Journal of Digital Contents Society Vol. 11 No. 3 Sep. 2010(pp. 331-339)

네트워크 보안 서비스 향상을 위한 도메인 구조설계와 성능분석 방법

문송철*, 노시춘**, 정지문**

요약

네트워크 보안에서의 효율성은 침입차단 성능과 시스템 performance로 대표된다. 네트워크 보안의 성능 향상을 위해서는 네트워크 인프라스트럭쳐에서의 기능적인 효율성을 우선 확보해야 한다. 그동안 네트워크 보안 효율성 제고 달성에 관한 많은 방법론들이 연구되었다. 이 같은 연구의 목적은 인프라스트럭쳐에서의 효율성 메커니즘 구현을 통해 빠른 응답시간내에 보다 우수한 침입차단을 실현하는 것이다. 이를 위해서 네트워크 보안 도메인 효율성 구조를 설계하고 구조별 효율성 측정방법을 연구함으로써 인프라스트럭쳐상에서의 보안방법론 모델을 제안하였다. 본 연구에서 제안한 방법론을 통해 체계적인 도메인 설계와 측정방법을 실시할 경우 운용인프라스트럭쳐 시스템상에서 보안 효율성 확보가 가능함이 입증되었다.

A Study for a Method of Designing of Security Domain Infrastructure and Its Efficiency Measuring

SongChul Moon*, SiChoon Noh**, JiMoon Jung**

Abstract

On intranet system, it is essential element for providing information to decrease response time. To realize this efficiencies of response time of the network , a lot of research have been conducted. The purpose of the research and implementation is to shorten the response time of information system. We can realize final goal of information system through fast response time. This final goal of information system is to secure the performance efeciency within the required time. In order to acquire the method of warranty of fast response time, the efficient measurement method is essential. This research suggests a latency test techniques being used on infrastructure system and also offers a response time measurement methodology. Methodology proposed in this research has proven that it is possible to measure response time through the scheduled method. Also it is possible to develop a enhanced networking capabilities, and information system capabilities for the development of information system.

keywords : Security Domain, Infrastructure,Measuring,Efficiency

1. 서론

네트워크 보안도메인은 물리적, 논리적인 네트워크 경로상에서 보안기능 수행을 목적으로 트래픽 소통 영역과 그룹을 구분하고 구성하는 방법론의 개념이다. 네트워크의 형상과 보안 차단 위치를 구성한 아키텍쳐로서 오늘날 보안 침해 기술 고도화와 네트워크의 개방성, 트래픽 물량 급증은 정보시스템에 대한 침해 위협을 한층 제고시키므로 보안기능 수행은 도메인별로 네트워크 특성이 구분되며 이 특성을 보안기능 측면에서 관리 하므로서 네트워크 보안의 효율성을 제고하는 방법이 필요하다. 보안도메인은 일반적인 네트워크 구조를 보안측면에서 관리하므로 도메인 별차별화가 가능하므로 도메인별 보안 메커

※ 제일저자(First Author): 문송철
접수일:2010년 07월 14일, 수정일:2010년 09월 28일,
완료일:2010년 09월 30일
* 남서울대 컴퓨터학과 교수
moon@nsu.ac.kr
** 남서울대 컴퓨터학과 교수

니즘이 적용이 가능하다. 본 연구는 네트 워크는 어떤 구조와 기준으로 보안도메인이 설계되어야 하는가에 대한 방법론 개발을 위해 네트워크 형상(Topology) 결정요소 선정, 보안 도메인 설정기준 결정, 구조도 선택기준 결정, 차단위치 결정, 경로방역망 구성기준을 도출하고 이를 보안기능 효율성 측면에서 검증한다.

2. 네트워크보안 메커니즘 요구 사항

<표1> 네트워크보안 매커니즘 구성

구 분	구 성 요 소
보호대상 네트워크 자원	• 인트라넷, LAN, 개별 서버, 클라이언트 • 국가·정부, 공공 네트워크·기업용 네트워크 • 운영체계, 데이터베이스·어플리케이션
사용 자원	소프트웨어·하드웨어, 인적 자원, 절차 제도
방역 방법	소프트웨어 기술, 인프라 구조, 관리적 방역
방역기능	예방 기능, 진단 기능, 치료 기능, 차단 기능

네트워크 보안도메인은 먼저 보안 메커니즘을 구성하고 있는 구성요소 파악이 필요하다. 방역 매커니즘 구성요소는 침투 바이러스에 대처하는 보호대상 네트워크 자원, 방역 사용자원, 방역방법론, 방역기능 유형 등이 있다[4][8].

○ **보호대상 자원:** 바이러스로부터 보호되어야 할 자원의 종류를 말한다. 예를들면 네트워크 규모 기준으로 인트라넷 시스템, LAN 시스템, 개별서버, 개별 클라이언트로 구분해 볼 수 있고 사용자 그룹 유형을 기준으로 국가나 정보기관 네트워크, 기업 네트워크, 각종 공공 네트워크로 나눌 수 있다.

○ **사용자원:** 전산자원을 기준으로 운영체제, 데이터베이스 어플리케이션 등으로 구분해 볼 수 있다. 사용자원은 방역작업에 사용되는 소프트웨어, 하드웨어, 절차와 제도, 인적자원이 있으며 방역에 어떤 방법을 적용하느냐의 기준에 따라 소프트웨어를 사용하는 기술적 방법, 하드웨어와 소프트웨어를 혼용 적용하는 인프라 구조 방역, 인적자원과 절차, 제도 등을 이용하는 관리적 방역으로 나누어진다[3].

○ **방역방법론:** 방역방법론은 소프트웨어 기술 방역, 관리적 방역, 인프라구조 방역등 3가지 카테고리로 나누어질 수 있다. 소프트웨어기술 방역은 악성코드 방역용 소프트웨어를 이용하여 악성코드를 진단, 예방, 삭제하는 것으로 주로 방역 대상 자원에 소프트웨어를 설치하여 활용한다. 관리적 방역이란 관리적 보안 영역에서 기술된 바와 같이 보안침해사고 피해에 대처할 수 있는 안전관리에 관한 제도, 절차, 수칙 등을 말하며 위험요소를 정보시스템으로부터 격리 차단 제거하는 각종의 관리 기법이다. 인프라 구조 방역은 악성코드 차단 인프라구조의 구성을 최적화하여 악성코드를 차단하는 방법론이다.

○ **방역기능 유형:** 목표로 하는 방역기능으로서 예방기능, 진단기능, 치료기능, 차단기능 등의 종류가 있다. 보안기능 요구사항은 특정 시스템이나 구조상에서 구현되어야할 보안기능 명세서이다. 기능 매커니즘은 이 기능 요구사항을 충족시켜주는 알고리즘이며 정보시스템 각 영역별로 특성화된다. 기능 메커니즘은 기능 요구사항을 알고리즘과 정보기술로 결합을 통해 구현한다. 보안기능은 네트워킹과 보안 결합기능 이다. 네트워킹은 트래픽을 중계, 교환, 전송하는 데이터 통신 기능이며 보안기능은 이 과정에서 예방 기능, 진단 기능, 치료 기능, 차단 기능으로서 보안을 보증한다. 보안영역은 네트워킹과 별도로 분리되지 않으며 네트워크 구조에서 존재,가동되며 상호 연동을 통해서 기능을 수행할 수 있다[5][6]

3. 네트워크 보안 도메인 인프라 설계

3.1 프레임워크는 구조 설계

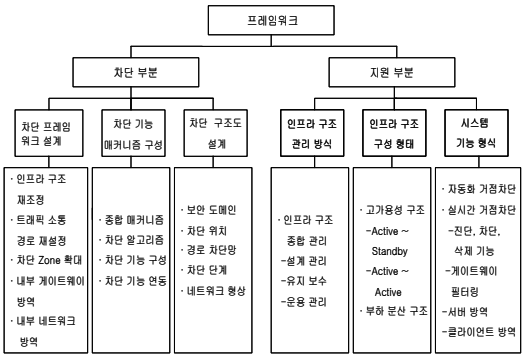
보안도메인 인프라 프레임워크는 구조를 구축하기위한 구조와 기능에 대한 기본 골격과 체계이다. 프레임워크는 구조 구현의 첫 번째 단계 과업으로 수행되고 구조 전반에 대한 골격을 형성하며 수행 방법론의 기본 구조를 형성한다. 프레임워크가 필요한 이유는 프레임워크가 구축됨으로서 인프라 하부구조와 기능이 구현되기 때문이다. 프레임워크는 톱-다운(Top-down) 구조의 상층부를 형성하여 하위계층 아키텍처 구조를 가이드 한다. 프레임워크를 구축하기 위해서는 먼저 기존구조의 한계와 문제점, 그 문제점에서 발췌되는 수정요소 그리고 이와 더불어 새로운 개념의 구조 요구사항이 결합되어 새로운 구조에 대한 설계사상이 수립되어야 한다.

이상과 같은 메커니즘은 다섯단계의 방역구간, 보안 인프라, 방역기능이 상호 연동되어 전체적인 방역 알고리즘을 구성한다[8][9].

① 기존의 네트워크 구조가 유일 소통 관문으로 설정되어 있는 외부스위치, 침입차단시스템은 그 자체를 방역 게이트웨이화 한다.

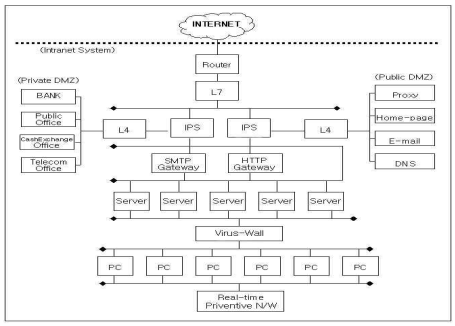
② 기존의 네트워크 구조가 유일 소통 관문이 존재하지 않는 내부 네트워크 유입관문, 내부 서버로 접속관문, PC자원 접속관문은 별도

의 방역 게이트웨이를 설정한다.
③ Tiers별 방역 분담구조는 네트워크 경로방역에서 트래픽 소통 구간별 방역기능 수행아키텍처이다.



(그림1) 네트워크 보안 도메인 프레임워크 모델

3.2 네트워크 경로방역망 설계기준



(그림2) 네트워크 경로방역망 설계 기준

방역 Zone은 스위치, 침입차단시스템, 내부게이트웨이, 서버 바이러스 월, Real-time 방역 네트워크 5개 Zone으로 구성한다. 각 방역 Zone에서는 구간의 특성을 고려하여 필수적 방역기능을 적용한다[8][10].

3.3 Tiers별 방역분담

경로방역이란 네트워크 인프라 구조방역 방법론중 거점방역 구조 운용시 발생하고 있는 방역누수와 방역 취약점을 해소시키기 위해서 네트워크 주요 경로에서 이동중인 악성코드를 차단하는 방법이다. 이 방식은 트래픽 소통경로 중 방역 Zone으로 설정된 주요경로의 진입관문에 차단용 게이트웨이를 설치하여 통과하는 모든 트래픽을 대상으로 감시기능과 필터링기능을 시행하는 것이다. 이상과 같은 순차적인 진단 과정을 통해 전체트래픽 소통구간중 방역기능 적용이 필요하고 기술적으로 가능하며 효율성이 기대되는 구간을 선정하여 다음과 같이 기본적인 방역 인프라 구조를 설계한다[9][11].

① 트래픽 통과경로를 따라 방역Zone을 구분하고 순차적 Tiers 단계마다 경로의 특성에 적합한 차별화된 방역방식을 적용한다.
② 기존의 경로방역 수단인 LAN 스위치 또는 침입차단 시스템 경로방역에 내부 게이트웨이(Interior Gateway) 방역과 서버 경로방역, 클라이언트 경로방역을 추가시킨다.
③ 내부 게이트웨이 방역은 트래픽 성격에 따라 SMTP 게이트웨이, HTTP 게이트웨이 방역, 기타 구간 방역으로 구분하여 경로별 차별화 방역이 필요.
④ 서버 방역은 인트라넷 내부 유통 바이러스 방역 대책으로 모든 서버자원을 대상으로 Server's 바이러스월을 설치한다.
⑤ 인트라넷 내부 클라이언트자원에 대한 경로방역으로서 PC자원을 대상으로 하는 Real-time 방역망을 구성한다.

<표2> Tiers별 방역분담

Tiers	네트워킹 기능	보안 기능	
		침입차단 기능	효율성지원 기능
스위칭	· 네트워크 로드밸런싱 · 캐시리다이렉션 · 서버로드 밸런싱 · 침입차단 로드밸런싱	· 웜 바이러스 차단 · 해킹 공격 차단 · 컨텐츠 스위칭 · 컨텐츠 필터링	· 서버 로드 밸런싱 · 침입차단 시스템 로드 밸런싱 · 네트워크 로드밸런싱 · 고가용성 구조 · 실시간 방역
침입차단 시스템 필터링	· 패킷필터링 · 접근제어 -IP,포트, 서비스 · 컨텐츠 필터링	· 메일 바이러스 필터링 · 패킷 필터링 · 접근 제어 -IP, 포트, 서비스 · 컨텐츠 필터링 · 사용자 인증 · 데이터 암호화	· 고가용성 구조 · 실시간 방역
게이트웨이 필터링		· 컨텐츠 필터링 · 해킹 차단 · 차단	· 실시간 방역 · 자동화 방역
서버 방역		· 유입차단 · 백신 업데이트 · 감염 진단 · 삭제	· 실시간 방역 · 자동화 방역
클라이언트 방역		· 유입차단 · 감염 진단 · 삭제 · 백신 업데이트	· 실시간 방역 · 자동화 방역

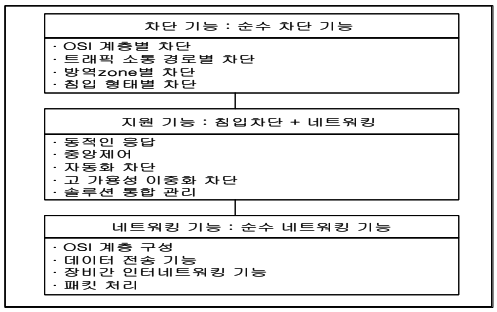
3.4 기능계층 구조 설계

동작 메커니즘 구조는 [그림3]과 같이 네트워킹 기능, 지원 기능, 보안 기능 3개영역으로 계층화된다.
○ **네트워킹 계층:**보안 인프라가 구성, 설정되는

기본틀인 네트워킹 계층의 기능을 말한다. 네트워킹 기능은 OSI 7 Layer별로 차별화된 네트워킹 기능구조를 형성하고 이 구조상에서 라우팅, 스위칭, 브로드캐스팅 등 인터네트워킹 기능, 데이터 전송 기능 그리고 패킷 처리기능을 수행한다.

○ **지원 기능:** 네트워킹 기능을 토대로 하지만 침입차단 기능 구현시 적용되어야할 필수적인 지원 또는 연관기능 이다. 지원기능은 다시 3개 세부영역으로 분류 되는데 고가용성 기능, 통합관리 기능 및 자동화 처리와 실시간 처리기능이다.

○ **침입차단 기능:** 인프라 구조의 목적에 해당되는 바이러스와 각종 악성코드 침입차단 기능이다. 침입차단 기능은 OSI 계층별 차단, 트래픽 소통경로별 차단, 차단Zone별 차단으로 분류될 수 있다. OSI 계층별차단은 OSI Layer2에서 Layer7까지의 계층별로 시행되는 차단기능 이다. 경로별 차단은 외부 라우터에서부터 최종 클라이언트까지의 트래픽 경로별로 수행되는 차단이다[10].

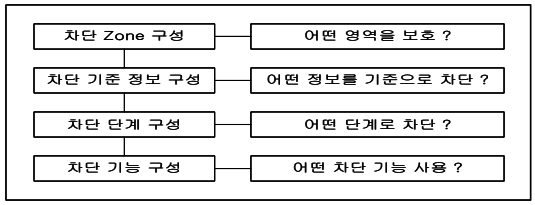


(그림3) 기능 계층 구조

3.5 보안 차단기능 기본구도

차단기능 기본구도는 차단 Zone별 차단, 차단 기준 정보별 차단, 차단 단계별 차단, 차단 기능별 차단으로 구성된다.

○ **차단 Zone별 차단:** 방역을 해야할 영역별로 어떤 기준으로 범위를 설정 하는가에 관한 것이다. 다음 [그림4]는 차단기능 기본구도 하에서 차단기능은 상호 어떤 연동관계를 구성하는지를 보여준다. 차단 Zone이 설정되면 그 결과를 토대로 차단 기준정보를 구성하고 이어서 차단단계를 구성한다. 그리고 이같은 제반 단계의 결과는 차단 기능 구성으로 나타난다. 차단기능 구성을 통해 실제적인 차단 기능이 구현 되도록 설계하였다[12][13].



(그림4) 침입차단 기능 기본구도

○ **차단 Zone:** 기존 구조의 하드웨어 리소스 기준은 각종 서버와 클라이언트를 방역대상 으로 삼는 것이다. 통합구조에서는 차단 Zone을 트래픽 경로별로, 정보자원별로, 하드웨어 리소스 로 세개의 카테고리로 구분하여 설정했다. 먼저 트래픽 경로는 설계 프레임워크에서 제시한 바와 같이 트래픽 경로를 기준으로 외부 라우터 - 외부 스위치, 외부 라우터 - 침입차단 시스템, 침입차단 시스템 - DMZ, 침입차단 시스템 - 내부 네트워크 등 4개 영역으로 편성한다.

○ **차단 기준 정보별 기준:** 기능 기본구도중 두번째 카테고리는 차단 기준정보별 기능이다. 차단을 어떤 기준정보, 어떤 키값으로 시행하느냐 하는 방법이다. 차단기능을 설명하기 위해서는 침투형태를 먼저 알아야 하는데 <표 6>에서는 Layer별 침투형태의 기능을 보여주고 있다. 차단 기준정보를 설정하기 위해서 Layer별 침투 형태를 검토한다. 침투형태는 Layer별로 구분된다. 2계층 차단 기준정보는 MAC주소, Layer3 차단 기준정보는 IP주소, 4계층의 경우 하위 계층 기준정보를 포함 TCP, UDP, ICMP 프로토콜 종류, TCP, UDP 포트번호로 설정된다. OSI계층에서부터 7계층까지의 기준정보는 컨텐츠 기반 정보를 기본으로 한다.

○ **차단 기능별 구성:** 차단기능이 어떤영역, 어떤종류로 구성되는가에 대한 기능이다. 차단기능은 현재 사용되는 영역별로 패킷스위칭, 패킷 필터링, 차단(Protection) 등으로 구성되는데 실제 현장에서 이같은 차단기능이 순수한 차단기능으로 구성되기도 하고 네트워킹 기능과 결합하거나 연동하여 구현되기도 한다. 이 구성에 따른 세부기능의 종류는 [표3]과 같다.

<표3> 차단 기능 기본 구도 구성

차단 Zone	차단 기준 정보	차단 단계	차단 기능
· 트래픽 경로 · 정보 자원 · 하드웨어 리소스	· MAC주소 · IP주소 · 프로토콜 종류 · TCP, UDP 서비스 종류	· 외부 관문 · 내부 관문 · 내부 게이트웨이 · 내부 네트워크	· 진단 · 삭제 · 거점 차단 · 치료 · 경로 차단

	· 컨텐츠 기반 · 트래픽 볼륨		

3.6 효율성구조 설계

효율성 구조는 네트워킹 기술을 통해 또는 시스템 원리를 통해 구현되며 한편으로는 네트워킹과 보안기술 융합을 통해서 구현된다. 데이터 통신 기술의 발전과 각종 서비스의 진화 또한 이로 인한 네트워크 접속점 다원화, 트래픽 급증 등은 모두 효율성 구조의 도입 요인이 되고 있다. 보안시스템의 경우 어느분야 보다도 시스템 안정성과 연속성 유지가 절대적이므로 효율성을 요구한다[13][14]

3.6.1 방역 시스템 기능 : 즉시성과 자동화 기능 확보

기존 인프라 구조의 한계성은 시스템적, 기능적, 구조적 3개측면 에서 고찰할 수 있다.

3.6.2 인프라 구조 관리 : 통합 관리

효율성구조 두번째 테마는 구조관리의 통합에 관한 것이다. 일반적 방역 구조관리 형태는 필요한 시기에 필요한 기술, 기능을 추가 또는 수정하는 방법이다. 이 방법은 인프라구조 관리 시 종합적 관리보다 개별 솔루션별 관리를 위주로 하고 관리계획 자체도 종합화 되지 않는 것이다. 이같은 개별관리 대신 설계에서 구축 운용까지 종합화된 마스터 플랜하의 구조 관리를 지향한다. 운용관리 통합구조란 방역 솔루션을 중앙 집중관리 구조로 채택함으로서 각종 방역 대상 자원을 일괄적으로 모니터링, 제어, 통제하여 방역구조 관리의 일관성과 효율을 도모한다

<표4> 인프라 구조 관리

구간	차단 종류	방 역 항목	설비 명칭
외부망 - 외부 스위치	스위칭 (Switching)	- 컨텐츠 스위칭 - 바 이 러 스 Protecting	외부 스위치 (Exterior Switch)
스위치 - 침입차단시스템	필터링 (Filtering)	애플리케이션레벨 - 컨텐츠 필터링 -바이러스필터링 - 액세스 제어	침입차단시스템 (Firewall)
침입차단시스템-내부망	내부게이트웨이 (Interior Gateway) 필터링	-트래픽 필터링 -바이러스필터링 - 이메일 필터링	내부게이트웨이 (Interior Gateway)
내부망-서버	서버 방역	-바이러스스캐닝	서버
내부망 - 클라이언트	클라이언트 방역	- Real-time 바이러스스캐닝	클라이언트

3.6.3 인프라 구성 형태 : 고가용성 구조

효율성구조 세번째 항목은 시스템구조 가용성에 관한 것이다. 어떤장비나 기술도 가용성 구조를 통한 운용의 계속성을 보장해주지 않으면 업무중단과 그로인한 각종 손실을 회피할 수 없다. 고가용성 구조란 시스템기능 장애에 대비하여

시스템구조를 액티브-액티브 (Active-Active)또는액티브-스탠바이(Active-Standby) 방식의 이중화를 구성하는 구조형식 이다. 또한 시스템구조에서 부하분배 원리를 적용하여 모든 트래픽의 시스템간 로드밸런싱을 구현하여 처리 대역폭을 확보하고 처리 신속성을 도모하는 것도 고가용성 구조 방식이다[3][15]

4. 제안성능 검증

4.1 목표 설정

효율성 검증방향은 새로운 차단구조 구현시 발생되는 방역성과를 정량적 정성적으로 측정 하는 것이다. 정량적 분석(Quantitative Analysis) 은 정보시스템 및 관련 자산에 대한 위협발생 확률과 잠재적 손실 크기를 곱해서 이를 화폐가치로 환산하여 위험의 정도를 측정하는 방법이다. 정량적 분석법에는 과거자료 접근법, 수학공식 접근법, 확률분포추정법, 점수법, 확률 지배(Stochastic dominance), 몬테칼로 시뮬레이션 등이 있다. 본 연구에서는 과거자료 접근법을 통해 실제 응용데이터를 채집 분석 하는 방법을 사용한다. 정성적분석(Qualitative Analysis)이란 정보시스템 및 관련 자산에 대하여 위협 발생으로 인한 손실크기를 화폐가치가 아닌 기술 변수(Descriptive Variable)로 나타내는 손실측정방법, 정성분석법에는 델파이법, 시나리오법, 순위결정법, 퍼지행렬법(FuzzyMetrics),질문서법(Questionnares)등이 있다. 검증목표 수준으로 선정되어 질 수 있는 범위와 한계는 다음 표와 같다[16].

<표5> 검증 목표 수준

구분	분 야	검 증 목 표 수 준
침입차단	· 기간중바이러스 발생	· 바이러스 발생은 어떤 패턴을 보이는 가에 대한 진단
	· 인프라구조 차단기능	· 구조가 차단 실적에서 어떻게 유작용하는가에 대한 진단
	· 개 선 구 조 Performance	· 개선 구조는 시스템 Performance 측면에서 어떤 변화 를 보이는 가
	· 차단단계 별효율성	· 차 단 단 계 별 차 단 실 적 과 Performance 상호 관계 검증
효율성	· 차단 구조의 고가용성 매커니즘	

○ 침입차단부분 측정은 악성코드 발생 패턴과 바 차단기능, 성능 결과치를 검증할 수 있다. 악성코드 발생패턴은 시간적 패턴과 종류별 패턴이 있다. 악성코드 차단기능, 성능 패턴은 개선구조에 의한 악성코드 차단 성취 여부, 차단이 이루어지는 메커니즘, 차단이 이루어진 기능, 차단이 성공한 경우 차단 수준이 될 수 있다[9].
○ 차단단계별 효율성 비교 분석은 인프라 구조 유형별 구분 즉 1단계, 3단계, 5단계 구조별로 방역효율 성과를 비교 분석한다.
○ 침입차단 분석의 또다른 부분은 개선구조로 인한 부작용(Side Effect)이다. 부작용이란 차단구조로 인해 발생되는 바람직하지 못한 현상이며 대표적으로 Performance지연 이다.
○ 효율성 부분은 바이러스 차단기능의 구조적 고가용성, 트래픽 부하분산 측정이 있다.

4.2 시험 환경

트래픽 환경은 A기업 인트라넷 시스템 상에서 실제 업무를 대상으로 검증을 실시했다. 인프라 구조가 설계사상으로 구비된 것은 아니므로 본 검증 작업을 위해 측정목적의 보강과 환경준비 단계를 거쳤다. 인용된 A기업 업무 환경과 인트라넷의 트래픽 처리 환경은 다음과 같다.

• 인트라넷 시스템내 접속자원 규모
- 각종 서버 100대,클라이언트 PC 160대
• 네트워크 구조
-인트라넷과 외부망과의 연결은 310mbps 속도로 복수 회선 네트워크로 구성됨
-인트라넷 입구에 침입차단시스템이 구성되어 있고 침입차단시스템 이후 구간에는 인트라넷이 구성됨.

4.3 시험구간

인트라넷 시스템에서 트래픽은 정상적인 시스템 처리구간을 통과하기 때문에 측정구간은 일반적 네트워크 구조도 구성구간과 동일하다. 즉 사용자 단말에서 시작된 트랜잭션은 사내 네트워크 구간을 거쳐 인터넷 구간을 통과하여 다시 사내 네트워크 구간에 도착하는 구성도이다. 측정용 에이전트 PC에서 출발한 트랜잭션은 Outbound 트래픽으로 사내시스템인 클라이언트 -> 서버 -> 내부게이트웨이 -> 침입차단시스템 -> 스위치 -> 외부라우터를 통과하여 인터넷 구간으로 접속된다. Inbound 트래픽은 인터넷 구간의 서버를 거쳐 인트라넷 구간인 외부라우터 -> 스위치 -> 침입차단시스템 -> 내부게이트웨이가지 접속되고 내부게이트웨이에서 서버 또는 클라이언트까지 접속된다[14][16].

4.4 분석항목

본 시험에 사용된 기존구조는 하나의 Exit Point인 외부라우터를 통해 애플리케이션스위치까지 단일경로를 이루고 애플리케이션 스위치와 침입차단 시스템간은 침입차단시스템의 수만큼 복수경로를 구성한다. 침입차단시스템에서 내부라우터 이후구간은 내부 네트워크까지 단일경로를 구성하여 전체적으로 단일경로의 사상이다. 개선후의 구조는 이원화된 Exit Point를 둔다. 이때 외부 네트워크는 인터넷을 사용하지 않아도 되는 업무용 데이터를 대상으로 전용회선 방식으로 구성하여 데이터의 소통에 사용된다. 스위치 -> 애플리케이션스위치 -> 침입차단시스템 구간은 침입차단시스템 숫자만큼의 복수 채널로 구성되고 침입차단시스템에서 내부 네트워크까지 경로는 DMZ 구간과 내부 네트워크로 분리된다.

<표6> 측정 항목

구 분	측정 구간	측정 항목	측정 단위
바이러스발생량	5개 구간	바이러스 및 악성트래픽 발생	• 건수
바이러스차단실적	스위칭 구간	구간바이러스차단실적	• 건수
	5개 구간 합계	총 구간 차단 실적	
Performance	내부 게이트웨이	CPU 부하율	• %
	서버 구간	CPU 부하율 시스템 프로세스수	• % • 건수
	스위칭구간	Latency	• micro second • mili second • second
	5개 구간 합계	응답 시간	
고가용성	3개 구간	부하부산율, Data-loss율	• %

4.5 보안 도메인 효율성 비교

네트워크 보안인프라 단계별 방역효율성을 분석하기 위해서 네트워크 구조상로 보안도메인을 기준으로 차단단계를 구성하고 방역을 시행시각 단계의 보안효율을 검증한다. 본 연구에서 설정한 유형은 방역단계를 기준으로 1단계, 3단계, 5단계 경우등 3가지 유형을 설정했다. 3가지 유형을 설정한 이유는 현재 우리나라 기업의 보안 인프라 구축 실태는 기본적 보안 인프라인 침입

차단시스템 설치 사례가 50%미만으로 기본 인프라가 미비한 상황에서 다단계 차단 구조를 적용하는 사례가 일반적이지 못하므로 차단 유형을 현실적 수준으로 설정한다[16][17].

○ 1단계 방역 구조

1단계 방역은 스위치, 침입차단시스템, 서버 방역망, 클라이언트 방역망 중 하나만을 가동했을 경우 방역 성취도를 나타낸다. 네가지의 경우 중 어느경우든 5개도메인 중 하나의 도메인만을 방역 대상으로 하고 있음으로서 나머지 4가지 도메인에 대해서는 경로차단기능 적용이 불가능하게 된다. 각각의 경우 방역 가능한 부분과 차단 불가능한 부분은 아래 [표7]과 같다.

<표7> 1단계 차단 방역 영역

차단 유형		외부관문	내부관문	내부유통	서버군	클라이언트군
1단계 차단	스위칭	차 단				
	침입차단시스템		차 단			
	서버 방역				차 단	
	클라이언트 방역					차 단

・ 방역 수준

- 차단 도메인 : 스위칭, 침입차단필터링, 서버 방역, 클라이언트 방역 중 1개 도메인
- 미차단 도메인 : 차단 1개 도메인외 나머지 4개 도메인

・ 평가 의견

- 가장 취약한 방역 방안
- 국내 기업에서 침입차단필터링 구조 1단계 차단이 가장 많이 사용되고 있음.

○ 3단계 방역 구조

<표8> 3단계 차단 방역 영역

차단 유형			외부관문	내부관문	내부유통	서버군	클라이언트군
3단계 차단	스위칭	스위칭	차 단				
		서버 방역				차 단	
		클라이언트 방역					차 단
	침입차단	침입차단시스템		차 단			
		서버 방역				차 단	
		클라이언트 방역					차 단

3단계 방역시 스위치를 기준 하는 3단계 차단과 침입차단 시스템을 기준하는 3단계 차단 두 종류가 있다. 어느 경우든 1단계 차단보다는 방역 성취도가 높지만 경로 차단을 시행치 못하는 도메인이 발생한다. 경로 차단 미시행 도메인은 스위칭, 서버, 클라이언트 방역의 경우는 패킷 필터링에 의한 침입차단 방역이 이루어지지 못하여 패킷의 IP주소 기준, TCP 포트 기준, TCP 프로토콜 기준의 세션 검사와 관리가 이루어지지 못한다. 또한 내부게이트웨이 단계에서의 방역 미 시행으로 내부경로상 유통 바이러스에 대한 대책은 서버 방역망과 클라이언트 방역망으로 대처해야 한다[15][18].

・ 방역 수준

- 차단 도메인 : 스위칭, 서버 방역, 클라이언트 방역 3개 도메인 또는 침입차단 필터링, 서버 방역, 클라이언트 3개 도메인
- 미차단 도메인 : 스위칭, 내부 게이트웨이 2개 도메인 또는 침입차단 필터링, 내부 게이트웨이 2개 도메인

・평가 의견

- 구조 형태로서는 가장 일반적 방역 방안
- 내부 게이트웨이 구간을 통한 경로 확산 차단 기능이 없어 취약성이 노출됨

○ 5단계 방역 구조

<표9> 5단계 차단 방역 영역

차단 유형		외부관문	내부관문	내부유통	서버군	클라이언트군
5단계 차단	스위칭	차 단				
	침입차단시스템		차 단			
	게이트웨이			차 단		
	서버 방역				차 단	
	클라이언트 방역					차 단

2) 5단계 방역

5단계 방역시 통합구조에서 구성한 보안도메인을 모두 적용하여 방역 처리하고 있다. [표9]는 차단 유형별 차단도메인을 나타내고 있다. 5단계 차단의 경우 구현하고자하는 차단단계가 모두 구현된다. 1차 외부 경계선에서의 침입을 Layer7

스위칭에서 97%이상 걸러주며 2차 패킷필터링 과정에서 패킷 자체의 여과를 거치면서 메일바이러스 위주 차단이 시행된다. 만일 그 단계에서 누락이 있다 하더라도 내부 게이트웨이 단계에서 내부 경로상 확산 차단하므로 안전 도메인을 형성하고 내부에서 매체 감염으로 새로운 침입이 발생하더라도 내부 게이트웨이 방역망에서 차단이 이루어진다[17].

4.6 응답 소요시간 분포

응답시간 분포는 다른환경 즉 클라이언트, 서버 등 하드웨어, 애플리케이션, 네트워크 환경에서 인프라 구조만을 변경한후 응답시간을 측정한다면 각 호스트시스템 상에서 애플리케이션 수행시간, 데이터베이스 엑세스와 처리시간이 포함되고 전산자원과 기술에 따라 처리시간이 상이할 수 있으나 측정 횟수를 증가시키고 통계신뢰도를 높일 경우 Performance 비교가 가능하다. 이같은 환경에서 응답시간 측정 결과는 [표10]과 같다. 기존구조에서 통합구조로의 증가 시간 비율은 평균 증가율은 5.75%이고 순간 최대 증가율은 10%까지 증가했다. 순간 최대 증가율이 10% 수준까지 증가한 것은 어느 일정순간 최대 증가치이며 측정당시의 네트워크 구간, 서버, 클라이언트 중 시스템 부하증가 요인 발생환경에서 기인한 것으로 추정할 수 있다.

<표10> 차단 유형별 방역 효율

차단 유형	차단 장치	방역 도메인		응답 시간 지연(%)
		차단	미차단	
1단계	스위칭	1	4개 영역 (80%)	평균 0% 최대 0%
	침입차단 필터링	1		
	서버 방역	1		
	클라이언트방역	1		
3단계 차단	스위칭 또는 침입차단 필터링	1	2개 영역 (40%)	평균 2.875% 최대 3.06%
	서버 방역	1		
	클라이언트방역	1		
	소계	3		
5단계	스위칭	1	없음	평균 5.75%미만 최대 7.65%미만
	침입차단 필터링	1		
	내부게이트웨이	1		
	서버 방역	1		
	클라이언트방역	1		
	소계	5		

4.7 종합성능 측정결과

이상의 차단결과와 Latency 소요시간 조사결과를 토대로 하여 차단 유형별로 종합적인 방역효율을 분석했다. 효율분석은 1단계차단, 3단계차단, 5단계차단 유형별로 차단효과와 Latency를 각각 분석하고 그 결과를 종합효율로서 평가하는 것이다. 이상적인 차단구조 모델은 차단율은 높을수록 유리하고 Latency는 낮을수록 유리하다. 따라서 크게 세가지 유형과 세부적으로는 일곱가지 차단 경우의 수 별로 차단율과 Latency를 감안 했을때의 가장 이상적 모델을 찾는 것이다. 1단계차단의 경우 1개도메인의 방역만 가능하고 나머지 4개도메인의 방역은 불가하다. 차단단계가 다단계일수록 방역율은 높고 Latency는 증가한다. [표10]은 차단유형별 방역효율 종합 분석결과를 보여주고 있다.

5. 결론

종합효율을 분석해보면 다단계 차단구조 적용시 전체적 Performance에 지장을 초래하지 않고 차단 기능이 수행된다. 즉 Performance 지연은 1단계 차단, 3단계 차단에서 미미한 정도이며 5단계 차단에서도 두드러지게 나타나지 않았다. 적어도 5단계 차단구조까지 Performance 영향을 걱정하지 않아도 된다. 차단 완전성은 1단계보다 3단계, 3단계보다 5단계가 절대 유리하다. 5단계 차단에서는 전방위 Zone으로 차단 영역이 확대되어 차세대형 차단 구조로서 가장 강력한 방역기능 실현이 가능하다. 결론적으로 차단단계 추가시 시스템 Performance 에는 업무 불편을 초래할 만큼의 지연이 발생치 않는다. 이같은 분석결과는 Performance 부담으로 인하여 다단계 차단구조 적용이 어렵다는 일반적인 관념을 뒤집는 것으로서 향후 보안시스템 구축시 정책 결정에 반드시 고려되어야할 사항이다. 본 연구를 통해 체계적인 메커니즘 설계시 개선된 네트워킹 기능과 정보시스템 기능을 위한 효율성 제고 방법론 개발이 가능함을 보여주고 있다. 정보시스템 인프라스트럭처의 효율성 여부는 사용자 또는 사용부서의 지속적인 진단과 튜닝을 필요로 한다.

참 고 문 헌

[1] 김태경 · 서희석 · 김희완, 서비스 응답시간 보장을 위한 패킷 손실에 관한 연구,2005
[2] 김태성,이금석, 웹 어플리케이션 응답시간 모

니터링 API의 설계 및 구현,2000
[3] 장윤정, "L7 스위치로 네트워크 활용도를 높여라", 네트워크타임스, 2003.
[4] Sichoon Noh, Dong Chun Lee, and Kuimam J.Kim, "Improved Structure Management of Gateway Firewall Systems for Effective Networks Security", Springer, 2003.
[5] Sichoon Noh, Dong Chun Lee, and Kuima m J.Kim, "ImprovedStructure Management of Gateway Firewall Systems for Effective Networks Security", Springer, 2003.
[6] D. Yoon and K. Cho, "General bit error probability of rectangular quadrature amplitude modulation," IEE Electronics Letters, vol. 38, no. 3, pp. 131-132, January 2002.
[7] J. K. Kwon, S. Park and D. K. Sung, "Log-likelihood ratio(LLR) conversion schemes in orthogonal code hopping multiplexing," IEEE Comm. Letters, vol. 7, no. 3, pp. 104-106, Mar. 2003.
[8] Sichoon,Noh,Dong Chun Lee,"Multi-Level Protection Building for Virus Protection Infrastructure", SCIE LNCS 3036,2004.6 [9] Sichoon,Noh,Dong Chun Lee,"Assurance Method of High Availability inInformation Security Infrastructure System", SCIE LNCS 3794,2005.12
[10] Sichoon,Noh,"Building of an Integrated Multilevel Virus Protection Infrastructure ", IEEE Computer Society,2005.12.
[11] Sichoon,Noh,"A Securing Method of Multispectral Protection Infrastructure for Malicious Traffic in Intrne System", DCS, 2006.02
[12] Sichoon,Noh,Dong Chun Lee,Kuimam J.Kim"Protection Structure Building for Malicious Traffic Protecting in Intrnwt Systems",SCIE LNCS3981,2006.05
[13] Sichoon,Noh,"Active-Active High Availability of Information Infrastructure System for Effective Network Security",IEEE Computer Society,2008.01
[14] Sichoon,Noh,"MSPI(Multi-Spectral Protection Infrastructure) System fo Optimal Network Security",IEEE Compu ter Society,2008.08
[15] Paul Woosnam, "10 hottest Technologies",Te lecommunications, 2003.4
[16] Peter Sevcik, "Internet Traffic and Performa nce", NetForecast, 2001
[17] ITU-T Rec. E.417, "Framework for the Netw ork Management of IP-Based Networks,"Feb. 2001.
[18] ITU-T Rec. Y.1221,"Traffic Control and Con gestion Control inIPBased Networks,"March 2002.

문 송 철

1995년: KAIST 정보공학석사
2005년: 국민대학교 정보관리학 박사

정보시스템 감리인

1996-1998 : 한보정보통신㈜ 철강SI사업부장, 이사
1999-2005 : ㈜가나시스텍 대표이사 사장
2005~현재 : 남서울대학교 컴퓨터학과 교수
관심분야 : 경영정보시스템, 소프트웨어공학

노 시 춘

1987년 : 고려대학교 경영정보학 석사
2005년 : 경기대학교 정보보호기술 박사

2002년: KT시스템보안부장
2004년: KT 충청전산국장
2005년~현재 : 남서울대학교 컴퓨터학과 교수
관심분야 : 차세대통신,정보보호,컴퓨터네트웍

정 지 문

1989년:연세대학교 공학대학원 석사
2008년:충북대학교 데이터베이스 박사

1987년:한국국방연구원(총괄팀장)
1994년: 혜천대학 전자계산과 교수
1994년~현재:남서울대학교 컴퓨터학과 교수
관심분야 : 데이터베이스, 클라우딩컴퓨팅