웹방화벽 기술동향 파악 및 시험방법론

조인준* · 김선영*· 김찬중*

*배재대학교

Web application firewall technology trends and testing methodology

In-june Jo* · Sun-young Kim* · Chan-joong Kim*

Pai chai University

E-mail : kcjzzang333@naver.com

요 약

기존 방화벽은 네트워크 계층의 보안은 지원하나 더 상위계층인 애플리케이션 계층의 취약한 웹 어플리케이션 보안은 지원하지 못하고 있는 실정이다. 이러한 상황에서 웹 애플리케이션의 취약점을 방어할 수 있는 웹방화벽(Web Application Firewall)은 기업의 중요한 보안문제를 해결하는 해결사로 자리 매김하고 있으며, 차세대에 각광받는 보안시스템으로 국내·외 시장에서 매우 활발한 시장을 형성할 것으로 전망된다.

그러나 아직 웹방화벽의 성능을 테스트할 수 있는 표준이 제시되지 않아 웹방화벽 제품들을 신뢰하고 선택하기엔 어려움이 있다. 기업에서는 자체적으로 BMT를 실시하기도 하나 개인은 성능테스트의 비용문제와 기술력에 한계가 있다.

본 연구에서는 국내 웹방화벽 업체가 실질적으로 활용 가능한BMT 평가 모델을 개발하였다. 제품 평가 기준인 ISO/IEC 9126에 의하여 8가지 제품 특성별로 웹방화벽의 성능과 특성에 맞는 항목을 도출하였다.

이로써 자사에서 평가해야 할 웹방화벽의 성능 테스트에 대한 부담을 해소할 수 있고 국내관련분야의 경쟁력을 강화할 수 있고 제품에 대한 신뢰도를 회복함으로 해외 제품에 대한 의존도를 감소할 수 있다.

ABSTRACT

Existing network layer firewall security support is one that does not support the higher layer, the application layer of a vulnerable web application security.Under these circumstances, the vulnerability of web applications to be able to defend a Web Application Firewall is positioned as a solver to solve the important security issues of businesses spotlighted in the next generation of security systems, and a very active market in the market other than domestic ·is expected to be formed.

However, Firewall Web has not yet proposed a standard which can be used to test the performance of the Web Application Firewall Web Application Firewall and select the products of trust hardly Companies in BMT conduct their own individual problems and the cost of performance testing technologies, there is a limit.

In this study, practically usable BMT model was developed to evaluate the firewall vendor. Product ratings ISO / IEC 9126, eight product characteristics meet the performance and characteristics of a web application firewall entries are derived.

This can relieve the burden on the need to be evaluated in its performance testing of Web firewall, and can enhance the competitiveness of domestic-related sectors, by restoring confidence in the product can reduce the dependence on foreign products.

키워드

웹 방화벽, 시험 방법론, BMT 평가모델, BMT 테스트

Ⅰ. 서 론

현대 사회는 정보화 사회이다. 정보화 사회인 만큼 웹도 끊임없이 발전하며 새로운 변화를 만들

어 가고 있다. 웹이 우리 사회에서 중요하고 꼭 필요한 존재이지만, 그만큼 정보보호 관련 사고들의 수가 증가하고 있다. 그 이유는 웹 공격의 특징을 살펴보면 웹 애플리케이션의 취약성이다. 웹은 통상적으로 웹 전용 루트 80, 443을 사용해 HTTP/ HTTPS의 소통이 이루어 진다. 하지만 방화벽, IDS, IPS, VPN 등의 기존 보안제품들은 열려진 80, 443 포트에 대한 필터링, 애플리케이션 레이어에 대한 필터링이 잘 이루어지지 않는다는 것이 문제다.

IPS와 웹 애플리케이션 보안제품을 비교해보면 IPS 역시 L7 스위치와 마찬가지로 IPS 제품이 보호하고자 초점을 맞추는 영역이 전체 네트워크라는 점이다. 따라서 IPS를 포함한 기존 방화벽, IDS, IPS의 경우 방화벽은 L4의 기능을 수행하므로 실제 패킷 내용에 대한 검사를 하지 않으므로 패킷의 위, 변조에 대한 보안이 불가능하고, IDS, IPS의 경우 시그니처 방식에 의한 계속적은 업데이트가 필요하므로 업데이트가 되어 있지 않은 새로운 웜이나 바이러스 공격, 해킹에 대한 차단 기능은 거의 불가능하다. 따라서 IDS, IPS는 현재 사용되어지고 있는 웹 애플리케이션에 대한 정보 이외의 다른 모든 정보는 드롭시킴으로서 쿠키 변조, 세션 하이재킹, 폼필드 변조, 파라미터 변조와 같은 새로운 공격 패턴이나 해킹 패턴에 대해서는 대응력이 취약하다.

이런 현 운용상황에 대한 구조적인 문제점을 극복하고 웹 취약성에 대한 해킹을 최소화하기 위해서 웹 애플리케이션을 위한 전용 보안제품이 요구되었으며 웹방화벽의 등장은 웹보안 문제의 해결사로 각광 받고 있다. 그러나 웹 애플리케이션 보안 제품의 형태와 기능은 기존 제품들과 비슷한 면도 있고 다른 면도 있지만 무엇보다 아직 제품 출시 초기시장이다 보니 명확한 형태에 대한 구별이 쉽지는 않은 형편이다. 따라서 정교하고 객관적인 BMT 서비스를 제공하기 위해 BMT 품질 평가 모델 개발이 시급하다고 할 수 있다.

II. 관련 연구

2.1) 웹 방화벽의 정의 및 구조, 분류

웹 애플리케이션 방화벽을 일반적으로 '웹 방화벽' 이라 부르는데, 애플리케이션의 계층 분석 기술과 정규화 기술을 바탕으로 특화된 검사 엔진을 탑재해서 URL에 따른 접근 제어 기능과 SSL 트래픽을 자체적으로 복호화 검사하여 처리하기에 기존의 보안 시스템과는 다른 차별성을 둔다.

웹 애플리케이션 방화벽은 분석해야 할 자료를 어디에서 얻는지에 따라 네트워크 기반과 웹 서버 기반으로 나누는데 네트워크 기반의 방화벽은 HTTP/ HTTPS 트래픽을 분석함으로 웹 서버의 종류와 상관없이 보호가 가능한데 비해, 웹 서버 기반은 웹 서버가 제공하는 API 기반으로 구현 되 해당 웹 서버의 플러그인 형식으로 탑재된다.

웹 2.0은 대화형 웹 프로그램을 사용하여 자바스크립트 같은 기술의 사용이 급증하였기에 보안상 문제점이 현재 많이 존재하고 있고, 악성 코드를 침투시키거나 데이터 조작을 통해 기존의 서비스에 영행을 끼치는 여러 가지 공격이 가능하다.

이러한 허점을 없애기 위해 기존의 모든 웹 코드를 수정하는 것에는 시간이 많이 걸릴 뿐더러, 기존의 방화벽으로는 이러한 공격에 대응하는 것이 부족하기에 웹 방화벽의 필요가 더욱더 절실해지고 있다.

웹 방화벽의 분류는 첫 번째로 설계 방식인 아키텍처, 또는 물리적 구성 방식에 따른 분류로써 네트워크 기반 웹 방화벽과 호스트 기반 웹 방화벽이 있다.

- 네트워크 기반 웹 방화벽

네트워크 기반 웹 방화벽은 방화벽이나 침입 방지 시스템과 유사하게 네트워크 구간에 인라인 트랜스패런트 및 프락시 방식으로 구성되며 전송되는 웹 트래픽에 대한 분석 및 차단 기능을 수행한다.

- 호스트 기반 웹 방화벽

호스트 기반 웹 방화벽은 각 웹 서버에 설치된 보안 에이전트와 마스터 서버, 그리고 관리자용 콘솔의 3-Tier 환경으로 구성되며, 웹 서버의 에이전트가 해킹 시도 및 이상 징후를 탐지하고 적용된 정책에 따라 차단 및 모니터링을 수행한다.

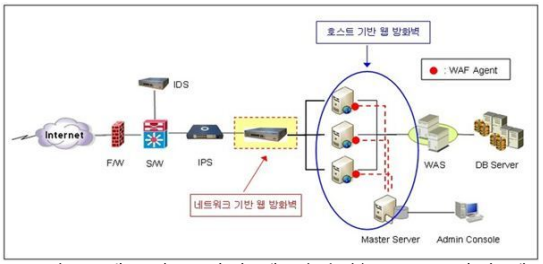

그림 1. 네트워크 기반 웹 방화벽/ 호스트 기반 웹 방화벽

두 번째로 내부 아키텍처 및 구현 알고리즘에

따른 분류를 살펴보겠다.

이 방식으로는 프락시 방식과 필터링 방식이 있다.

- 프락시 방식

웹 서버 앞단에 웹 방화벽이 클라이언트의 요청을 받아 필터링 처리 한 후, 다시 웹 서버와 재접속을 맺는 방식(대리접속 방식)으로, 초창기의 소프트웨어 기반 및 하드웨어 기반 웹 방화벽에서 적용된 방식이다.

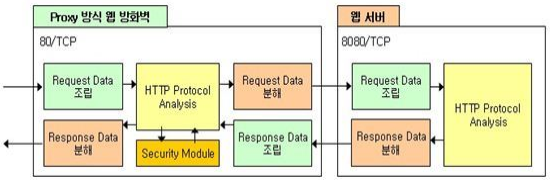

그림 2. Proxy 방식 웹 방화벽

- 필터링 방식

웹 방화벽이 웹 서버의 플러그인 모듈처럼 동작하는 방식으로 클라이언트의 요청을 받은 웹 서버가 처리 대기 상태에서 보안 모듈에 의해 필터링 처리된 후 정상 트래픽에 대해서만 클라이언트에게 응답하는 방식이다.

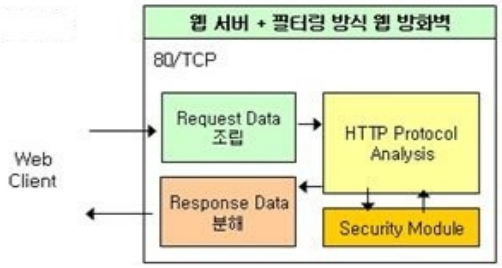

그림 3. Filtering 방식 방화벽

2.2) ISO-9126

ISO-9126은 소프트웨어 품질의 특성을 정의하고 품직 평가의 Metrics를 정의한 국제 표준으로 사용자, 개발자 관점에서 본 소프트웨어의 품질 특성에 대해 설명하고 있다.

주요한 품질의 특성 및 하부 부특성은 다음과 같다.

표 1. 소프트웨어 품질 특성

소프트 웨어 품질					
기능성	신뢰성	사용성	효율성	유지보수성	이식성
-적합성 -정확성 -상호운용성 -보안성 -준수성	-성숙도 -오류허용성 -회복성 -준수성	-이해성 -교육성 -운영성 -친밀성 -준수성	-시간반응성 -자원효율성 -준수성	-분석성 -변경성 -안정성 -시험성 -준수성	-적응성 -설치성 -공존성 -교체성 -준수성

-기능성 : 특정 조건에서 사용될 때 명시된 요구와 내재된 요구를 만족하는 기능을 제공하는 소프트웨어 제품의 능력

-신뢰성 : 명세된 조건에서 사용될 때, 성능 수준을 유지할 수 있는 소프트웨어 제품의 능력

-사용성 : 명시된 조건에서 사용될 경우, 사용자에 의해 이해되고, 학습되고 사용되고 선호될 수 있는 소프트웨어 제품의 능력

-효율성 : 명시된 조건에서 사용되는 자원의 양에 따라 요구된 성능을 제공하는 소프트웨어 제품의 능력

-유지보수성 : 소프트웨어 제품이 변경되는 능력. 환경, 요구사항 및 기능적 명세에 따른 수정, 개선, 혹은 개작 등이 포함

-이식성 : 한 환경에서 다른 환경으로 전이될 수 있는 소프트웨어 제품의 능력

III. 웹 방화벽 시험 방법론 개발

BMT 평가 항목을 도출하기 위하여 먼저 8가지 구분 항목을 웹 방화벽 관점에 적용하여 각 구분 항목별로 기술하고, 이를 근거로 최종적으로 BMT 모델을 도출한다.

1. 웹 방화벽의 기능성(Functionality)

웹 방화벽의 품질 평가에 있어서 기능성이란 소프트웨어가 특정 조건에서 사용될 때 명시된 요구와 내재된 요구를 만족하는 기능을 제공하는 소프트웨어 제품의 능력으로 다른 품질 특성들은 주로 소프트웨어가 언제, 어떻게 하는 것에 관련이 있으나 기능성은 기능적 요구를 충족하기 위해서 소프트웨어가 무엇을 하는가에 평가의 관점이 있다고 할 수 있으며 웹 방화벽의 경우 탐지 기능이 주 기능이므로 탐지와 관련된 소프트웨어적 하드웨어적 기능이 잘 제공되어 지는지 그 요소는 무엇인지, 사용자 문서에

명확히 서술하도록 하고 이러한 기능들이 제대로 작동하는지를 평가하여야 한다. 그 외에도 웹 방화벽의 기능과 성능을 충분히 고려한 평가가 이루어져야 한다.

웹 방화벽은 기능적인 측면이 가장 중요하므로 본 연구를 통해서 조사된 웹 방화벽의 기능들에 대한 내용이 모두 기능성 평가 항목에 제시되어 져야 할 것이다.

국내외 시스템을 모두 적용하여 가장 주가 되는 기능에서부터 각 회사의 제품들이 부가적으로 제시하는 기능까지 모두 적용하여 항목을 도출하였으며 제품 설명서에 제시한 기능을 참고로 평가항목을 도출하였다.

기능성에서 체크되어져야 할 몇 가지를 기술하면 다음과 같다.

가. 탐지 기능

웹 애플리케이션의 취약점을 이용한 공격에 대하여 정확한 탐지가 가능하여야 한다. 버퍼 오버플로우나, 쿠키 변조, 웹 서버에 URI요청시 악의적인 파일의 Include를 탐지하여야 한다. 웹 서버/웹 애플리케이션의 오류를 야기할 nt ldT는 표준에 어긋나는 URI 요청시 이를 차단하여야 한다.

로그 관리에서는 출발지 IP나 목적지 URI별 로그 검색 관리를 통하여 악의적인 근원지를 파악하거나 공격 목적지 URI별로 검색지원이 가능하여야 하며 이러한 기능이 제공되는지 파악해야 한다. 또한 IDS/IPS에서 처럼 단순 시그니처 비교(패턴매칭)방식은 오히려 오탐률을 높일 뿐이다. 좀더 지능적인 탐지 기능 즉, 자가학습/ 운영 모드게 제공되고 있는지도 파악해야 한다.

표 2. 탐지기능 평가 항목

구분	평 가 항 목	
탐지기능	1) Buffer Overflow	버퍼를 초과하는 악의적인 코드 전송여부
	2) Cookie Poisoning	쿠키 변조와 접근 권한, 쿠키 도용 여부
	3) Cross Site Scripting	악성 스크립트를 전송하게 하는 공격 탐지
	4) Directory Listing	URL에 웹컨텐츠가 없을 경우 탐지 여부
	5) DoS	대량의 접속 요청 트래픽 탐지
	6) Error Handling Problem	웹서버나 DB 오류메시지를 통한 공격 탐지
	7) Extension Filtering	보안상 위협이 되는 실행 파일의 업로드 방지
	8) File Upload	공격 도구 업로드 방지
	9) Include Injection	웹서버에 URI 요청시 악의적인 파일 Include 탐지 및 차단
	10) Input Contents Filtering	문자열 변환기능 탐지
	11) Forceful Browsing	주소창의 직접입력을 통한 임의 파일 접근 탐지
	12) Hidden Field Manipulation	Hidden Field 조작을 통한 데이터 위변조 공격 탐지
	13) Invalid HTTP	HTTP 표준에 어긋나는 접근 시도 차단
	14) Invalid URI	표준에 어긋나는 URI 요청 차단
	15) IP Filtering	특정 IP의 웹 트래픽 차단
	16) Privacy File Upload	개인정보 포함 여부 조사
	17) Privacy Output Filtering	개인정보 마스킹 처리 및 차단
	18) Privacy Input Filtering	개인정보가 서버에 전송될때 차단하는 기능
	19) Parameter Tampering	웹애플리케이션의 URL이나 인자를 임의 변경 탐지
	20) Response Header Filtering	웹서버로부터 필요 이상의 정보를 주는 필드를 필터링
	21) Request Method Filtering	불필요한 HTTP 요청이나 공격에 악용될 수 있는 HTTP Method 필터링
	22) SQL Injection	내부DB의 데이터 유출, 변조 등 공격 탐지
	23) Stealth Commanding	웹애플리케이션에서 외부 프로그램 연결시 악의적인 명령어 삽입 공격 탐지
	24) Suspicious Access	도구에 의한 접속 등을 탐지
	25) Unicode Directory Traversal	Unicode로 인코딩된 주소를 통한 파일/디렉토리 접근 탐지
	26) Web Site Defacement	홈페이지 위변조 탐지

계산 결과	총 26개에 대한 정보를 평가하는 항목으로 제시하였으며 항목별 평가를 통해서 품질을 평가함		
측정 방법	평가 유형 1을 적용하여 Y/N/NA로 평가함		
계산식	제품 정보제공 = (Y로 측정된 항목 수) / (전체 평가 항목 수)		
결과값		개선사항	

나. 접근 제어

웹 방화벽은 URI별, IP별 접근제어를 지원한다. 접근제어를 위해 일반적으로 웹 방화벽은 두 모델을 혼합하여 구현하고 있다. 먼저 Positive Security Model 기반의 필터링 모듈이 HTTP 요청을 검사한다. 이 모듈에서는 등록된 URI에 대한 접근제어 수행, 특정 Method의 수행 여부 제어 등 접근 및 사용이 허가된 목록을 기준으로 필터링을 수행한다. 공격에 대한 대응으로 공격이 탐지된 HTTP 요청은 바로 차단하거나 다른 URI로 보낼 수 있다. 이러한 기능을 지원하고 있는지 체크하여야 하며 또한 탐지 항목에 대하여 DB로 구축하여 정보를 저장하고 있는지 체크하여야 한다.

표 3. 접근제어기능 평가 항목

구분	평 가 항 목	
접근제어기능	1) URI별 접근 제어	홈페이지 주소(URI)별 접근 제어
	2) IP별 접근 제어	출발지 IP별 접근 제어
	3) IP Black List 관리	동일 IP에서 지속적인 공격시 접속 차단
	4) 트래픽 분석을 통한 자동 학습	보호해야 할 URI를 웹서버 트래픽 분석을 통해 자동 등록
	5) 학습/운영 모드 제공	URI학습 및 탐지만 수행하는 학습모드와 차단을 수행하는 운영모드 구분
계산 결과	총 5개에 대한 정보를 평가하는 항목으로 제시하였으며 항목별 평가를 통해서 품질을 평가함	
측정 방법	평가 유형 1을 적용하여 Y/N/NA로 평가함	
계산식	제품 정보제공 = (Y로 측정된 항목 수) / (전체 평가 항목 수)	
결과 값		개선사항

다. 대응 기능

공격을 차단하였거나 외부로부터 침입을 탐지하였을 경우 바로 관리자에게 보고하는 기능을 평가하여야 한다. 실시간 모니터링의 기능이 동작되면서 이상행동이 탐지되었을 경우 관리자에게 이메일이나 휴대폰 전송 등 즉시 보고하는 체계가 있는지 체크하여야 하며 또한 통계 보고서도 구축되어 매월 혹은 주간의 정확한 통계가 이루어져 보고 되고 있는지 정확히 평가하여야 한다.

표 4. 대응기능 평가 항목

구분	평 가 항 목	
대응기능	1) 침입 차단	공격 탐지시 접속 차단
	2) 에러 코드 전송	공격 탐지시 공격자에게 HTTP에러코드 전송
	3) Page Redirection	공격 탐지시 지정된 웹페이지로 강제 이동
	4) 복수개의 경고 페이지	정책/개인정보/도메인별 별도의 경고 메시지 Alert 기능 지원 여부
계산 결과	총 4개에 대한 정보를 평가하는 항목으로 제시하였으며 항목별 평가를 통해서 품질을 평가함	
측정 방법	평가 유형 1을 적용하여 Y/N/NA로 평가함	
계산식	제품 정보제공 = (Y로 측정된 항목 수) / (전체 평가 항목 수)	
결과값		개선사항

2. 웹 방화벽의 상호운영성(Interoperability)

망의 구조를 고려해 보아야 하는데 우선 어느 망에 접속을 해도 전체망에 영향을 주지 않아야 하고 새로운 장비로 교체시 혹은 서로 장비들끼리 마찰이 없이 잘 작동 되어야 한다. 물론 전체 트래픽에도 영향을 주지 말아야 하고 설치와 제거가 쉬워야 한다.

3. 웹 방화벽의 보안성(Security)

보안성에 대해서는 언급하지 않는 것이 타당하다고 보여진다. 웹 방화벽 자체가 보안장비이며 각 회사는 자사의 제품에 대하여 이미 CC 인증 평가를 대부분 받아 시장에서 활발한 경쟁을 이루고 있는 상태이다. 그러므로 보안성 평가에 대하여는 앞에서 언급한 CC 평가로 갈음한다. 그러나 BMT 평가 모델에서는 웹 방화벽에서 지원되는 보안성에 대하여 구체적으로 기술한다.

4. 웹 방화벽의 신뢰성(Reliability)

소프트웨어가 규정된 조건에서 사용될 때 규정된 성능 수준을 유지하거나 사용자로 하여금 오류를 방지할 수 있도록 하는 소프트웨어 제품의 능력으로 일정 단위 시간 동안 소프트웨어가 고장이나 결함없이 제대로 성능을 발휘하는 능력을 소프트웨어 신뢰성이라 할 수 있으며 웹 방화벽의 신뢰성 평가는 장비의 고장과 함께 공격에 어느 정도 강한지 견고성을 중심으로 평가되어져야 하며 특히 치명적인 오류가 발생했을 경우 어떻게 대처하고 있는지 제시되어져야 할 것이다.

5. 웹 방화벽의 사용성(Usability)

웹 방화벽이 규정된 조건에서 사용될 때 사용자에 의해 이해되고 학습되며 선호될 수 있게 하는 소프트웨어 제품의 능력이 사용성을 평가하는 평가항목으로 구성되어질 것이며 웹 방화벽의 사용자가 실제로 차단과 사전 예방의 기능에 대한 확인여부 및 모니터링을 하는 과정에서 쉽게 제품을 학습할 수 있도록 구성되었는지를 평가하고 특히 사용자 관점에서 인터페이스가 충분히 고려되어졌는지를 평가하여야 한다.

6. 웹 방화벽의 이식성(Portability)

다양한 환경에서 운영될 수 있는 소프트웨어 제품의 능력을 평가하는 품질 특성인 이식성은 소프트웨어를 운영하기 위하여 요구되는 하드웨어, 소프트웨어 및 운영체제 등의 환경을 평가하기 위한 항목이다. 웹 방화벽의 경우 지원되는 환경을 조사하고 다른 장비와의 충돌여부 및 연동성을 파악하여야 할 것이다.

7. 웹 방화벽의 효율성(Efficiency)

웹 방화벽은 통상적으로 위험을 탐지하거나, 어느 정도 신속하게 탐지하는지, 또는 대응하는데 평균 처리시간을 제시하여야 하며 그 반응 시간의 적절성을 체크하여야 한다. 자원에 대한 효율성은 웹방화벽 시스템의 메모리 사용 정도, 시스템의 데이터 전송 속도 등 적정성을 체크하여 최적의 기능을 제공하고 있는지 평가해야 한다.

8. 웹 방화벽의 유지보수성(Maintainability)

유지보수성이란 소프트웨어 제품을 변경할 수 있는 능력을 말하는 것으로 변경에는 운영환경과 요구사항 및 기능적 사양에 따른 소프트웨어의 수정, 개선 혹은 개작 등이 포함되어지며 웹 방화벽의 경우 운영환경에는 크게 영향을 받지 않을 것으로 예상되며 성장단계에 있으므로 업그레이드 버전 즉, 기능의 추가가 쉽게 이루어질 수 있는지 그에 따른 모듈 추가가 용이한지 변경을 중심으로 평가할 수 있도록 하여야 할 것이다.

Ⅳ. 결론

웹보안의 해결책으로 등장한 웹방화벽은 차세대 보안장비로 각광받고 있으나 선택의 어려움이 있었다. 특히 우리나라의 장비 현실은 아직도 민간, 공공 부분을 막론하고 특정 벤더 즉, 인지도가 높은 벤더에 의한 독점화가 심각한 수준에 이르렀다. 이러한 현실은 시장 왜곡과 기술 종속을 심화시킬 뿐만 아니라 웹 방화벽의 품질 향상을 저해시키는 요인이 될 수 있다.

본 연구에서는 웹방화벽 BMT 평가 모델을 개발하였다. 이는 개발 업체의 제품 평가 모델 개발에 대한 비용 및 인력 부담을 해소하고 웹방화벽의 신뢰성을 증진시키며 국내외 시장 활성화를 이루는데 기여할 것으로 전망한다.

참고 문헌

[1] 인터넷 침해사고 동향 및 분석 월보, 한국인터넷진흥원, 2012 Vol. 06.
[2]www.boan.com/news/download.php?subUploadDir...1355...
[3] Web Security Solution All Guide, 월간정보보호21c, 2008. 7.
[4] ITFIND 주간기술동향 통권 1312호, 2007. 9.
[5] http://isstory83.tistory.com/28
[6]http://www.datanet.co.kr/news/articleView.html?idxno=53251
[7] http://hackerboy.egloos.com/1056661
[8]http://www.datanet.co.kr/news/articleView.html?idxno=31302
[9] 2007 국내 정보보호산업 시장 및 동향 조사(연구보고서), 한국정보보호진흥원, 2007년.
[10] 2010 국내 정보보안산업 실태조사(연구보고서), 한국인터넷진흥원, 2010년
[11] 2011 국내 정보보안산업 실태조사(연구보고서), 한국인터넷진흥원, 2011년
[12] Yankee Group, Application Assurance Platforms Arise from Web Application Firewall Market's Ashes, 2005년12월
[13] Gartner, Hype Cycle for Data and Application Security 2007
[14] Stratecast(a Division of Frost & Sullivan), Web

Application Firewalls Poised to Become Mainstream, , 2009년 2월
[15] Technavio, Global Web Application Firewall Market 2009-2013, 2010년 3월
[16] Forrester Research, Web Application Firewall: 2010 And Beyond, 2010년 2월
[17] Frost&Sullivan, Web Application Firewall-A Critical Defence for an Information-Centric World, 2010년 3월
[18] 정혜정외, 모바일 RFID 미들웨어 품질 평가 모델 개발, TTA 연구과제보고서, 평택대학교, 2007년.
[19] 권원일, 정창신, 소프트웨어 제품 품질에 관한 국제 표준화, TTA 저널, 제85호, 2003년 1월.
[20] 오영배, 소프트웨어 제품 품질평가, TTA 저널, 제 105호, 2006년 6월.
[21] 정연서, 류걸우, 장종수, 네트워크 보안을 위한 ESM 기술 동향, ITFIND 주간기술동향 보고서, 2001년 12월
[22] 고종영외, 보안정책을 표현하는 침입차단시스템의 지식기반 모델링 및 시뮬레이션, 한국정보보호진흥원 위탁과제연구보고서, 2001년
[23] 국가 정보보호 기반조성 현황, 국가정보보호백서, 2007년
[24] OWASP, 2004년 1월호
[25]http://www.datanet.co.kr/news/articleView.html?idxno=43262
[26] http://isstory83.tistory.com/28