효율적인 방화벽 정책 관리를 위한 보조 시스템 개발

윤경섭*, 강태훈O
*인하공업전문대학 컴퓨터정보과,
O인하공업전문대학 컴퓨터정보과
e-mail: ksyoon@inhatc.ac.kr*, lord8333@gmail.comO

Developing an Auxiliary System for Efficient Firewall Policy Management

Kyung Seob Yoon*, Tae Hoon KangO
*Dept. of Computer Science, Inha Technical College,
ODept. of Computer Science, Inha Technical College

● 요 약 ●

정보통신 기술의 발달은 보안 위협의 증가라는 결과를 함께 가져왔고 국내뿐만 아니라 국외로도 보안 정책 관리에 대한 필요성이 지속적으로 강조되었다. 본 논문에서는 여러 보안 장비 중 방화벽 정책 관리를 도울 수 있는 보조 시스템을 개발하였다. 이를 위해 오픈소스 방화벽 솔루션을 가상 환경에 구축하고 방화벽 정책을 추출 및 분석하여 미 동작 정책과 중복 정책을 식별하였다. 이러한 점검 보조 도구를 정책 관리에 이용한다면 낮은 이해도로 인한 Human Error의 발생을 가능한 줄이고 그 결과, 외부 위협의 최소화를 이룰 것이라 기대한다.

키워드: 정보보안(Information Security), 방화벽(Firewall), 정책(Policy), 관리(Management)

I. Introduction

오늘날 정보통신 기술의 발달과 함께 보안의 중요성이 대두되고 있다. 서비스 규모가 커질수록 자연스럽게 물리적 장비 및 네트워크 접점 또한 증가하였으며 외부로부터의 침입이 빈번해지는 원인이 되었다[1]. 서비스 제공자들은 외부로부터의 허용되지 않은 침입을 차단하기 위해 방화벽, IDS, IPS와 같이 네트워크 입력, 출력을 통제할 수 있는 정보보호 장비를 도입하여 허용할 장비 또는 차단할 장비를 구분하기 시작했다.

이러한 정보보호 시스템 및 보안 장비 운영 결과 낮은 이해도와 Human Error로 인해 잘못 적용되었을 경우 차단되어야 할 외부 IP가 허용되어 내부의 중요 자산에 접근 후 서비스 중단, 바이러스 유포, 개인정보 유출 등 심각한 침해사고가 발생할 수 있다. 만약 현재 또는 앞으로 적용할 정책에 대한 사전 검증 및 관리적 평가를 한다면 Human Error의 발생을 줄이고 운영 및 관리적 미흡을 보완할 수 있을 것이다.

본 논문에서는 방화벽 시스템의 정책 관리를 도울 수 있는 보조 시스템을 개발하고자 한다.

II. Preliminaries

2. Related works

2.1.1 정책 관리의 필요성

자산 또는 서비스 규모가 큰 정보시스템 일수록 다수의 보안 정책이 존재할 것이다. 그 중 낮은 정책 이해도 및 Human Error로 인하여 "미사용 및 중복 정책"이 발생할 수 있는데 이것을 검토하여 제거하지 않을 경우 업무 효율성이 저하되어 네트워크 보안 체계의 약화로 이어질 수 있다. Fig. 1의 KISA(한국 인터넷진흥원)에서는 주기적인 정책 점검에 대한 중요성을 강조하고 그 기준을 제공하고 있다[2].

S-09 (상)	5. 기능관리 > 5.1 정책 관리
취약점 개요	
점검내용	■ 보안장비 정책에 미사용 및 중복된 정책이 존재하는지 점검
점검목적	■ 주기적인 정책 검토를 통해 미사용 및 중복된 정책을 제거하여 향후 발생 가능한 보안 위협을 제거하고 보안장비의 고가용성을 유지하기 위함
보안위협	■ 미사용 및 중복된 정책을 제거하지 않는 경우, 보안장비 관리자의 업무 편의성 및 효율성이 저하되며 설정되어 있는 정책 중 관리자가 인지하지 못한 정책으로 인해 네트워크 보안 체계가 약화될 수 있음
참고	※ **발생 가능한 보안 위협:** 비인가자의 네트워크 접근 및 내부 정보 유출, 악성코드 삽입 등 ※ 관련 점검 항목 : A-92(하)

Fig. 1. 주요정보통신기반시설 취약점 분석/평가 상세가이드

정보보호 업무 준수 현황을 점검하는 ISMS-P 인증심사 기준 또한 보안 정책을 포함한 정보보호 관리체계의 점검을 강조하고 있다. Fig. 2는 KISA에서 제공하는 ISMS-P 인증기준 안내서이다[3].

항 목	1.4.2 관리체계 점검
인증기준	관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.
주요 확인사항	• 법적 요구사항 및 수립된 정책에 따라 정보보호 및 개인정보보호 관리체계가 효과적으로 운영되는지를 점검하기 위한 관리체계 점검기준, 범위, 주기, 점검인력 자격요건 등을 포함한 관리체계 점검 계획을 수립하고 있는가? • 관리체계 점검 계획에 따라 독립성, 객관성 및 전문성이 확보된 인력을 구성하여 연 1회 이상 점검을 수행하고 발견된 문제점을 경영진에게 보고하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 정보통신망법 제28조(개인정보의 보호조치) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행) • 개인정보의 기술적·관리적 보호조치 기준 제3조(내부관리계획의 수립·시행)

Fig. 2. ISMS-P 인증기준 안내서

또한 Fig. 3은 관련 전문 인력 및 지식이 미흡할 수 있는 중소기업 대상으로 정보보호 정책 설정을 위한 가이드를 제공하고 있다[4].

나) 정책 설정 방법

침입차단 시스템의 접근통제 정책 설정은 제품마다 차이가 있기 때문에 제품 사용설명서를 참조하여야 하며, 필수 요구사항은 다음과 같음

<표 11-1> 침입차단 시스템 접근통제 정책

출발지 주소	출발지 포트	목적지 주소	목적지 포트	정책
외부	Any	내부메일호스트	SMTP	허용
외부	Any	내부뉴스호스트	NNTP	허용
외부	Any	내부NTP호스트	NTP	허용
외부	Any(UDP)	내부DNS호스트	DNS(UDP)	허용
Any	Any	Any	Any	거부

Fig. 3. 중소기업 정보보호 실무가이드

정책 관리에 대한 관심은 국내/외적으로도 계속되고 있다. Web Application Security를 주제로 2001년부터 현재까지 활동 중인 국제 연구 그룹 OWASP(The Open Web Application Security Project)는 주기적으로 발표하는 보안 위협 요소 Top 10에 Security Misconfiguration을 최근 2010년부터 현재까지 10년간 항상 포함하였다는 점을 고려하면 보안 장비의 정책 점검에 대한 필요성은 계속 강조되었다[5].

순위	2017	2021
1	Injection	Broken Access Control
2	Broken Authentication	Cryptographic Failures
3	Sensitive Data Exposure	Injection
4	XML External Entities(XXE)	Insecure Design
5	Broken Access Control	Security Misconfiguration
6	Security Misconfiguration	Vulnerable and Outdated Components
7	Cross-Stie Scripting(XXS)	Identification and Authentication Failures
8	InSecure Deserialization	Software and Data Integrity Failures
9	Using Components with Known Vulnerabilities	Security Logging and Monitoring Failures
10	Insufficient Logging & Monitoring	Server-Side Request Forgery

Fig. 4. 2017, 2021 OWASP Top 10

2.1.2 보안 정책 운영 중 발생할 수 있는 문제점

정책 운영 중 발생할 수 있는 관리적 문제점을 분석해본다면 중복 정책 및 논리적 오류 정책이 있다.

첫째, 중복 정책은 동일한 기능을 하는 정책이 2개 이상 다수 존재하는 정책을 말한다.

둘째, 논리적 오류 정책은 우선순위에 따라 상위 정책에 의해 하위 정책이 무시되는 경우이다.

두 가지 경우 모두 운영 기법의 한 종류로 주로 사용되지만, 낮은 정책 이해도 및 Human Error로 인해 잘못 적용되었을 경우 의도한 대로 적용되지 않는 문제가 발생하여 심각한 침해사고를 야기할 수 있다.

본 논문에서는 가장 큰 위협이 되는 외부 접근을 통제할 수 있는 장비인 방화벽을 대상으로 중복 정책과 논리적 오류 정책을 식별하는 보조 시스템을 개발하고자 한다.

III. The Proposed Scheme

3.1 환경 구성

정책 점검에 사용될 방화벽 솔루션은 Netgate의 오픈소스 방화벽 솔루션 pfSense[6]를 활용하여 VMware 환경 하에 임의의 가상 인프라를 구축하였고 올바르게 구현된 정책과 위험하게 구축된 정책 크게 두 가지 Case를 적용하여 테스트 하였다.

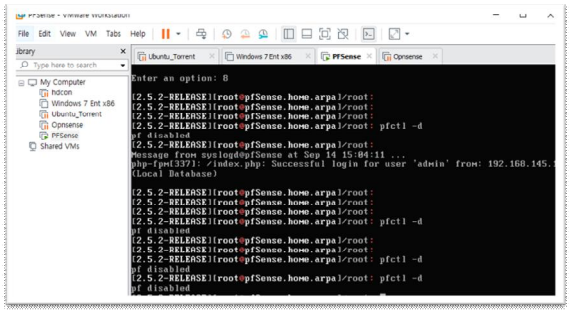

Fig. 5. 가상환경에 구현한 pfSense 방화벽

3.2 분석 및 설계

3.2.1 요구기능 분석

Fig. 6에서 보듯이 개발에 앞서 이 시스템이 적용되어 작동할 흐름도를 파악하였다.

첫째, 점검 전 단계에서는 방화벽으로부터 정책의 백업 파일을 Export하고 개발 시스템에 입력한다.

둘째, 점검 단계에서는 입력된 정책 파일을 분석하여 중복 정책과 논리적 오류 정책을 식별한다.

셋째, 점검 후 단계에서는 식별된 결과를 정해진 양식에 따라 보고서를 출력한다. 보안을 위해 정책 파일은 완전 삭제한다.

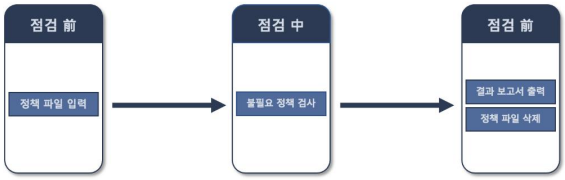

Fig. 6. 업무 흐름도

파악된 전체 흐름을 바탕으로 총 14가지의 기능을 식별하였고 요구기능 명세서를 작성하였다.

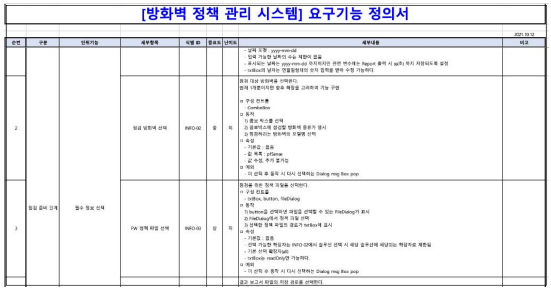

Fig. 7. 요구기능 명세서

3.2.2 UI 설계

Fig. 7의 요구기능 명세서를 바탕으로 UI를 설계하였다. UI에 사용된 컴포넌트는 오픈소스를 활용하였다.[7]

Fig. 8. UI 화면

3.2.3 보고서 설계

요구기능 명세서를 바탕으로 보고서 Form을 설계하였다. 보고서 Form은 크게 세 구역으로 구분할 수 있다.

첫째, Base Profile은 점검과 관련된 기본적인 정보인 점검 날짜, 정책 파일 경로, 파일 버전을 표시한다.

둘째, Result는 정책 점검 결과의 요약사항을 나타낸다. 사용 중인 미 동작 정책(Overlap Policy)과 중복 정책(Duplicate Policy)의 개수를 나타낸다.

셋째, Detail Data는 상세한 점검 결과를 나타낸다. 어떤 Service에서 어떤 IP가 중복 또는 미 동작 중인지를 알 수 있다.

3.4 구현

최종적으로 구현된 정책 검사 과정은 다음과 같다.

첫째, Protocol 종류별 Sequence ID를 구분한다. Protocol, IP/Port 모두가 일치하는 경우이다. 이 중 하나라도 불일치한다면 검사 대상이 아니므로 정책 파일을 읽는 과정에서 동일 Protocol로 미리 집합을 만들어 구분한다면 불필요한 검사 횟수를 더욱 줄일 수 있을 것이다.

둘째, 같은 Protocol을 사용하는 정책의 IP/Port의 범위검사를 수행하여 중복된 범위 값을 추출한다. 이 때, IP 범위 검사 시 문자열로 표현된 IP는 정수로 변환하여 이미 정수로 표현된 Port와 동일한 방법으로 범위 검사를 수행한다.

셋째, 각 정책의 허용/차단 동작을 확인하여 두 정책의 동작이 서로 같으면 중복 정책이고, 서로 다르면 둘 중 하위 순번의 정책이 미 동작하는 경우로 판별한다.

넷째, 모든 정책의 검사를 수행하고 중복된 IP/Port, Protocol 결과 값을 Report Form에 맞게 출력한다. Fig. 9는 점검 결과 화면이다.

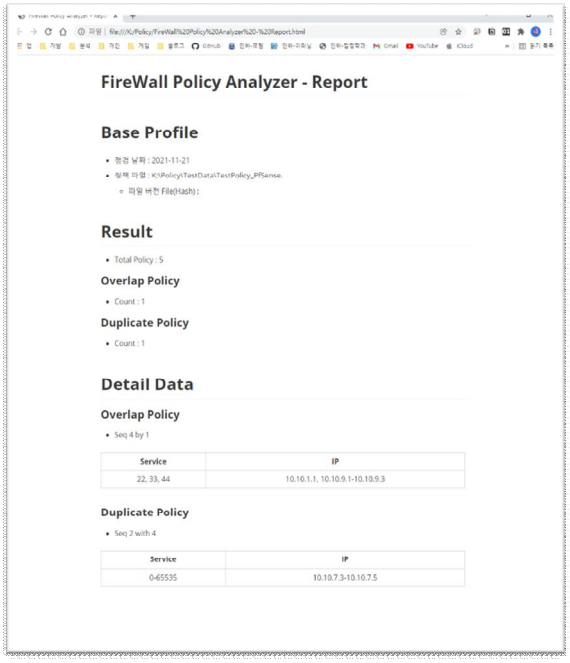

Fig. 9. 점검 결과

IV. Conclusions

다양한 정보보호 장비 중 네트워크를 이용한 직접적인 침입을 통제하는 방화벽 시스템의 정책 관리를 도와주는 보조 시스템을 개발하였다. 그 결과 방법 중 중복 정책과 논리적 오류를 가지는 정책을 식별할 수 있었다.

본 보조 시스템은 손쉽게 접근할 수 있는 오픈 소스 방화벽을 대상으로 개발하였으나 실무에 적용한다면 정책 추가/삭제/변경과 같은 작업 시 보다 효율적으로 검토하고 Human Error를 최소화할 수 있는 결과를 기대할 수 있을 것이다.

REFERENCES

[1] National Intelligence Service, "National Information Security White paper", pp. 101-105, May 2021.

[2] Korea Internet & Security Agency, "Detailed Guide for Analysis and Evaluation of Vulnerabilities in Major Information and Communication Infrastructure", p. 338, March 2021.

[3] Korea Internet & Security Agency, "Personal Information & Information Security Management System Certification guide", p. 44, January 2019.

[4] Korea Internet & Security Agency, “Practice guide for SME information protection.” Vol. 2, No. 2, p. 117, February 2020.

[5] The OWASP Foundation, "OWASP Top Ten", September 2021, https://owasp.org/www-project-top-ten/

[6] Netgate Firewall Solution, Ver. 2.5.2, https://www.pfsense.org/

[7] Material Design In XAML Ver. 4.2.1 https://github.com/MaterialDesignInXAML/MaterialDesignInXamlToolkit