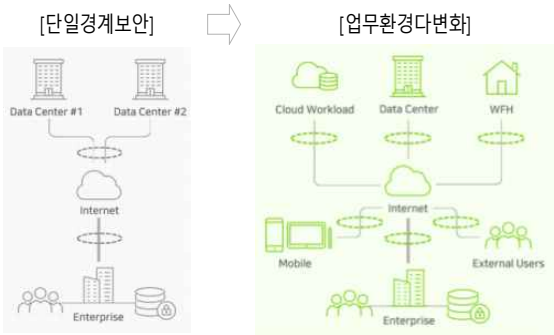
★ 이 논문은 2023년도 중부대학교 학술연구비 지원에 의하여 이루어진 것임

* 중부대학교/정보보호학과

1. 서론

ZTNA(Zero Trust Network Access)는 제로트러스트 보안 모델의 일환으로, 기존의 VPN(Virtual Private Network)이나 네트워크 기반의 접근제어시스템과는 다르게, 네트워크 리소스에 대한 접근을 검증하고 허가하는 접근제어방식으로 네트워크 내부와 외부 모두에서 작동한다.[5,6] 이전의 네트워크 환경은 모든 위협이 조직 외부에서 발생하며 내부 네트워크에 액세스할 수 있는 모든 사용자를 신뢰할 수 있다고 가정하고 네트워크 경계에 보안 솔루션을 배포하여 모든 인바운드 및 아웃바운드 트래픽을 검사하고 공격자는 외부에, 조직의 중요한 데이터는 내부에 보관하는 것으로 간주하였다.[4]

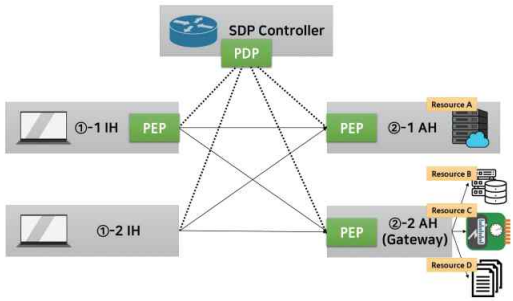
이는 신뢰를 기반으로 하는 Perimeter모델을 사용하여 일단 신뢰된 사용자 즉 네트워크 내부에 접근하는 사용자에게 너무 많은 권한을 부여하는 것을 제한하지 않음으로써 리소스에 대한 안전하고 적절한 접근통제 구현에 어려운 측면이 노출되어 왔다. 더욱이 현재의 추세인 원격이나 클라우드 및 분산형 업무환경에서는 기존의 신뢰기반의 단일 경계보안모델인 Perimeter모델이 더 이상 효과적이지 못하다는 인식이 광범위하게 확산되어 왔다.



※ 요인 : 비용증가 / 운영복잡성증가 / 보안위협증가

<그림 1> 보안 모델의 한계와 변화 [1]

이에 대한 보완 방안으로서 설계된 소프트웨어 정의경계솔루션(SDP)은 사용자 ID를 기반으로 승인된 사용자만 리소스에 액세스할 수 있도록 제한하여 조직의 위협 표면과 사이버 위험에 대응하고자 하는 프레임워크이다. MFA등의 강력한 사용자 인증과 디바이스인증, 제로트러스트 적용 그리고 리소스에 대한 보안 액세스 등의 기능을 통해 원격 업무나 클라우드 환경에서 노출될 수 있는 많은 보안위협에 효과적인 대응방안을 제공하였다.



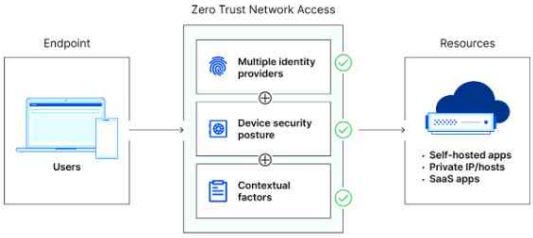
<그림2>SDP기반 제로트러스트 아키텍처구성도[7]

<그림2> 구성도는 제로트러스트 접근제어를 위한 주요 컴포넌트인 정책결정지점(Policy Decision Point)를 SDP Controller가 그리고 리소스 또는 리소스 게이트웨이(Accepting Host, AH)가 정책시행지점(Policy Enforcement Point)역할을 수행한 모델이다[7].

SDP접근방식과 유사하게 ZTNA는 조직 내에 이미 위협이 존재한다는 가정에 따라 구축된 보안 접근 방식으로 사용자, 기기, 애플리케이션이 자동으로 신뢰하는 것이 아니라 네트워크의 모든 요청에 따라 엄격한 신원확인이 적용되도록 구현한다. 이를 위해 기본적으로 요구되는 보안원칙으로는 최소권한의 원칙, 디바이스 액세스 제어, 지속적인 모니터링 및 유효성, 내부망 이동방지, 다단계인증(MFA) 등을 있다.[2]

< 그림3>와 같이 ZTNA는 사용자, 기기, 애플리케이션 등에 대한 신원 확인과 권한 부여를 통해 접근을 관리하게 하는데, 사용자가 실제로 필요로 하는 리소스에만 접근할 수 있도록 제한함에 있어서 기본적으로 '신뢰하지 않는다(Trust No One)'는 원칙에 따라 기업 내부와 외부를 모두 신뢰하지 않으며, 모든 접근 시도에 대해 신원을 검증하고 권한을 부여하는데, 그 보안 아키텍처 구축의 핵심 원칙은 다음과 같이 정리할 수 있다.

- 마이크로세그먼테이션: 네트워크를 작은 세그먼트로 분할하여 접근을 제어함으로써 보안을 강화
- 제로트러스트 인증: 사용자의 신원을 확인하고 디바이스의 보안 상태를 평가하여 접근을 승인 또는 거부
- 애플리케이션 중심의 접근 제어: 리소스마다 다른 수준의 접근 권한을 부여함으로써 보안을 강화
- 인텔리전스 기반 접근 제어: 실시간으로 위협을 탐지하고 대응함으로써 보안을 유지



<그림3> ZTNA액세스 제어[4]

이러한 ZTNA는 사용자 및 기기의 신원을 항상 검증하고 필요한 권한을 제공하는 접근관리 함으로써 펜데믹 이후 확산되는 원격업무에서의 접근 통제에 효율적 대응방안을 지원하고, 특히 클라우드 및 분산형 환경에서의 효율적 업무지원과 보안성 강화를 위한 민첩성과 유연성을 제고한다. 또한 사용자, 디바이스, 애플리케이션 간의 상호작용을 모니터링하고 평가하도록 함으로써 보안 위협 식별과 위험관리에 유용하게 작용하는 측면이 있다. 아울러 컴플라이언스 유지를 위해 시스템적으로 엄격한 데이터 보호 및 개인정보 보호를 위한 규정 및 규제 요구를 적용하고 준수하도록 설정하여 운영할 수 있다.[4]

이렇듯 ZTNA의 보안 강화, 사용자 경험 향상, 민첩성 및 유연성 제공, 위험 관리, 그리고 컴플라이언스 준수 등 기업 운영상의 공통적인 니즈를 충족시킬 수 있는 프레임워크로 인식되고 있다.

본 연구에서는 클라우드 및 분산 환경에서 요구되는 제로트러스트 프레임워크에 대해 그 구성과 보안요구사항 등에 대해 살펴본다. 아울러 ZTNA 도입운영에 따른 문제점과 보완사항을 점검하고 보다 안전한 ZTNA 구현에 대한 방안을 제시한다.

2. 관련연구

2.1 ZTNA 보안모델

ZTNA는 제로트러스트 보안모델을 구현하는 기술로써 네트워크 내부와 외부 모두에 존재할 수 있는 위협에 대응하기 휘하여 모든 사용자와 모든 장치에 대해 내부 리소스에 대한 액세스 권한을 부여하기 전에 엄격한 검증을 요구하도록 설계한다.[9]

SDP 접근방식과 마찬가지로 ZTNA에서는 연결된 디바이스에서 연결된 대상 이외의 그 어떤 네트워크 리소스(애플리케이션, 서버 등)에 접근하거나 인식하지 못하도록 한다.

2.2 상용화 ZTNA 솔루션

상용화된 ZTNA 솔루션들은 조직의 요구사항과 환경을 고려하여 도입하는 경우 다양한 기능과 유연성을 제공으로 조직들이 제로트러스트 보안 모델을 쉽게 구현하고 네트워크 보안을 강화할 수 있다. 사용자의 신원을 확인하고 접근을 관리하기 위한 제로트러스트 보안 모델을 구현하는 일부 주요 상용화된 ZTNA 솔루션들의 알려진 특징을 살펴보면 다음과 같다.[8]

- Cisco Secure Access Service Edge(SASE): Cisco의 SASE는 클라우드 기반의 보안 서비스를 통해 사용자의 위치와 상관없이 네트워크 접근을 제어 (VPN과 ZTNA를 지원하는 통합 클라이언트)
- Palo Alto Networks Prisma Access: Palo Alto Networks의 Prisma Access는 클라우드 기반의 보안 서비스로서 ZTNA 구현 (ZTNA, 보안 웹 게이트웨이, 서비스형 방화벽 등이 통합된 형태)
- Zscaler Private Access: Zscaler Private

Access는 클라우드 기반의 보안 서비스로서 모든 사용자와 기기트래픽에 대한 포괄적인 가시성과 통제 및 일관된 보안 지원(자동화된 사용자-애플리케이션 액세스 분할을 위한 AI 생성 정책이 적용)

- Akamai Enterprise Application Access: Akamai의 Enterprise Application Access는 사용자의 위치와 디바이스를 고려하여 접근을 관리하고 보호(브라우저를 통해 보호된 애플리케이션에 액세스 및 클라이언트 기반 툴도 지원)
- Microsoft Azure Active Directory (Azure AD) Conditional Access: Microsoft Azure AD의 Conditional Access는 클라우드 기반의 접근 제어 서비스로서 ZTNA를 구현(사용자의 신원과 리소스에 대한 조건을 기반으로 접근을 관리)
- Citrix Secure Access: Citrix의 Secure Access는 사용자가 원격으로 안전하게 접근할 수 있도록 제어(VPN, 가상 데스크톱, Citrix EB, 서비스형 데스크톱 제품과 호환, 클라우드는 물론 온프레미스 방식을 지원)
- Cloudflare Access: Cloudflare Access는 클라우드 기반의 접근 제어 솔루션으로서, 사용자의 신원과 위치에 따라 접근을 제어(인터넷 트래픽에 대한 인사이트로 학습시킨 머신러닝 알고리즘을 기반으로 ZTNA구현)
- VMware Workspace ONE Access: VMware의 Workspace ONE Access는 다양한 애플리케이션에 대한 신뢰할 수 있는 접근을 제공(제로트러스트 보안 모델을 준수하여 사용자의 신원과 기기 상태를 기반으로 접근을 관리)
- Proofpoint Meta Access: Proofpoint Meta Access는 클라우드 기반의 접근 제어 및 보안 솔루션(사용자의 신원을 확인하고 접근을 제어하며 모든 애플리케이션에 대한 안전한 접근을 제공)
- Barracuda CloudGen Access: Barracuda의 CloudGen Access는 클라우드 기반의 보안 서비스로서 제로트러스트 보안 모델을 구현(사용자의 신원을 검증하고 접근을 관리하여 네트워크 보안을 강화)
- ZTES(BeyondCorp Zero Trust Enterprise Security): Google의 비욘드콥 (Background에서 추가적인 SW나 Agent를 구동할 필요가 없기 때문에 복잡성을 줄여주고 신속한 roll-out이 가능)

아울러 국내에서도 LG CNS Smart Work Gateway, NHN Security Penta Security Systems, SK텔레콤 CIC Zero Trust Platform, 알테어 Altair SecureAccess, 아이티즈스메트릭스 iITZ ZTNA 등 다양한 상용화된 ZTNA솔루션이 제공되고 있는 것으로 조사된다.

3. 안전한 ZTNA 구축을 위한 이슈

3.1 ZTNA의 보안취약점

ZTNA는 전통적인 네트워크 보안 모델에 비해 많은 이점을 제공하지만, 여전히 일부 보안 취약점이 존재할 수 있다. 주요한 ZTNA 보안 취약점을 살펴보면 다음과 같다:

- 인증 취약점: ZTNA는 사용자의 신원을 확인하는 데 중요한 역할을 하지만 그러나 약한 인증 매커니즘 또는 인증 데이터의 유출로 인한 취약점은 인증 과정을 우회하거나 위조된 신원으로 접근을 시도하는 공격에 이어질 수 있다.
- 접근 제어 취약점: ZTNA에서 사용자에게 부여된 접근 권한을 효과적으로 관리하지 못할 경우, 비인가된 사용자가 리소스에 접근할 수 있다. 또한, 애플리케이션 및 서비스를 보호하지 않고 공격자가 악의적으로 접근할 수 있는 취약점이 있을 수 있다.
- 네트워크 및 트래픽 분석 취약점: ZTNA 솔루션은 네트워크 트래픽을 분석하여 비정상적인 활동을 탐지하고 대응해야 하는데, 사전에 탐지하지 못한 취약점이 있을 경우에는 여전히 이로 인해 공격자가 네트워크 내에서 의도치

않은 활동을 수행할 수 있다.

- 암호화 취약점: ZTNA에서 사용되는 암호화 기술에 취약점이 있다면, 공격자가 암호화된 통신을 해독하여 중요한 데이터를 노출시킬 수 있다.
- 서비스 및 구성 관리 취약점: ZTNA 솔루션의 서비스 및 구성 관리 시스템에 취약점이 있는 경우, 공격자가 서비스를 비정상적으로 수정하거나 중단시킬 수 있다.

3.2 안전한 네트워크 보안

클라우드 기반 네트워크 보안은 그것이 어디에 있든 리소스를 보호하기 위해 구축되어야 한다. 이것을 위해 필수적으로 점검해야 하는 항목을 다음 체크리스트에서 볼 수 있다.[3]

- 네트워크 아키텍처 매핑 : 사용자 장치, 온프레미스 서비스 및 어플라이언스, 클라우드 서비스 등
- 요구사항 평가 : VPN 교체, 클라우드 방화벽, 제로 트러스트 솔루션, DNS 필터링, 장치 상태 확인 등
- MFA로 SSO 활성화
- 그룹 액세스 정책 정의
- 규정 준수 요구사항 정의

위의 평가를 기반으로 한 프레임워크인 ZTNA는 표준 로그인 및 MFA 인증을 사용하는 애플리케이션 수준뿐만 아니라 상태 확인, 시간 및 위치와 같은 상황 기반 권한을 활용하는 장치 수준에서 회사 리소스를 보호한다. 따라서 ZTNA 아키텍처는 다음의 사항을 기본원칙으로 고려할 필요가 있다[3].

- 애플리케이션액세스를 네트워크 액세스와 별도로 취급
- IP 주소를 네트워크에 노출금지
- 장치의 위험 및 보안상태를 액세스결정의 요소로 통합
- 사용자 위치, 요청시기 및 빈도, 요청되는 앱 및 데이터 등의 추가 요소와 관련된 위험을 평가
- MPLS 기반 WAN 연결 대신 TLS를 통해 암호화된 인터넷 연결을 사용

3.3 ZTNA 솔루션의 추가적인 보안요구사항

상용화된 ZTNA 솔루션은 많은 이점을 제공하지만, 일반적으로 다음의 몇 가지 한계와 추가적인 보안 요구사항이 제기된다.

- 복잡성과 운영비용: ZTNA 솔루션을 구현하고 운영하는 것은 복잡할 수 있고, 네트워크 구조와 사용자 인프라에 맞게 구성하고 유지보수하기 위한 전문적 지식과 경험이 요구되며 이에 따른 운영비용이 추가될 수 있다.
- 성능과 지연 : ZTNA 솔루션은 사용자의 신원을 확인하고 접근을 제어하기 위해 추가적인 인증 및 권한 검증 단계를 거치므로, 일부 경우에는 성능 저하와 지연이 발생할 수 있다.
- 유저 경험: 추가적인 보안 절차가 유저경험을 저하시킬 수 있고, 너무 많은 인증 단계나 권한 요청은 사용자들이 업무에 지장을 초래할 수 있다.
- 전환 및 통합 문제: 기존의 네트워크 인프라나 보안 시스템을 ZTNA 솔루션으로 전환하는 것은 복잡할 수 있고, 또한 다른 보안 솔루션과의 통합도 고려되어야 한다.
- 신뢰된 디바이스와 보안 업데이트: ZTNA는 사용자의 디바이스의 보안상태를 고려하여 접근을 허용 또는 차단하며 이를 위해서는 신뢰된 디바이스의 확인 및 보안 업데이트가 요구된다.
- 다양한 접근 포인트: 클라우드, 모바일, IoT 등 다양한 접근 포인트를 고려하여 ZTNA 솔루션을 구현해야 하는데, 이러한 다양성은 보안요구를 더욱 복잡하게 만들 수 있다.

4. 결론

비즈니스의 목표는 기업의 보안을 강화하는 동

시에 사용자의 편의성을 유지하는 것이기 때문에 이러한 한계와 추가적인 보안 요구사항을 고려하여 조직은 ZTNA 솔루션을 선택하고 구현할 때 전략적으로 접근해야 한다.

이에 ZTNA의 보안 취약점 개선을 위한 방안을 다음과 같이 제시할 수 있다.

- 인증 강화: 더 강력한 인증 매커니즘을 도입하여 사용자의 신원을 보다 안전하게 확인할 수 있다. 이중 인증(2FA)이나 다단계 인증(MFA)과 같은 추가적인 인증 요소를 도입하여 보안을 강화할 수 있다.
- 액세스 제어 강화: 사용자의 접근 권한을 더욱 엄격하게 관리하여 비인가된 접근을 방지할 수 있다. 접근통제의 기본원칙인 최소 권한 원칙을 적용하고 접근 권한의 범위를 정확히 제어한다.
- 보안 감시 및 분석: 네트워크 트래픽을 실시간으로 모니터링하고 비정상적인 활동을 식별하는 보안 감시 시스템을 구축하여 즉각적으로 대응할 수 있도록 한다. 이를 통해 신속한 대응과 취약점의 식별을 가능하게 한다.
- 암호화 강화: 강력한 암호화 기술을 적용하여 데이터의 안전한 전송을 보장한다. 최신의 암호화 표준 및 프로토콜을 채택하여 데이터 보호 수준을 높인다.
- 정기적인 보안 검토 및 평가: ZTNA 솔루션 및 관련 보안정책 및 절차를 정기적으로 검토·평가하여 발견된 취약점을 해결하고 보안 수준을 유지한다. (외부전문가에 의한 감사와 평가 및 피드백 가능)
- 사용자 교육 및 인식 제고: 사용자에게 보안의 중요성을 교육하고 인식시킴으로써 사회 공학 공격 및 사용자 실수에 의한 보안 위협을 줄일 수 있다.

이러한 개선 방안을 통해 ZTNA 솔루션의 보안 취약점을 줄이고 더욱 견고한 보안을 확보할 수 있다. 종합적인 접근 방식과 지속적인 보안 관리가 필요하다.

참고문헌

[1] Genians, “글로벌 보안 버즈워드(Buzzword), 제로 트러스트, EDR 그리고 확장된XDR”. https://www.genians.co.kr/blog/trend_zt_xdr

[2] CLOUDFLARE, “Zero Trust아키텍처로 이어지는 로드맵”, 2022.

[3] Harmony SASE, “NETWORK SECURITY MUSTS CHECKLIST” CHECK POINT.

[4] CLOUDFLARE, “Zero Trust 네트워크 액세스란?” https://www.cloudflare.com/ko-kr/learning/access-management/what-is-ztna/

[5] 이다인 외1인, “제로트러스트원리를반영한보안강화요소기술적용방안연구” 융합보안논문지 제22권제3호 pp.1-9, 2022.

[6] 박원형, “제로트러스트 보안 모델에서 보안관제 시스템강화 연구” 융합보안논문지 제22권제2호 pp.51-57, 2022.

[7] 제로트러스트가이드라인 1.0, 제로트러스트포럼, 2023

[8] Josh Fruhlinger,“원격액세스보안업그레이드” ZTNA 솔루션17종 선택가이드, Net World, 2023.

[9] ‘Enabling Zero Trust Security with VMware Workspace ONE’, WHITE PAPER - OCTOBER 2019.

〔저자소개〕

유 승 재 (Seung-Jae Yoo)
1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교 정보보호학과 교수
email : sjyoo@joongbu.ac.kr