Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.6, Dec. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.6.1087

방화벽 접근정책의 계층적 가시화 방법에 대한 연구*

김 태 용,[1†] 권 태 웅,[1] 이 준,[2] 이 윤 수,[2] 송 중 석[3‡]
[1,2,3]한국과학기술정보연구원 (연구원, 선임연구원, 책임연구원)

A Study to Hierarchical Visualization of Firewall Access Control Policies*

Tae-yong Kim,[1†] Tae-woong Kwon,[1] Jun Lee,[2] Youn-su Lee,[2] Jung-suk Song[3‡]
[1,2,3]Korea Institute of Science and Technology Information(KISTI)
(Researcher, Senior Researcher, Chief Researcher)

요 약

빠르게 진화하는 다양한 사이버공격으로부터 내부 네트워크와 정보를 보호하기 위해 다양한 보안장비를 사용한다. 그 중 대표적으로 사용하는 보안장비는 방화벽이며, 방화벽은 접근정책이라는 텍스트 기반의 필터링 규칙을 사용해 내·외로부터 통신하는 접근을 허용하거나 차단하여 악의적인 공격을 사전에 방어할 수 있다. 내부의 정보를 보호하기 위해 수많은 접근정책들이 사용하며, 점차 증가하는 접근정책을 효율적으로 관리하기에 여러 가지 어려움이 발생한다. 그 이유는 텍스트 기반의 많은 정보를 분석하기 위해서는 많은 시간 소요와 잔존하는 취약한 정책을 보완하기에는 한계점이 있다. 이와 같은 문제점을 해결하기 위해, 본 논문에서는 직관적인 접근제어 정책 분석 및 관리를 위한 3D 기반의 계층적 가시화 방법을 제안한다. 특히, 계층적 가시화를 통한 드릴-다운 사용자 인터페이스를 제공함으로써, 복잡한 대규모 네트워크의 접근제어 정책을 세부적으로 분석을 지원한다. 제안된 가시화 방법론의 실용성 및 유효성 검증을 위해 시스템을 구현하고, 이를 실제 대규모 네트워크 방화벽 분석에 적용함으로써 성공적으로 제안된 가시화 방법의 적용이 가능함을 보인다.

ABSTRACT

Various security devices are used to protect internal networks and valuable information from rapidly evolving cyber attacks. Firewall, which is the most commonly used security device, tries to prevent malicious attacks based on a text-based filtering rule (i.e., access control policy), by allowing or blocking access to communicate between inside and outside environments. However, in order to protect a valuable internal network from large networks, it has no choice but to increase the number of access control policy. Moreover, the text-based policy requires time-consuming and labor cost to analyze various types of vulnerabilities in firewall. To solve these problems, this paper proposes a 3D-based hierarchical visualization method, for intuitive analysis and management of access control policy. In particular, by providing a drill-down user interface through hierarchical architecture, Can support the access policy analysis for not only comprehensive understanding of large-scale networks, but also sophisticated investigation of anomalies. Finally, we implement the proposed system architecture's to verify the practicality and validity of the hierarchical visualization methodology, and then attempt to identify the applicability of firewall data analysis in the real-world network environment.

Keyworkds: Firewall, Access Control List, Hierarchical Visualization, 3D Drill-Down User Interface, Policy Anomaly

Received(11. 12. 2020), Modified(11. 27. 2020), Accepted(11. 28. 2020)
* 본 연구는 한국과학기술정보연구원(KISTI) 지원으로 수행하였습니다.
† 주저자, skytaeyong@kisti.re.kr
‡ 교신저자, song@kisti.re.kr(Corresponding author)

I. 서 론

급속도로 발전하는 통신 및 보안기술의 발전과 함께 다양한 최첨단의 보안장비들이 개발되고 있지만, 네트워크 보안의 핵심 필수 요소로서 방화벽은 대부분의 기업부터 공공기관, 정부에 이르기까지 널리 활용되고 있다. 방화벽은 기본 기능으로써 접근제어 정책(access control policy, 이하 접근정책)을 바탕으로 외부 사용자로부터 내부 네트워크의 접근을 관리하며, 또한 내부 네트워크에서 외부로 나가는 정보를 안전하게 전달하는 역할을 수행한다. 최근 네트워킹 IT 회사 임원과 경영진을 대상으로 설문조사를 수행한 Network World의 '2020 State Of the Network' 보고서에 따르면[1], 설문 응답자의 88%는 외부로부터 다양한 공격을 방어하기 위해 방화벽 사용을 최우선으로 고려하고 있다고 응답하는 등 네트워크 최상단의 방어수단으로써 방화벽은 그 중요성이 날로 증대되고 있다.

방화벽 운용을 위한 기본적인 접근정책의 구성은 프로토콜, 출발지 IP, 출발지 포트, 도착지 IP, 도착지 포트 및 IN/OUT의 동작으로 이루어지며, 이 요소들을 활용하여 내/외부에서 발생하는 트래픽과 접근정책 간의 비교를 통해 네트워크 패킷의 접근허용 및 차단을 수행한다. 일반적으로 방화벽 기본 정책은 차단정책(ALL-DENY)을 기반으로 수립되며, 이는 초기 설정부터 모든 경우에 대하여 차단을 수행하고 예외적으로 통신이 필요한 부분만 허용하는 화이트리스트(White list) 형태의 운용을 의미한다. 반면에 기본 허용정책(ALL-ALLOW)은 방화벽 설치 구간의 모든 네트워크 통신을 허용하는 방식으로써, 내부에서 내부로 통신하는 구간에서 주로 사용되며 방화벽 관리자는 유해 IP 및 불필요한 서비스(Port)에 대하여 차단할 수 있는 용도로 사용된다.[2]

일반적으로 관리자의 숙련도와 분석에 따라 적절한 우선순위로 결정된 방화벽 접근정책의 설정을 바탕으로 안정적인 네트워크 보안 수준 달성이 가능하다. 하지만 최근 다양한 개인용 단말의 증가와 더불어 대규모 네트워크의 사용이 활발해짐에 따라 방화벽의 접근정책 개수가 급격히 증가하고 있으며, 이에 수반되는 복잡한 접근정책 리스트 구조로 비효율적인 방화벽 접근정책 설정이 발생하고 있다. 특히 탑-다운(top-down) 방식으로 적용되는 접근정책의 특성상 정책 간 중첩 및 중복 등의 관계이상[3]으로 인한 네트워크 오류를 발생시키는 경우가 크게 증가하고 있다.

접근정책은 주로 표(table) 형태의 텍스트 기반 리스트로 관리되기 때문에 직관적으로 정책 간의 문제점을 파악하기 어렵고, 특히 전체적인 접근정책 간의 관계와 순서의 고려가 필수적으로 요구되기 때문에 단편적인 정책 간의 비교로는 최적화된 방화벽 설정이 불가능하다. 비록 이러한 문제를 해결하고 방화벽 정책 설정의 효율성을 향상시키기 위해 다양한 시각화 기법을 고려한 방법 및 점검 도구들이 제안되고 있지만[4][5][6], 2D그래프 방식의 특성상 복잡한 정책 관계를 표현하는데 있어서 직관성이 떨어지며, 관리자가 점검도구를 숙지하고 사용하기까지 많은 시간이 소요되는 문제점이 발생하고 있다.

이와 같은 문제점을 해결하고 관리자의 최적화된 방화벽 접근정책 설정을 돕기 위하여, 본 논문에서는 대규모 접근정책의 계층적 구조 가시화 방법을 제안한다. 제안한 방법은 정책 현황(사용량, 연결성)과 정책 간 문제점을 분석하고, 정책의 요약정보 및 세부정보를 직관적으로 파악할 수 있도록 시각화를 제공한다.

본 논문은 다음과 같이 구성되어 있다. 제 2장에서는 방화벽 접근정책 간 발생할 수 있는 관계이상에 대하여 설명하고, 방화벽 접근정책을 효율적으로 관리하기 위한 기존 가시화 기반의 도구들에 대하여 알아본다. 3장에서는 본 논문에서 제안하는 접근정책의 계층적 가시화에 대한 방법론을 설명하고, 4장에서 제안된 방법을 바탕으로 구현된 실제 시스템을 통해 그 기능과 활용 방안을 확인한다. 5장에서는 실제 대규모 네트워크에 적용 사례를 통해 제안하는 방법론의 유효성을 증명한다. 마지막으로 6장에서는 본 논문의 결론과 향후 연구에 대해 기술한다.

II. 관련연구

본 장에서는 방화벽 접근제어 정책의 역할과 최적화 필요성에 대하여 함께 살펴보고, 특히 보안상 취약점을 노출시키거나, 네트워크 통신 간 접근 문제를 초래하는 대표적인 방화벽 접근정책의 문제점(관계이상)에 대하여 살펴본다. 마지막으로 접근제어 정책을 효율적으로 관리하기 위한 도구들과 접근정책 최적화를 위해 제안된 다양한 시각화 연구들에 대하여 소개한다.

2.1 방화벽과 접근정책 및 그 역할

방화벽은 외부(낮은 신뢰수준) 네트워크와 내부(높은 신뢰수준) 네트워크 간의 트래픽을 제어하는 역할을 수행하는 장비로써 네트워크 보안관리를 위해 널리 사용되고 있다. 네트워크 보안을 위한 방화벽의 역할은 1980년대 라우터로부터 시작되었으며, 본래 네트워크를 연결하는 역할 뿐만 아니라 네트워크 간 분리를 통해 서로 다른 네트워크를 차단하는 용도로 사용하여 보안관리를 수행하였다[10].

방화벽은 순서관계를 갖는 필터링 규칙을 사용하고 있으며, 순차적으로 정의된 규칙과 일치하는 패킷에 대하여 차단 또는 허용을 통해 내/외부의 네트워크 트래픽을 제어한다. 각 필터링 규칙 항목은 프로토콜, 출발지 IP, 출발지 Port, 목적지 IP, 목적지 Port, 접근 허용 및 차단으로 구성되어 있으며, 구성된 객체들은 단일 값 또는 범위 값, 그리고 그룹으로 설정이 가능하다. 이 방식은 단순하면서 매우 효율적이지만, 대규모 네트워크의 경우 모든 패킷에 대하여 모든 정책을 순차적으로 검사해야 하기 때문에 성능저하 및 처리속도가 느려지는 경우도 있다. 이러한 문제를 해결하기 위해 패킷 단위가 아닌 세션 단위의 검사를 수행하는 상태기반 감시(SPI, statefulpacket inspection) 방식의 방화벽이 등장하였으며[11], 일상적인 트래픽과 같은 특성을 가지면서 특정 애플리케이션에 공격을 취하는 지능형 공격 패턴에 대응하기 위해 애플리케이션에 대한 영향 분석을 수행하는 침입탐지시스템(IPS,Intrusion prevention system), 웹 어플리케이션 방화벽(WAF,Web application firewall), 통합 위협관리(UTM,Unified threat management)등과 같은 방화벽 기능을 포함한 네트워크 통합보안 시스템의 형태로 발전되고 있다.

대부분 네트워크 최상단에 위치한 방화벽의 특성상 접근정책을 통한 네트워크 관리로부터 안정적인 보안수준의 달성이 가능하지만, 접근정책 관리는 규칙 간 순서 관계를 포함한 상호 의존적 성질과 그 복잡성 때문에 관리자의 많은 숙련도와 분석 시간을 요구해왔다. 특히, 지속적인 네트워크와 시스템 환경의 발달로 인해 규칙 간 중복 또는 중첩과 같은 관계이상이 발생하고 있고 이로 인한 네트워크 접속 오류 등의 발생률이 크게 증가하고 있기 때문에 접근정책의 관계이상에 대해 주기적인 점검과 빠른 정책 수정이 요구되고 있다[9].

2.2 접근정책 간 대표 관계이상

네트워크의 확장으로 인한 단말 및 통신대상의 증가, 유해 IP 및 Port의 추가 발생 등의 이유로 접근정책은 주기적인 관리가 필요하다. 하지만 2.1절에서 살펴본 것과 같이 관리해야 할 접근정책의 수가 증가하면서 중복되거나 중첩되는 정책, 비활성화 정책 등이 관계이상을 유발할 수 있으며, 이로 인해 방화벽의 불필요한 접근정책들에 의해 보호되어야 할 내부 네트워크가 외부로부터 공격에 노출될 위험성이 존재한다. 본 절에서는 특히, 정책 리스트의 정책 간 순서 및 포함관계에서 비롯된 대표적인 관계이상으로써 Al-Shaer[3] 가 정의한 중첩, 중복, 상관관계, 일반화의 4가지 종류의 정책 간 관계이상에 대하여 알아보고 구체적인 예를 살펴본다.

2.1.1 중첩 이상(Shadowing Anomaly)

중첩 이상 규칙은 Table. 1과 같이 접근정책 간 Action 필드를 제외 한 나머지 필드가 일치하거나 포함될 경우이다. p2는 p1에 의해 그늘져 있어 절대 활성화되지 않으며 이를 그림자 이상 규칙으로 정의하고 그늘진 규칙은 무의미한 정책으로 오류로 간주한다.

그림자 이상 규칙 발생 시 허용된 트래픽이 차단되거나 차단된 트래픽이 허용될 수 있다. 장비를 운영하는 관리자는 그림자 이상 규칙이 발생된 접근정책을 제거하여 오류를 수정할 필요가 있다.

Table 1. Case Example of Shadowing Anomaly

ID	Protocol	S_IP	D_IP/Port	Action
p1	TCP	*.*.*.*	10.16.1.12/80	Allow
p2	TCP	14.12.37.*	10.16.1.12/80	Deny

2.1.2 중복 이상(Redundancy Anomaly)

중복 이상 규칙은 Table. 2와 같이 접근정책 간 모든 필드가 일치하거나 포함될 경우이다. p2는 p1에 중복되므로 p2를 제거하여도 정책 효과는 변경되지 않는다. 중복 접근정책은 최상위 정책을 제외한 나머지 중복된 정책을 제거하더라도 전혀 문제가 되지 않아 완전히 제거할 필요가 있다. 관리자는 기존 정책과 신규 정책을 중복으로 적용하지 않도록 주의를 기울여야 한다.

Table 2. Case Example of Redundancy Anomaly

ID	Protocol	S_IP	D_IP/Port	Action
p1	TCP	10.16.1.*	*.*.*.*/80	Allow
p2	TCP	10.16.1.*	14.12.33.40/80	Allow

2.1.3 상관관계 이상(Correlation Anomaly)

상관관계 이상 규칙은 Table. 3과 같이 첫 번째 규칙이 두 번째 규칙과 서로 교차되어 일부 일치하거나 포함될 경우이다.

상관관계 이상 규칙 발생 시 순서가 뒤바뀔 경우 정책 효과가 달라지기 때문에 관리자는 이점을 유의하여 정책 반영 시 적절한 순서를 선택하여 반영하도록 주의를 기울여야 한다.

Table 3. Case Example of Correlation Anomaly

ID	Protocol	S_IP	D_IP/Port	Action
p1	TCP	10.16.1.20	*.*.*.*/80	Deny
p2	TCP	*.*.*.*	10.16.33.40/80	Allow

2.1.4 일반화 이상(Generalization Anomaly)

일반화 이상 규칙은 Table. 4와 같이 일반 규칙 앞에 있는 특정 규칙과 모든 패킷이 일치하고 Action이 다른 경우이다. p2는 p1의 일반화로, 두 규칙의 순서가 뒤바뀌면 접근정책 효과가 변경되어 p1은 p2에 의해 무의미한 정책이 된다.

일반화 이상 규칙은 상관관계 이상 규칙과 마찬가지로 순서가 뒤바뀔 경우 정책 효과가 달라진다. 이에 관리자는 이점을 유의하여 정책을 반영하도록 주의해야 한다.

Table 4. Case Example of Generalization Anomaly

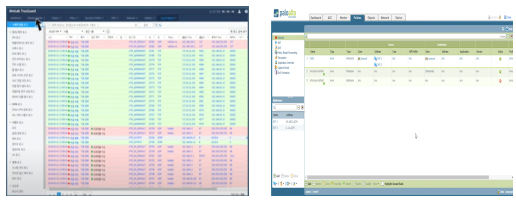
ID	Protocol	S_IP	D_IP/Port	Action
p1	TCP	10.16.1.20	*.*.*.*/80	Allow
p2	TCP	*.*.*.*	*.*.*.*/80	Deny

2.3 접근정책 최적화를 위한 도구 및 가시화 기법

네트워크가 방대해지고 복잡해지면서, 방화벽 접근정책을 관리하고 최적화하기 위한 다양한 기술 및 도구들이 제안되어져 왔으며[5][12][13], 안랩[15], 팔로알토[14] 등 방화벽 제조사를 중심으로 Fig. 1와 같은 관리자를 위한 텍스트 기반 정책 관리 인터페이스 등을 개발하여 제공하고 있다.

하지만 텍스트 기반의 접근정책 정보 제공에서 나아가 복잡한 정책 간 관계를 직관적으로 파악하고 이상현상의 수정을 돕기 위한 방법으로써, 정책 가시화 기법에 대한 연구가 활발히 진행되고 있다. 정책 가시화에 대한 초기 연구로써 PolicyVis[4]는 허용, 차단 트래픽에 대하여 IP와 Port 각각을 차원으로 하여 막대그래프로 표시함으로써 각 정책이 영향을 미치는 부분을 2차원 평면에 직관적으로 표현하였다(Fig. 2). 특히 각 막대그래프가 중첩되는 부분을 정책 간 관계 이상이 발생하는 부분으로 판단하는 방식으로 간단한 인터페이스를 통해서 쉽게 정책을 점검할 수 있는 효율적인 도구로 제안되었다. 다만, 인터페이스 측면에서 접근정책의 세부 현황과 관계이상의 정보(즉, 유형)를 표현할 수 없고 단편적인 결과만 제공하기 때문에, 접근정책의 수정 및 관리를 위해서는 관리자가 다시 세부 정책 리스트를 확인하고 파악해야 한다는 단점이 존재한다.

단순 그래프 형식의 정책 가시화 방법에서 나아가 Florian 등[8]은 복잡한 방화벽 구성을 더욱 직관



(1) AhnLab TrusGuard[15] (2) Paloalto Firewall[14]

Fig. 1. Text-based User Interface for Management Access Control Policy

Fig. 2. Example of ACL Visualization from PolicyVis[4]

적으로 표현하기 위하여 Fig. 3과 같은 계층적 구조의 선버스트(sun-burst) 시각화 방식을 제안하였다. 각 정책과 객체 그룹에 대하여 특정한 색을 매칭하고, 연관된 정책 간의 계층적 구조를 나타내기 위해 원점으로부터 포함관계에 따라 차트를 확장하는 형태로 시각화를 수행하였다. 그러나 복잡한 구조의 표현을 위하여 제안되었지만, 접근정책의 수가 증가할수록 각 정책에 할당되는 차트 면적이 감소하여 세부정보를 파악하기 어려우며 전체 차트 크기에도 제약이 있어 전체 현황을 파악하기에는 다소 직관성이 떨어지는 단점이 존재한다.

이러한 문제점을 보완하고 관리자의 직관성을 향상시키기 위하여 3D 기반의 접근정책 가시화 방법이 제안되어지고 있다[6][7]. 특히 NViZ[6]은 방화벽 로그를 분석하여 네트워크 통신량 정보와 함께 전체 정책 간 연결 가시화 인터페이스의 제공 방법을 제안하였다(Fig. 4.). 특히 공간상에 각 정책을 배치하고 전체 연결 상태를 한눈에 파악하기 쉽도록 표시함으로써 관계이상 및 보완사항을 찾기 쉽게 하였다. 다만, 관리자의 직관성을 돕기 위해 정책 및 네트워크의 상세 정보를 가시화에서 배제함으로써 세부정보를 파악하기 위해서 재 검색을 수행해야 하는 불편함이 존재한다.

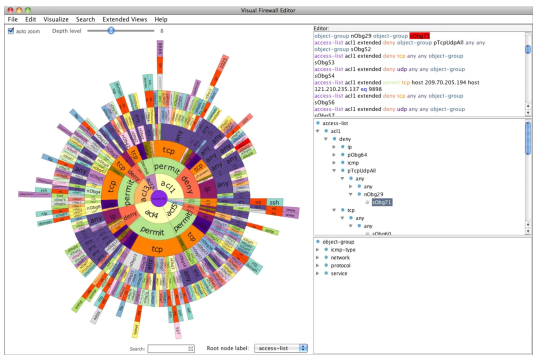


Fig. 3. ACL Visualization by Sunburst Method[8]

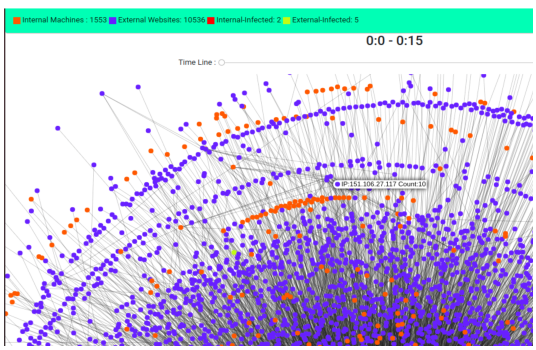


Fig. 4. Communication Visualization from NViZ[6]

이와 같이 방화벽 접근정책 관리 및 최적화를 돕기 위하여 다양한 가시화 방법이 제안되어져 왔지만, 실 사용 측면에서 정책 간 전체 현황 파악 및 세부정보 표시 등의 부분에 대한 개선이 요구되고 있다. 본 연구에서는 이러한 문제점을 보완하고 복잡한 구조의 텍스트 기반 접근정책 가시화[15][14]에서 나아가, 접근정책의 관계 및 전체 현황정보를 한눈에 파악할 수 있는 3D 기반의 계층적 가시화 방법론을 제안하고 이를 실제 구현하여 그 효용성을 확인한다.

III. 계층적 접근정책 가시화 방법론

기존 텍스트 기반의 방화벽들이 정책들의 관계이상을 해결하기 어려운 이유는 크게 4가지로 다음과 같다.

- 관계이상 인지의 어려움
- 관계이상의 원인정책을 파악하기 어려움
- 수정 필요한 정책들의 우선순위 결정이 어려움
- 정책 수정 시 발생 가능한 부작용 파악의 어려움

제안하는 가시화 방법론은 이러한 문제점들을 해결하기 위하여 고안되었다. 대규모의 복잡한 접근정책을 한 화면에 계층적으로 표현하는 방법을 제안함으로써, 관리자에게 정책의 현황 및 정책 간의 문제점 등을 쉽고 빠르게 파악할 수 있도록 도와준다. 특히 단일 접근정책 뿐만 아니라 정책 간 관계이상 판별을 통한 규칙 재 구성 등의 통합적인 관리가 필수적인 방화벽 접근정책 관리에 있어서, 전체 현황 및 세부정보를 한눈에 표현하는 3차원 시각화 및 드릴다운 검색을 제공함으로써 관리자는 문제점을 쉽게 인지하고 보완이 가능하다. 구체적으로 접근정책 간 주요 관계이상을 파악하여 이를 상위 계층에 요약정보 형태로 표현하고, 나아가 직관적인 세부정보 제공을 위해 3차원 원통형(cylindrical) 공간상에 각 정책을 배치하고 관계에 따라 그래프로 연결한다. 이와 같은 새로운 접근정책 가시화 방법을 제안함으로써 대규모 네트워크 접근정책의 효율적인 통합관리가 가능하도록 기여한다.

3.1 방화벽 접근정책 관계이상 분석 방법론

2.2에서 설명한 4종류의 방화벽 접근정책 관계이상을 본 논문에서 제안하는 가시화 방법론에 적용하기 위해 아래와 같이 4가지 분석 모델로 정의하였다.

① 중첩 이상(Shadowing Anomaly) : 중첩 이상 규칙은 수식 (1)과 같이 p2의 Action을 제외한 나머지 5개 필드가 상위 정책 p1 의 부분집합일 경우를 말한다. 방화벽은 top-down 방식으로 정책 간의 우선순위를 결정하기 때문에 상위에 위치한 정책을 우선적으로 적용한다. 따라서 정책의 우선순위가 관리자의 의도에 따라 설정이 된 것인지 주기적인 검토 및 수정이 필요가 있다.

$$F = \{protocol,\ sip,\ sport,\ dip,\ dport,\ action\}$$

$$\begin{cases} p1_f \supset p2_f & (f|f \in F \text{ and } f \neq action) \\ p1_{action} \neq p2_{action} \end{cases} \quad (1)$$

② 중복 이상(Redundancy Anomaly) : 중복 이상 규칙은 접근정책들 간 포함관계를 가질 경우를 의미하며, 수식 (2)와 같이 정의 가능하다. 중복된 정책 중 최상위 정책을 제외한 나머지 정책들은 방화벽에 영향을 미치지 않으며, 하위 정책들을 제거한다 하더라도 오작동의 원인이 되지 않는다. 오히려 이러한 불필요한 정책들은 방화벽 성능저하의 원인이 되기 때문에 주기적으로 점검하여 제거하는 것이 효율적인 방화벽 운영에 도움이 된다.

$$p1_f \supseteq p2_f \quad (\text{Only if}, \quad f|f \in F) \quad (2)$$

③ 상관관계 이상(Correlation Anomaly) : 수식 (3)은 연관 이상 규칙을 나타내는 것으로 상위 정책과 하위 정책의 필드들이 서로의 부분집합이 되는 경우, 이를 연관 이상이라 정의한다. 상관관계 이상은 빈번하게 발생하면서도 매우 위험한 결과를 초래할 수 있어 반드시 확인하여 제거하거나 적절한 정책의 우선순위를 부여해야만 한다.

$$\begin{cases} p1_g \subset p2_g & (g|g \in G \text{ and } G \subset (F - action)) \\ p1_h \supset p2_h & (h|h \in G^c \text{ and, } G^c \subset (F - action)) \\ p1_{action} \neq p2_{action} \end{cases} \quad (3)$$

④ 일반화 이상(Generalization Anomaly) : 일반화 이상 규칙은 3.1.1의 중첩 이상과 정반대의 경우이다. Action을 제외한 모든 필드에서 상위정책이 하위정책의 부분집합일 경우 이를 일반화 이상이라 한다.

$$\begin{cases} p1_f \subset p2_f & (f|f \in F \text{ and } f \neq action) \\ p1_{action} \neq p2_{action} \end{cases} \quad (4)$$

일반화 이상은 대부분의 관리자들이 정책 설정의 편의를 이유로 가장 많이 사용하고 있는 관계이상이다. 다수의 정책이 일반화 이상의 관계를 가질 경우 타 관계이상들과 마찬가지로 의도치 않은 동작을 야기할 수 있어 룰의 추가, 수정, 삭제 시 관리자의 많은 주의 및 검증을 요하게 된다.

3.2 계층적 가시화 방법 가시화 모델

본 논문에서 제안하는 가시화 방법은 Fig. 5에서와 같이 각 정책 간 관계이상과 같은 핵심 요약정보를 표시하는 상위계층(upper layer), 그리고 각 접근정책의 세부정보와 더불어 정책 간 연결성을 가시화 하는 하위계층(lower layer)의 두 계층으로 구성된다.

① 상위계층(upper layer) : 방화벽 접근정책들 간의 관계이상에 대한 요약정보를 표현하는 계층으로, 접근정책의 현황 및 문제점을 신속/정확하게 인지할 수 있도록 한다. 해당 계층의 상세내용은 3.2.1절에서 설명한다.

② 하위계층(lower layer) : 방화벽 접근정책을 가시화하는 계층으로, 각각의 접근정책을 하나의 아이콘으로 변환 및 정해진 규칙에 따라 배열함으로

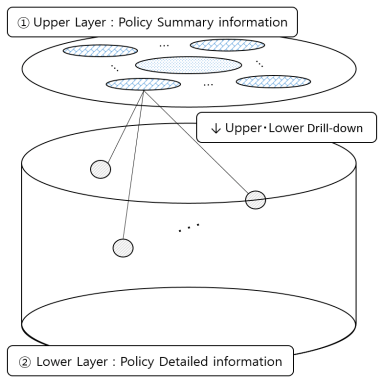


Fig. 5. Conceptual Image of Hierarchical Visualization Methodology methodology

써 정책의 특징(복잡성, 사용량)을 인지할 수 있도록 표현한다. 상세한 내용은 3.2.2절에서 설명한다.

상위계층에 표현된 관계이상은 하위계층의 연관성 있는 정책들과 연결선으로 연결되어 있어, 관계이상과 관계이상을 발생시키는 접근정책들을 직관적으로 인지할 수 있으며, 이에 대한 분석이 가능하다.

3.2.1 상위계층 가시화 방법

Fig.6.는 접근정책 계층적 방법론의 상위계층 개념도이다. 제안하는 방법론의 상위계층은 2개의 요소로 구성되어 있다.

① Status Summary dashboard : 방화벽 접근정책과 관계이상 개수를 요약정보로 표현하는 정보판으로, 관리자가 요약정보에 표현되는 정책의 개수, 그리고 문제점을 직관적으로 인지할 수 있는 정보를 제공한다.

② Anomaly Plate : 방화벽 접근정책의 사용 규칙은 상위정책부터 하위정책까지 순차적으로 처리된다. 상위정책부터 정책을 순차적으로 관계이상에 대해 분석하고 발견되는 접근정책 개수에 따라 Anomaly Plate 객체(이하 객체)를 생성한다. 생성된 객체는 관계이상으로 발견된 상위정책 Rule ID와 4개 분류된 관계이상 유형 중 발견된 유형을 요약정보로 표현하여 관리자에게 제공한다. 관리자는 객체의 개수를 줄이는 것만으로도 접근정책의 보안을 강화할 수 있는 방법을 제안한다.

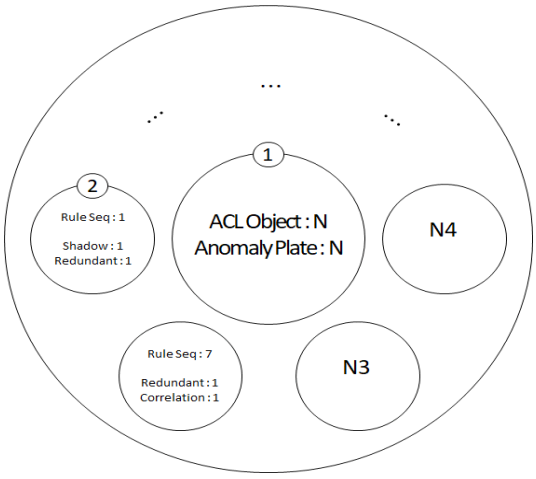


Fig. 6. Visualization Methodology for Upper Layer Components

3.2.2 하위계층 가시화 방법(공간 배열 알고리즘)

하위계층에는 정책간의 관계이상을 유발하는 접근정책들을 배치하고 이를 Anomaly Plate와 연결함으로써 보다 직관적으로 정책간의 관계를 파악할 수 있도록 하였다. 본 방법론에서는 접근정책들의 효율적인 화면배치 및 가시성을 위해 아래와 같은 수식 (6), (7), (8)을 활용하여 원기둥 내 각 정책들의 좌표 $(r,h,\theta)_{p_i}$를 결정하였다. 좌표가 결정된 정책들은 Fig. 7.과 같이 화면에 가시화 되며, 이는 배치된 위치만으로도 각 정책의 특징을 파악할 수 있게 도와준다. 각 요소에 대한 정의 및 상세 설명은 다음과 같다.

$$P_{\forall} = \{p_0,\ p_1,\ \ldots\ ,p_{n-1}\ ,p_n\}$$

$$r_{p_i} = \frac{\#\ of\ IP/Port\ in\ p_i}{MAX(\#\ of\ IP/Port\ in\ P_{\forall})} \times R\ \ (p_i | p_i \in P_{\forall}) \tag{6}$$

$$h_{p_i} = \frac{hit\ \ count\ \ of\ p_i}{MAX(hit\ \ count\ \ of\ P_{\forall})} \times H\,(p_i | p_i \in P_{\forall}) \tag{7}$$

$$\theta_{p_i} = \frac{i}{n+1} \times 2\pi\ \ (p_i | p_i \in P_{\forall}) \tag{8}$$

① h_{p_i} : 원기둥 내에서 정책 p_i의 높이를 결정하기 위한 방법이다. 제안하는 시스템에서는 각 정책의 정책 적중 횟수(히트수, hit count)에 비례하여 높이를 결정한다. 전체 정책 P_{all}중 가장 높은 적중 횟수를 갖는 정책의 높이를 H로 지정하고, 이를

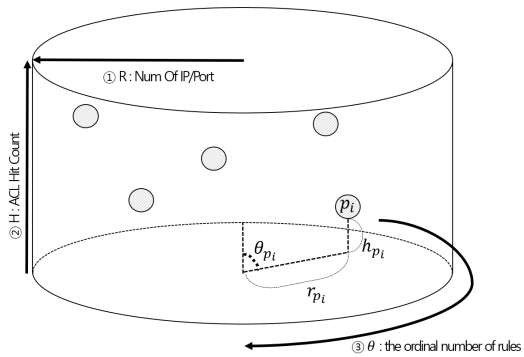


Fig. 7. Conceptual Image of Visualization Methodology in Lower Layer

기준으로 나머지 정책들도 각 정책의 히트수에 비례하여 높이를 설정하였다. 이와 같은 방법은 각 정책의 높이에 따라 정책의 중요도를 판단하는데 도움을 주기 때문에 정책의 수정/삭제 시 발생하는 문제점을 파악하는데 도움을 준다. 예를 들어 Table 4.의 p_1과 p_2의 Hit count가 각각 50, 100이라 하였을 시, h_{p_1}은 다음과 같이 계산할 수 있다.

$$h_{p_1} = \frac{50}{100} * H = \frac{H}{2} \quad (9)$$

② r_{p_i} : 정책 p_i의 배치 시 원기둥의 중심으로부터의 얼마나 멀리 배치할 것인가를 결정하기 위한 방법이며, 기본적인 방법은 h_{p_i}를 구하는 방식과 동일하다. 본 시스템에서의 r(반지름)은 정책의 범위 즉, 얼마나 많은 IP와 Port들을 다루고 있는 정책인지에 따라 결정된다. 전체 정책 P_{all}중 가장 높은 적중 횟수를 갖는 정책의 r_{p_i}를 R로 지정하고, 이를 기준으로 나머지 정책들도 각 정책의 IP/Port 수에 비례하여 r값을 설정하였다. 예를 들어 Table 4.의 경우 p_1과 p_2의 IP개수가 각각 50, 100이기 때문에 r_{p_1}은 다음과 같이 계산된다.

$$r_{p_1} = \frac{1+2^{32}+1}{2^{32}+2^{32}+1} * R \approx \frac{R}{2} \quad (10)$$

③ θ_{p_i} : 정책의 가시화함에 있어 중요한 것은 각 정책을 중첩없이 배치함으로써 정책의 특징들을 직관적으로 이해할 수 있도록 하는 것이 중요하다. 제안하는 방법론에서는 전체 정책의 개수 및 우선순위(정책의 순서)에 따라 각 정책의 각도를 결정하였다. 정책의 인덱스를 전체 정책의 개수로 나누고 최대 각도인 2π를 곱하였다. 단, 이러한 방법론을 적용할 경우 0과 2π는 동일 각도(0°)로 표현되기 때문에 두 개의 정책이 중첩되어 표현될 수 있다. 이를 방지하기 위하여 정책의 인덱스는 0번부터 n번까지 총 n+1개로 표현하였다. 예를 들어, 전체 룰이 10개라 가정하면, 정책의 인덱스는 0~9까지 부여되며 각각의 각도는 $0, \frac{2\pi}{10}, \frac{4\pi}{10}, \cdots, \frac{18\pi}{10}$가 되어 가시성을 저해하는 중첩현상을 방지할 수 있다.

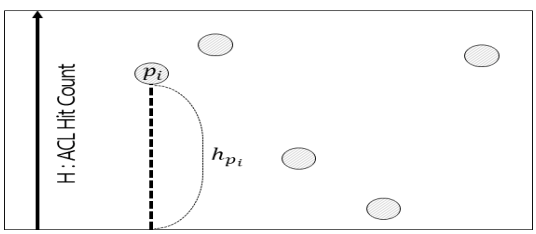


Fig. 8. Horizontal Cross-section View of Lower Layer

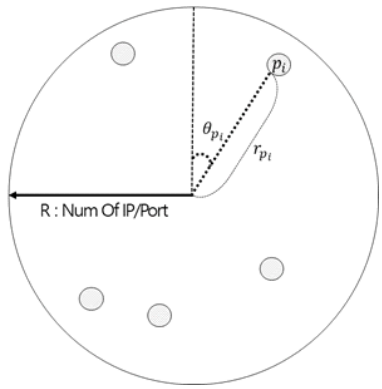


Fig. 9. Vertical Cross-section View of Lower Layer

3.2.3 드릴-다운 가시화 방법

본 논문에서 제안하는 방법론의 궁극적인 목표는 관계이상을 발생시키는 원인을 파악하고 이를 제거함으로써 안정적인 방화벽 운영환경을 구축하는데 있다. 제안하는 방법론은 접근정책 간의 요약 정보를 상위계층에 표현하고 이와 관련된 정책들을 하위계층에 표현하여 연결(드릴-다운)함으로써 관리자가 신속히 접근정책의 문제점을 파악할 수 있도록 구성하였다. 이와 반대로 접근정책을 선택하였을 경우에는 해당 접근정책과 관련된 관계이상들과 연결(역(inverse)드릴-다운)함으로써 선택된 정책이 얼마나 많은 관계이상을 유발하고 있는지 확인할 수 있다. 이는 관리자로 하여금 제거해야하는 관계이상에 가장 큰 영향을 미치는 정책들을 선택하는데 도움을 줄 수 있다.

예를 들어 방화벽 관리자들은 보안성 강화를 위해 주기적으로 방화벽 정책 점검 및 불필요한 정책들을 수정/삭제한다. 제안하는 방법론은 잔존하는 관계이상 파악 및 특정 룰 삭제 시 삭제대상이 미치는 영향력을

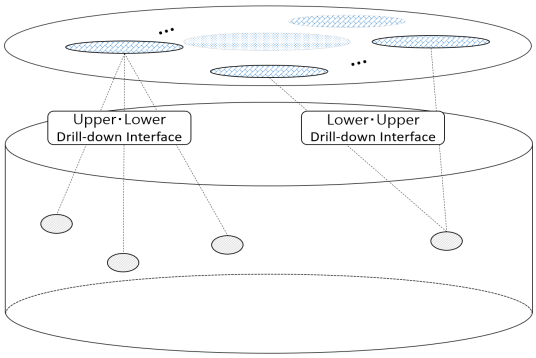


Fig. 10. Conceptual Image of Drill-down & Inverse Drill-down Interface

가시적으로 표현하여 보다 직관적인 이해가 가능하도록 하였으며, 1~2번의 클릭만으로 부작용 없이 삭제/수정 대상 정책을 결정할 수 있다.

IV. 계층적 가시화 기반 접근정책 점검도구의 구현

4.1 점검도구의 전체 시스템 구성 및 사용자 인터페이스

본 논문에서 제안한 3차원 기반 계층적 가시화 방법을 적용한 방화벽 접근정책 점검도구의 구현은 Fig. 11에서와 같이 크게 4가지 부분으로 구성된다. 먼저 방화벽 정보를 수집하기 위해 시스템 로그(syslog)를 수집하고, 수집된 로그로부터 각 결측치 및 이상치 등으로 보정 한 후 필드별로 분할하여 데이터베이스에 저장한다. 그리고 2.2절에서 알아본 것과 같은 정책 간 관계이상 및 문제점들을 분석 엔진(Analyzer Engine)을 통해 분석 후, 가시화 엔진(Visualization Engine)에서 3차원 가시화 및 인터렉티브 사용자 인터페이스를 적용하여 시각화를 수행한다.

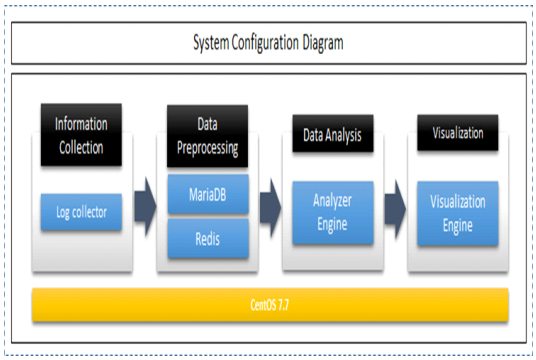


Fig. 11. Visualization System Configuration Diagram

Table 5.는 3장에서 제안하는 계층적 접근정책 가시화 방법론을 구현하고 구동하기 위한 세부 H/W 및 S/W 구성으로서, H/W 서버는 사용자의 운용상황을 고려하여 별도의 고사양 서버가 아니더라도 일반적으로 시스템에 적용하기 적합한 수준으로 구성하였으며(Intel i7 core, 32GB RAM 등), Software의 경우, 관리 및 유지보수의 편의성을 위해 오픈소스 위주의 시스템 구성을 시도하였다(Tomcat[16], Maria DB[17], Redis[18] 등). 특히 저사양 시스템에도 적합한 게임 엔진인 유니티(UNITY)[19]를 활용하여 원활한 3차원 가시화를 시도하였으며, 접근정책 수집 및 전처리를 위해 Python을 사용하였다.

Fig. 12.은 계층적 가시화를 구현한 점검도구(이하 가시화 시스템)의 메인 인터페이스 화면이다. 중앙부분에 3장에서 제안한 방법을 토대로 한 상/하위 계층이 구성되어 있으며, 구체적으로 상위계층은 방화벽 접근정책의 전체 정보에 대한 정책현황과 관계이상 등을 요약정보를 나타내며, 하위계층은 각 접근정책과 관계이상 간 연결상태 및 분포 등을 확인할 수 있도록 세부정보를 나타내고 있다.

뿐만 아니라 Fig. 13.과 같이 전체적인 접근정책 및 관계이상에 대한 정보를 좌측 상단의 요약정보 인터페이스에서 제공하여 접근정책의 직관적인 정보인지를 가능하게 하고 있으며, 관리자의 세부정보 검색

Table 5. Hardware & Software Detailed Specifications for Development of the Proposed System

type		Detailed specification
H/W	CPU	Inter i7 core
	Momory	32GB
	HDD	2TB
S/W	Web Interpace	Tomcat
	Database	Maria DB
		Redis
Engine	Visualization	Unity 3D
	Data collection & preprocessing	Python

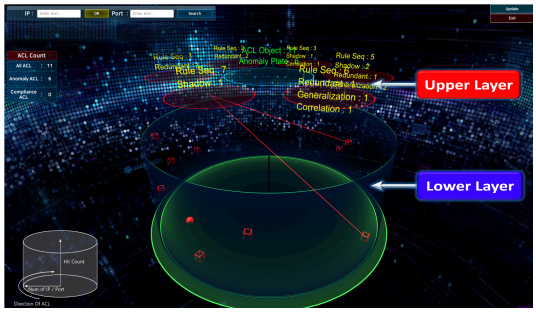


Fig. 12. Overall Display of Implemented System

Fig. 13. User Convenience Function

을 돕기 위해 IP 및 Port 기반 검색 기능을 상단에 제공한다.

4.2 접근정책 요약정보 및 관계이상 정보 가시화

2장 및 3장에서 살펴 본 것과 같이 비록 접근정책 간 관계이상 및 문제점들의 분석 기법은 널리 알려져 왔지만, 순서관계에 많은 영향을 받는 접근정책의 특성상 그 수가 많아질수록 전체 정보를 파악하고 처리하는데 많은 노력이 필요하다. 이에 본 시스템에서는 Fig. 14(a)과 같이 전체 접근정보 리스트에 대한 요약정보를 제공함으로써, 관리자가 접근정책 총 개수와 정책 간 관계이상이 발생한 정책 개수 및 유형에 대한 요약정보를 상위 계층으로부터 쉽게 알 수 있게 한다. 특히 시각화 공간 중앙 상단에 해당 정보를 가시화함으로써 관리자가 가장 먼저 정책 현황과 보안 상태에 대해 인지할 수 있도록 도와준다.

뿐만 아니라, 요약정보에 시각화된 정보(Fig. 14(a))의 세부내역으로써 Fig. 14(b)에서는 이상이 발생한 정책(rule seq.)을 기준으로 세부 요소(component)를 생성하여 정책 번호와 더불어 발생한 관계이상의 구체적인 유형(즉, 중첩, 중복, 연관 및

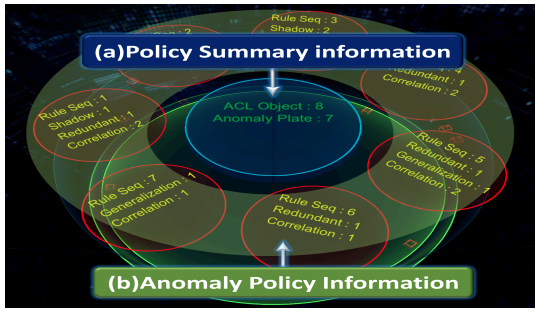


Fig. 14. Implementation of Upper Layer Components

일반화 이상)을 시각화한다. 표현되는 관계이상 내역(Fig. 14(b)의 붉은 원)은 각 정책의 관계이상 발생 횟수에 따라 유동적으로 생성되며, 화면상의 인터렉티브 인터페이스(Interactive interface)를 바탕으로 관리자는 해당 세부요소에 대해 클릭 이벤트 발생시켜 드릴다운(drill-down) 방식으로 더욱 구체적인 내용을 확인해 나갈 수 있다.

4.3 드릴다운 인터페이스 기반 접근정책 관리

본 논문에서 제안한 계층적 가시화 방법 및 드릴다운 인터페이스를 통하여 관리자는 효율적인 방화벽 접근정책의 관리가 가능하다. Fig. 15는 접근정책 관계이상 결과 확인 및 조치를 위한 간단한 시나리오를 나타낸다.

먼저 관리자는 (1)상위계층의 요약정보를 통해 현재 운용되고 있는 접근정책(ACL Object)의 총 개수와 정책들에서 발생한 관계이상의 총 횟수(Anomaly Plate)를 직관적으로 파악할 수 있다. 이 정보를 바탕으로 접근정책 간 세부 정보를 파악하기 위하여 가장 우선순위에 있는 정책을 선택하고(2), 해당 접근정

Fig. 15. Scenario of ACL Management based on Drill-Down Interface

책 플레이트의 클릭을 통해 드릴다운 검색을 수행한다(3). 시스템은 Fig. 15에서와 같이 선택된 3번 정책에 발생한 2가지 중첩이상과 1가지 중복이상의 세부내역을 테이블 형태로 제공해주며(5) 이를 통해 관리자는 이상행위의 종류와 정책의 선택(4)을 통해 추가 검색을 수행할 수 있다.

뿐만 아니라, 관리자는 특정 관계이상만을 선택(필터링)하여 복잡한 정책 간 관계들 속에서 원하는 정보를 쉽게 파악할 수 있다. Fig. 16에서와 같이 하위계층의 가시화를 통하여 관리자는 확인하고자 하는 관계이상의 선택을 수행한다. 특히 정책과 관계이상의 그래프 연결선을 통하여 가장 복잡도(연결성)이 높은 정책을 쉽게 파악할 수 있으며, 이를 통해 관계이상 정책의 수정에 대한 우선순위를 부여하고 순차적으로 보완하여 수월하게 잔존하는 접근정책의 취약점을 감소시키는 것이 가능하다.

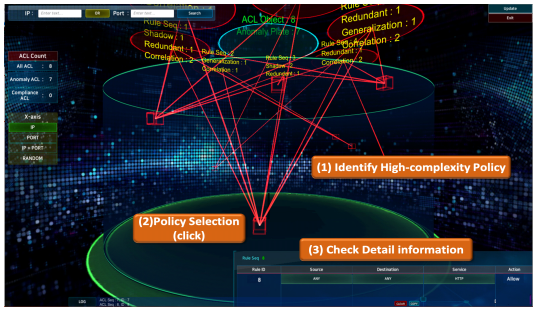


Fig. 16. Management ACL using Policy Connectivity

V. 활용 사례를 통한 유효성 검증

본 논문에서 제안된 방법론의 실제 활용 측면의 유효성을 검증하기 위하여, 기존 시스템과의 인터페이스 비교 및 가시화 점검도구를 활용한 대규모 네트워크상에서의 접근정책 취약점 보완과정에 대하여 알아본다.

5.1 접근정책 문제점 도출 및 결과 제공

3.1절에서 설명한 방법론을 본 논문에서 제안하는 실제 구현된 시스템에 적용하여 접근정책 간 문제점을 도출하고 그 결과를 시각화로 보여줌으로써, 정책 간 제안한 가시화 시스템의 유효성을 검증한다.

Fig. 17은 2.2절과 3.1절에서 설명한 방법론을 적용하여 구현된 화면으로, 방화벽 접근정책 100개를

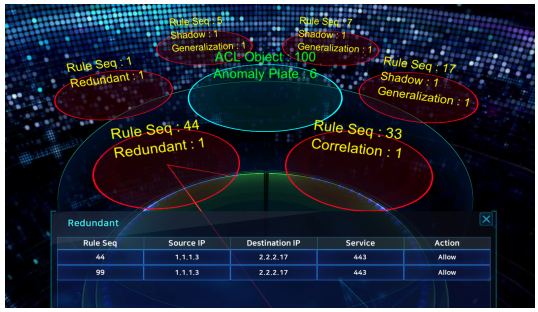


Fig. 17. Analysis of access policy problems and providing results

분석하여 총 6개의 관계이상 결과를 시각화로 제공한 것을 볼 수 있다. 예로, 상위 요약정보 중 분석된 결과로 ACL 44번과 ACL 99번은 중복정책임을 보여주며, 상세정보를 통해 모든 규칙이 동일한 규칙임을 보여주며, 이 외에도 중첩, 그림자 이상, 일반화 이상 등 본 논문에서 제안하는 정책의 관계이상 정보를 직관적으로 인지 및 관리할 수 있는 기능을 검증하였다.

5.2 기존 시스템과의 비교 및 활용 사례 분석

2.1절에서 알아본 바와 같이, 대부분의 방화벽 제조사들은 접근정책을 관리하기 위한 자체 인터페이스를 제공하지만 텍스트 테이블 형태만의 정보를 제공하기 때문에 네트워크가 복잡해질수록 관리자에게 어려움을 야기한다.

Table. 6은 논문에서 제안하는 시스템과 대표적으로 사용하는 방화벽 4개를 대상으로 관계이상 분석 결과를 그래프 및 표 등 다양한 시각화 기능을 제공하는지에 대해 비교하였다. 제안하는 시스템을 제외한 나머지 방화벽들은 접근정책 중 중복된 정책에 대해서만 정책 수립 시 관리자에게 알람 기능을 제공하였다. 반면에 제안한 시스템을 활용하여 접근정책의 최적화를 시도하는 경우는 Fig. 18과 같이 관계이상 유형을 사용자 인터페이스에 시각화로 표현하여 관계이상의 발생 여부(상위계층)와 이상을 유발한 정책(하위계층)을 즉각적으로 인지할 수 있으며, 접근정책의 문제점 확인/수정/삭제 등 불필요 정책(ANY, 취약한 Port)을 추가적인 작업 없이 직관적으로 파악하여 효율적으로 관리 할 수 있는 방안을 제공한다. 그림에서 쉽게 확인할 수 있다시피 이상을 발생시킨 정책 간 관계이상 그래프가 연결되어있고, 특히 다량의 관계이상이 발생하고 있는 정책을 복잡한 검색과정이 필요 없이

Table 6. Comparing Supported Functions between Proposed System and Conventional Systems

System Functions		Proposed System	AhnLab[15]	Paloalto[14]	Secui[21]	Wins[22]
Anomaly analysis	Shadowing	○	x	x	x	x
	Redundancy	○	○	○	○	○
	Correlation	○	x	x	x	x
	Generalization	○	x	x	x	x
Graphical interface (GUI)	Dashboard	○	○	○	○	○
	Interactive user interface	○	x	x	x	x
	Visual chart elements	○	○	○	○	○

가장 먼저 확인할 수 있다.

Fig. 18은 실제 방화벽 운용 시에 발생한 관계이상의 예로써, 접근정책 규칙 중 'ANY' 옵션은 정책의 허용에 대해서는 사용하지 않는 것이 일반적이지만, 관리자의 부주의에 의해 사용하게 됨으로써 전체 100개의 접근정책 간 99개의 관계이상(중복)을 발생시킨 경우이다. Fig. 19와 같은 일반적인 방화벽 접근정책 관리 시스템을 통해 해당 문제를 파악하려면 텍스트 기반의 복잡한 정보에 대해 관리자는 관계이상이 발생한 모든 정책을 필터링해서 찾아낸 후, 순서 관계에 따라서 가장 선순위 정책부터 후순위 정책까지 전탐색(full search)을 통해 비교해나가야 한다. 하지만 본 논문의 가시화 시스템은 직관적으로 관계이상의 원인이 되는 정책을 분석하여 도출하여 요약정보로 보여주며 세부정보를 통해 정책의 활용도 및 문제점을 시각화로 표현해 줌으로써, 관리자는 직관적인 문제점을 파악하고 조기에 보안 취약점을 보완할 수 있도록 도와준다.

Fig. 19는 실제 Fig. 18에서 집중적으로 발생한 관계이상(중복) 문제점을 해결한 결과로써, 이상현상 수정을 위하여 관계 그래프가 집중된 정책을 손쉽게 확인하고 해당 정책의 'ANY' 허용 옵션을 '특정 IP' 허용으로 간단히 변경을 수행하였다. 관계이상 해소 결과는 상위 계층의 요약정보에서 관계이상 발생 개수가 99개에서 4개로 줄어든 것을 통해 직관적으로 파악이 가능하며, 시각화로 남아있는 그래프의 숫자를 통해서도 쉽게 파악이 가능하다. 이와 같은 가시화 시스템의 드릴다운 검색 방법을 통해서 복잡한 관계이상 발생 시에도 빠르게 검색 및 보완이 가능하며, Fig. 19에 존재하는 나머지 관계이상도 같은 방법을 통해 효율적인 접근정책 운용이 가능함을 확인 할 수 있다.

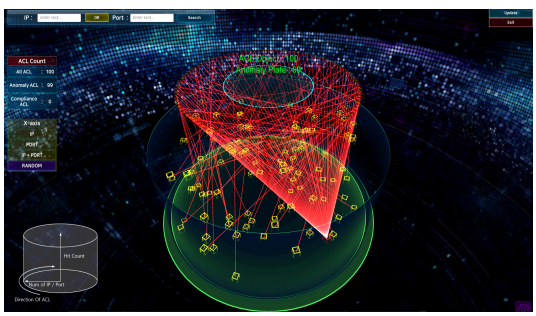


Fig. 18. Complex Anomaly Status on Real-world Situation

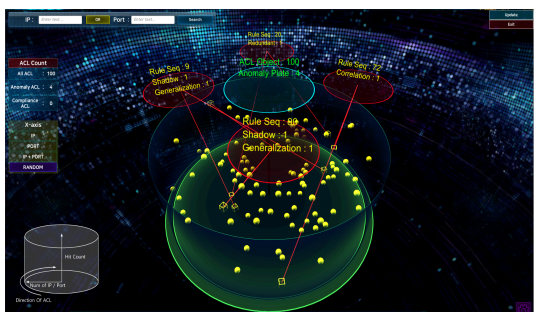


Fig. 19. Security Condition after Revising Anomaly Policy

VI. 결론 및 향후연구

본 논문에서는 보안상 취약점을 발생시킬 수 있는 방화벽 접근정책 간 관계이상을 직관적으로 파악하고 보완할 수 있는 새로운 계층적 가시화 방법론을 제안

하였다. 제안된 가시화 방법론은 상위계층과 하위계층으로 나뉘어 접근정책 및 관계이상에 대하여 각각 요약 및 세부 정보를 제공하며, 특히 사용자(관리자) 측면에서 친화적인 3D 기반 드릴다운 인터페이스를 통해 복잡한 대규모 네트워크의 직관적인 방화벽 접근정책 관리를 가능하게 하였다. 뿐만 아니라, 제안한 방법론의 유효성을 검증하기 위하여 실제 기관에서 운용중인 방화벽의 접근정책 분석을 통한 특징과 문제점 파악 과정을 기존 시스템과 비교하여 살펴보았으며, 특히 방화벽의 수많은 텍스트 기반 접근정책을 새로운 시각화 방법론을 통한 분석 및 결과를 제공하는 것만으로도, 기존의 정책을 관리하기 위한 방법들보다 더 효율적인 방법이 될 수 있음을 확인하였다.

다만, 본 논문에서는 단일 방화벽의 분석을 위한 가시화 방법론을 제안하였으나 대규모 네트워크에서 일반적으로 활용되는 다중 방화벽 방식의 접근정책 분석 및 관계이상 가시화 방법을 향후 추가적으로 진행할 예정이다. 또한 방화벽 보안관리에서 중요한 요소인 'ANY' 허용정책, 취약한 불필요 서비스(Port) 및 유해 IP관리 등과 같은 부분을 즉각적으로 인지 할 수 있는 가시화 표현을 통해 잔존하는 위험요소를 직관적으로 관리 할 수 있는 연구를 지속적으로 진행할 예정이다.

References

[1] Michael Cooney, "Network World 2020 State of the Network: SD-WAN, edge networking and security are hot", NetworkWorld, 14 Apr. 2020, IDG Communications, Inc. https://www.networkworld.com/article/3537559/state-of-the-network-sd-wan-edge-networking-and-security-issues-heat-things-up.html, Accessed 18 June 2020.

[2] W. Stallings, "Network security essentials: applications and standards.", pp. 374-397, 2016.

[3] E. S. Al-Shaer and H. H. Hamed, "Modeling and management of firewall policies." IEEE Transactions on network and service management 1.1, pp. 2-10, 2004.

[4] T. Tran and E. S. Al-Shaer, R. Boutaba, "PolicyVis: Firewall Security Policy Visualization and Inspection." LISA. Vol. 7. pp. 1-16, Nov. 2007.

[5] E. S. Al-Shaer and H. H. Hamed, "Firewall policy advisor for anomaly discovery and rule editing." International Symposium on Integrated Network Management. Springer, Boston, pp. 17-30, Mar, 2003.

[6] A. K. Meena and N. Hubballi, "NViZ: An Interactive Visualization of Network Security Systems Logs." 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS). IEEE, pp. 685-687, Jan, 2020.

[7] Ui-Hyong Kim and Jung-Min Kang, Jae-Sung Lee, Hyong-Shik Kim, Soon-Young Jung, "Practical firewall policy inspection using anomaly detection and its visualization." Multimedia tools and applications 71.2, pp. 627-641, 2014.

[8] F. Mansmann and T. Göbel, W. Cheswick, "Visual analysis of complex firewall configurations." Proceedings of the ninth international symposium on visualization for cyber security, pp. 1-8, 2012.

[9] A. Wool, "Trends in firewall configuration errors: Measuring the holes in swiss cheese." IEEE Internet Computing 14.4, pp. 58-65, 2010.

[10] K. Ingham and S. Forrest, "A history and survey of network firewalls." University of New Mexico, Tech. Rep, 2002.

[11] Y. Bartal and A. Mayer, K. Nissim, A. Wool, "Firmato: A novel firewall management toolkit." Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No.

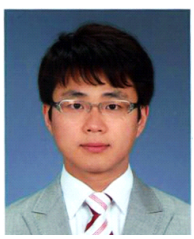
99CB36344). IEEE, pp. 17-31, May, 1999.
〔12〕 Q. Duan, and E. S. Al-Shaer, "Traffic-aware dynamic firewall policy management: techniques and applications." IEEE Communications Magazine 51.7, pp. 73-79, 2013.
〔13〕 H. Hu and G. J. Ahn, K. Kulkarni, "Detecting and resolving firewall policy anomalies." IEEE Transactions on dependable and secure computing 9.3, pp. 318-331, 2012.
〔14〕 Paloalto Networks, PA-Series user manual, https://www.paloaltonetworks.co.kr/network-security/pa-series, Accessed 21 June 2020.
〔15〕 AhnLab, TrusGuard Firewalls, https://www.ahnlab.com/kr/site/product/productView.do?prodSeq=10, Accessed 24 June 2020.
〔16〕 Apache Tomcat, Tomcat 7.0.104 Software, http://tomcat.apache.org/, Accessed 23 June 2020.
〔17〕 MariaDB Foundation, MariaDB 10.3, https://mariadb.org/, Accessed 23 June 2020.
〔18〕 Redislabs, redis 6.0, https://redis.io/, Accessed 23 June 2020.
〔19〕 Unity Techinologies, Unity Core Platform, https://unity.com/, Accessed 23 June 2020.
〔20〕 Likert, Rensis. "A technique for the measurement of attitudes." Archives of psychology (1932).
〔21〕 SECUI, SECUI MF2, https://www.secui.com/product/mf2/, Accessed 25 June 2020.
〔22〕 Wins, Sniper NGFW, http://www.wins21.co.kr/product/product_030101.html?num=28/, Accessed 25 June 2020.

〈저 자 소 개〉

김 태 용 (Taeyong Kim) 정회원
2014년 2월: 목원대학교 정보통신공학과 졸업
2016년 2월: 공주대학교 융합과학과 석사
2016년 6월~2019년 3월: SK인포섹 책임
2019년 4월~현재: 한국과학기술정보연구원 과학기술사이버안전센터 연구원
〈관심분야〉 보안관제, 네트워크 보안, 네트워크 가시화, 정보시스템 취약점 점검・분석

권 태 웅 (Taewoong Kwon) 정회원
2012년 2월: 숭실대학교 컴퓨터학부 졸업
2014년 8월: 고려대학교 정보보호대학원 정보보호학과 석사
2014년 12월~현재: 한국과학기술정보연구원 과학기술사이버안전센터 연구원
〈관심분야〉 정보보호, 보안관제, 네트워크 보안, 네트워크 가시화

이 준 (Jun Lee) 정회원
2010년 2월: 한국항공대학교 정보통신공학과 졸업
2012년 2월: 한국항공대학교 정보공학 석사
2017년 8월: 한국항공대학교 정보공학 박사
2017년 4월~2017년 11월: 일본산업기술종합연구소(AIST) 연구보조원
2017년 12월~2019년 12월: 일본산업기술종합연구소(AIST) 박사후연구원
2019년 12월~현재: 한국과학기술정보연구원 과학기술사이버안전센터 선임연구원
〈관심분야〉 인공지능, 보안관제, 지식추출, 자연언어처리, 네트워크 보안



이 윤 수 (Younsu Lee) 정회원
2007년 2월: 전남대학교 산업공학과 졸업
2010년 2월: 충남대학교 대학원 컴퓨터공학과 석사
2017년 2월~현재: 고려대학교 대학원 컴퓨터공학과 박사과정
2007년 3월~현재: 한국과학기술정보연구원 과학기술사이버안전센터 선임기술원
〈관심분야〉 차세대 보안관제기술 연구・개발, 보안이벤트 실시간 가시화, 정보시스템 취약점 점검・분석

송 중 석 (Jungsuk Song) 정회원
2003년 2월: 한국항공대학교 통신정보공학 졸업
2005년 2월: 한국항공대학교 정보공학 석사
2009년 3월: 교토대학교(일본) 지능정보학 박사
2009년 4월~2010년 9월: 일본정보통신연구원 정보통신 보안연구소 전문연구원
2010년 10월~2011년 9월: 일본정보통신연구원 네트워크 보안연구소 선임연구원
2011년 10월~2018년 3월: 한국과학기술정보연구원 과학기술사이버안전센터 선임연구원
2018년 3월~현재: 한국과학기술정보연구원 과학기술사이버안전센터 책임연구원
2012년 9월~현재: 과학기술연합대학원대학교 데이터 및 HPC 과학 교수
〈관심분야〉 보안관제, 침해사고대응, 인공지능, 네트워크 보안