2024
-08

네트워크 보안 기술서

대표이사: 선영주

한라 KPC 漢拏

목차

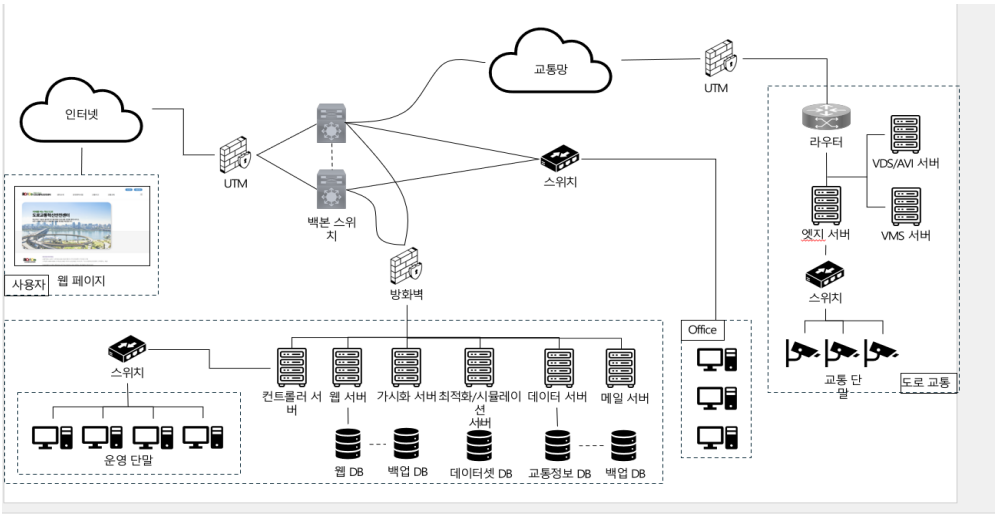
1 네트워크 구성도 개선 배경

도로교통혁신안전센터(ROADo) 측에서 공공기관의 네트워크 보안을 강화하기 위해 On-premise 환경의 기존 네트워크 구성의 문제점을 분석하고, 이를 바탕으로 개선된 네트워크 모델을 제안하는 것을 요청했다. 이 기술서의 목적은 기존 네트워크의 문제점을 철저히 검토한 후, 보안 강화를 위한 핵심 요소와 적용 가능한 최첨단 기술들을 제시하는 데 있다.

특히, 스마트 신호등 도입 등으로 인해 교통망이 향후 민간기관의 클라우드인 SaaS(Software as a Service) 환경으로 전환될 예정인 점을 고려하여, 본 기술서에서는 도로교통혁신안전센터의 On-premise 환경 내 내부망 구성과 외부와의 통신 시 보안성을 극대화할 수 있는 네트워크 구성을 집중적으로 다룬다. 아울러, 현재 네트워크 구조에 추가로 도입이 요구되는 네트워크 보안 장비들을 상세하게 비교 분석하여, ROADo의 보안 요구 사항에 최적화된 솔루션을 제안하고자 한다. 이를 통해, ROADo의 네트워크 보안을 한층 강화하고, 지속 가능한 보안 체계를 구축할 수 있는 전략적 방향을 제시하고자 한다.

2 기존 네트워크 구성의 문제점

다음은 도로교통혁신안전센터에서 제시한 기존의 네트워크 구성모델이다.



[그림 1] ROADo의 기존 네트워크 구성도

2.1. 웹서버의 내부망 배치

현재 ROADo의 웹페이지 서버는 내부망에 배치되어 있어, 외부 사용자가 접근할 때 외부로부터의 공격에 쉽게 노출될 수 있는 구조다. 이러한 배치는 외부 공격자가 내부망으로 침투할 수 있는 통로를 제공하며, 내부망 전체의 보안성을 저하시킬 수 있다. 특히, 외부 사용자가 운전면허교육 서비스나 교통교육 서비스를 신청할 때 개인정보를 입력하게 되는데, 이러한 민감한 정보가 내부망에서 처리됨에 따라 보안 위협이 상당히 높아진다. 이로 인해 악의적인 공격자가 내부에 위치한 웹서버를 경유하여 다른 중요 서버로 접근할 가능성도 배제할 수 없으며, 이는 전체 시스템의 보안에 심각한 취약점을 초래할 수 있다.

2.2. 구성상의 망 분리 미적용

국가정보원의 국가정보보안 기본지침 제40조에 따르면 공공기관은 망 분리를 의무화하고 있다. 이는 2006년 공공기관 망 분리 의무화 시행과 2007년 행정안전부와 국가정보원의 업무 전산망 분리 지침 발표 이후, 현재까지 공공기관의 필수적인 보안 조치로 자리잡았다. 물리적 망 분리는 업무망과 인터넷 망을 물리적으로 분리하여, 망 간 접근경로를 원천적으로 차단하는 방식이다.

그러나 현재 ROADo의 네트워크 구성을 살펴보면, 망 분리에 대한 적용이 부족한 상황이다. 기관이 클라우드로의 전환을 준비 중이지만, 민감정보를 처리하는 환경에서는 물리적 망 분리가 반드시 적용되어야 한다. 특히, 현재 운전면허 서비스와 교통교육 서비스와 같은 주요 업무에서 개인정보와 같은 민감한 데이터를 처리하고 있기 때문에 망 분리의 미적용은 심각한 보안 리스크를 초래할 수 있다. 클라우드 도입과 망 분리를 병행하는 것이 어려울 수 있지만, 공공기관으로서 민감정보 보호를 위한 망 분리는 반드시 준수해야 할 보안 요구사항이다.

2.3. 통합로그 관리시스템의 부재

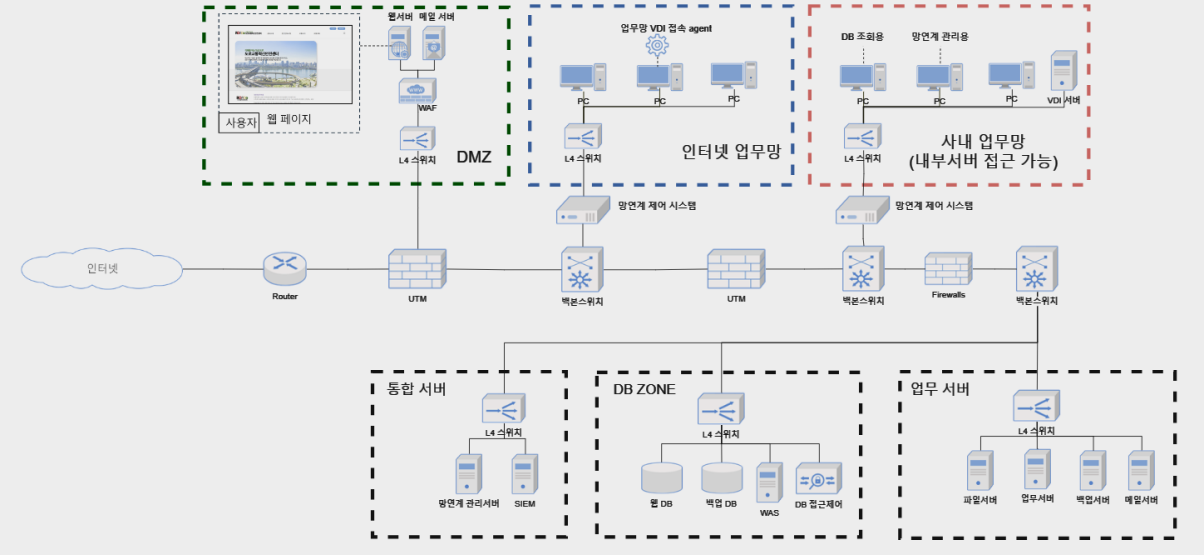
ROADo의 기존 네트워크 구성에서는 네트워크 내 다양한 시스템 및 보안 장비에서 생성되는 로그 데이터를 통합적으로 관리하고 분석할 수 있는 시스템이 부재한 상황이다. 이러한 부재는 보안 위협을 조기에 탐지하고 효과적으로 대응할 수 있는 능력을 저하시킨다. 통합로그 관리시스템(SIEM)이 없기 때문에, 보안 사고 발생 시 로그 데이터를 기반으로 한 정확한 원인 파악과 대응이 어려워져, 사건의 규모가 확대될

위험이 있다.

또한, 통합된 로그 관리 체계가 없으면 네트워크 내에서 발생하는 이상 징후를 실시간으로 모니터링하고 즉각적으로 대응할 수 있는 능력이 부족해지며, 이는 보안 사고를 미연에 방지하기 위한 사전적 대응 능력을 약화시키는 결과를 초래할 수 있다. 이러한 상황에서 SIEM의 도입은 필수적이며, 보안 사고 발생 시 신속하고 정확한 대응을 가능하게 하는 중요한 보안 요소로 작용할 것이다.

3 개선된 네트워크 구성 상세설명

다음은 기존의 네트워크 구성도에서 발견된 보안 취약점을 해결하고자 개선한 네트워크 구성도이다.



[그림 2] 개선된 네트워크 구성도

3.1. DMZ (Demilitarized Zone) 구성

외부 사용자가 접근하는 웹페이지 서버와 외부 기관과의 자료 공유를 위한 메일 서버를 DMZ 영역에 배치해, 외부로부터의 접근을 통제하면서도 내부망과는 완전히 격리된 구역에서 운영되도록 구성했다. 이를 통해 외부 공격 발생 시 내부망으로의 침투를 원천적으로 차단할 수 있다. DMZ 구역에서는 웹 애플리케이션 방화벽(WAF)을 활용해 웹 서버에 대한 다양한 공격을 실시간으로 방어하며, L4 스위치를 통해 부하 분산 및 트래픽 제어를 수행하도록 설계했다. 이로 인해 SQL 인젝션, 크로스 사이트 스크립팅(XSS) 등의

고도화된 웹 공격으로부터 시스템을 보호하고, SSL/TLS 암호화를 적용해 데이터 전송의 안전성을 확보할 수 있다.

3.2. 망분리 적용

외부 인터넷 업무망과 사내 업무망을 물리적, 논리적으로 완전히 분리해 망 분리를 구현했다. 인터넷 업무망은 외부 인터넷에 접속할 수 있지만, 내부망과는 철저히 분리되어 있어 외부로부터의 접근이 원천적으로 차단된다. 그러나 긴급한 상황에서 인터넷 업무망의 PC에서 사내 업무망에 접근해야 할 필요가 있을 경우를 대비해, 사내 업무망에 VDI(Virtual Desktop Infrastructure) 서버를 배치했다. 이를 통해 인터넷이 가능한 PC에서 업무용 VDI 접속 에이전트를 통해 사내 업무망으로 제한적 접근이 가능하도록 하였으며, 이때도 내부 서버망으로의 접근은 엄격히 제한된 환경을 유지한다.

사내 업무망은 사내의 업무를 위한 전용 네트워크로, 업무 서버 페이지에 접근할 수 있고, 사용자의 직무와 부서에 따라 일부 내부 서버와의 연결이 허용된다. 개인정보를 처리하는 부서는 DB 조회용 시스템에 접근할 수 있으며, 정보보안부서는 인터넷 PC와 업무망 PC 간의 파일 전송을 관리하고 승인할 수 있는 망 연계 관리 서버와 통합로그 관리시스템(SIEM)에 접속할 수 있다. 이러한 네트워크는 방화벽을 통해 접근 통제 정책에 따라 엄격히 관리되며, 허가된 자만이 네트워크에 접근하고 허가된 작업만 수행할 수 있도록 권한 리스트를 관리하며 이를 방화벽 정책에 적용한다. 사용자의 권한은 6개월마다 평가되어, 필요한 경우 조정된다. 이와 같은 구성으로 사내망 사용자는 정당한 권한을 부여 받은 자만이 내부 업무망을 통해 데이터베이스(DB) 등에 접근할 수 있다.

3.3. 망 연계 시스템 적용

인터넷 업무망과 사내 업무망 간의 보안성을 유지하면서도 필요한 정보의 연계를 원활히 할 수 있도록 망 연계 시스템을 적용했다. 인터넷 업무망과 사내 업무망 사이의 정보 교환은 반드시 정보보안부서의 승인을 거친 후에만 가능하도록 구성해, 정보 유출 위험을 최소화했다. 망 연계 시스템은 보안 통제 기능을 통해 인터넷망과 업무망 간의 데이터 전송을 안전하게 관리하고, 비인가 데이터 전송을 차단한다. 이를 통해 내부 정보의 유출 방지와 데이터 무결성을 보장하며, 시스템은 다양한 보안 정책을 적용해 외부 접근을 철저히 통제하고, 데이터 송수신 과정에서 실시간으로 위협을 탐지하고

차단하는 역할을 한다.

3.4. 통합로그관리시스템(SIEM) 도입

다양한 시스템 및 보안 장비들에서 생성되는 로그 데이터를 실시간으로 수집, 저장, 분석할 수 있는 통합로그관리시스템(SIEM)을 도입해 보안 위협을 사전에 탐지하고 대응할 수 있는 능력을 강화하고자 한다. SIEM은 각종 이벤트와 로그 데이터를 분석해 이상 징후를 탐지하며, 이를 통해 보안 사고 발생 시 신속하고 정확한 대응이 가능하다. 이 시스템은 망 연계 관리 서버와 연동되어 모든 네트워크 활동을 실시간으로 모니터링하며, 필요 시 관리자에게 경고를 발송한다. 이를 통해 잠재적인 보안 위협에 대한 대응 속도가 크게 향상되어 보안 사고로 인한 피해를 최소화할 수 있다.

3.5. 네트워크 장비배치

외부 인터넷으로부터의 접근은 라우터와 1차 UTM 장비를 통해 제어되며, 이 장비들은 외부 위협을 실시간으로 탐지하고 방어한다. 이후 DMZ로 접근하는 트래픽을 처리하며, 내부망으로 유입되는 패킷은 1차 백본 스위치로 이동한다. 1차 백본 스위치에서는 인터넷 업무망으로의 접근을 허용하며, 이후 2차 UTM과 2차 백본 스위치를 거쳐 사내 업무망으로의 접근이 이루어진다. 사내 업무망으로 접근하는 트래픽은 방화벽을 통과한 후 내부 서버망으로 이동하며, 최종적으로 3차 백본 스위치를 통해 각각의 서버 구역으로 분배된다. 네트워크의 각 구역(DMZ, 인터넷 업무망, 사내 업무망, 내부 서버망)은 L4 스위치를 통해 상호 연결되어 부하 분산과 트래픽 제어가 효율적으로 이루어진다. 이와 같은 계층적 네트워크 장비 배치를 통해, 외부와 내부의 모든 트래픽을 철저히 관리하고 보안성을 극대화할 수 있다.

4 개선된 네트워크 구성으로 인한 기대효과

도로교통혁신안전센터의 네트워크 구성을 개선함으로써 공공기관의 보안 강화와 네트워크 운영의 효율성을 동시에 실현할 수 있다.

우선, 웹 서버와 같은 외부 서비스용 시스템을 DMZ에 배치해 외부 공격으로부터 내부망을 철저히 격리할 수 있다. DMZ 내에 웹 방화벽(WAF)을 구축해 웹

애플리케이션에 대한 공격을 실시간으로 방어하고, 외부에서 내부망으로의 직접적인 접근을 차단해 보안 수준을 크게 향상시킬 수 있다. 외부 인터넷으로부터 내부망으로의 접근은 다수의 보안 장비(라우터, UTM, 백본 스위치 등)를 통해 계층적으로 제어되며, 이를 통해 각 보안 장비가 상호 보완적으로 작동하여 외부 위협을 탐지하고 차단하는 다층 방어 구조를 강화할 수 있다.

또한, 외부 인터넷망과 내부 업무망을 완전히 분리해 외부로부터의 불법적인 접근을 원천적으로 차단할 수 있다. 이로 인해 내부의 중요한 정보가 외부 공격에 노출되는 것을 방지할 수 있으며, 정보 유출 가능성을 최소화할 수 있다. 동시에, 망 연계 시스템을 통해 외부 인터넷망과 내부 업무망 간의 데이터 교환이 필요한 경우에도 엄격한 보안 정책을 적용해 안전하게 데이터를 전송할 수 있어, 업무 효율성을 유지하면서도 보안성을 확보할 수 있다. 이는 외부와의 정보 교류가 필수적인 공공기관에서 특히 중요한 요소이다.

마지막으로, 통합로그관리시스템(SIEM)을 도입해 네트워크 내 모든 시스템과 보안 장비에서 발생하는 로그 데이터를 실시간으로 수집하고 분석할 수 있다. 이를 통해 보안 사고를 조기에 탐지하고 신속하게 대응할 수 있으며, SIEM 시스템은 실시간으로 네트워크 활동을 모니터링하고 이상 징후가 발견될 시 즉시 관리자에게 경고를 발송한다. 이를 통해 잠재적 보안 위협에 대한 대응 속도를 크게 향상시킬 수 있으며, 보안 사고 발생 시 피해를 최소화하는 데 중요한 역할을 할 것이다. 통합로그관리시스템을 통해 축적된 데이터를 기반으로 미래의 보안 위협에 대한 예측과 대응 전략을 강화할 수 있어, 지속적인 보안 강화에도 기여할 수 있다.