디지털산업정보학회 논문지 제5권 제4호-2009년 12월

Multi-level 네트워크의 보안 도메인을 위한 통합 아키텍쳐 설계 및 효율성 측정방법 연구

나 상 엽* · 노 시 춘**

A Study for the Designing and Efficiency Measuring Methods of Integrated Multi-level Network Security Domain Architecture

Na, Sang Yeob · Noh, Si Choon

〈Abstract〉

Internet network routing system is used to prevent spread and distribution of malicious data traffic. This study is based on analysis of diagnostic weakness structure in the network security domain. We propose an improved integrated multi-level protection domain for in the internal route of groupware. This paper's protection domain is designed to handle the malicious data traffic in the groupware and finally leads to lighten the load of data traffic and improve network security in the groupware. Infrastructure of protection domain is transformed into five-stage blocking domain from two or three-stage blocking. Filtering and protections are executed for the entire server at the gateway level and internet traffic route ensures differentiated protection by dividing into five-stage. Five-stage multi-level network security domain's malicious data traffic protection performance is better than former one. In this paper, we use a trust evaluation metric for measuring the security domain's performance and suggested algorithm.

Key Words : Network Security, Multi-level Domain, Architecture

Ⅰ. 서론

전통적인 네트워크보안 중심 메커니즘은 소위 네트워크상의 거점(traffic station 또는 traffic node)방역으로 대표된다. 거점 방역은 경로(traffic route) 방역과 비교되는 개념으로 트래픽 유통단계 최종 종단점, 즉 서버와 클라이언트 등 단말 시스템에 적용되는 방역이다[3]. 거점방역을 기조로 하는 오늘날의 방역방식에는 어느정도 기능적 취약 요인이 내재되어 있다. 순간적 전파 악성코드를 종단점에서 삭제, 차단하므로 방화벽, 백신기술, 자동화 방역 환경에서도 방역누수가 지속된다. 악성코드는 네트워크 경로를 통해 인트라넷 내부 확산을 반복한

* 남서울대학교 컴퓨터학과 교수
** 남서울대학교 컴퓨터학과 교수

다[4-5]. 본 연구는 네트워크 경로확산 악순환의 현실적 대안으로 네트워크 경로상 적용 네트워크보안 도메인 통합아키텍쳐 설계방법과 절차, 이상적 형상 및 도메인을 도출하고 현장운용 실적을 토대로 효율성을 측정한다.

Ⅱ. 네트워크보안의 방역 누락요소

인트라넷 시스템을 기준으로 모든 네트워크 경로에는 게이트웨이와 서버, 클라이언트 방역에 불구하고 악성코드가 존재한다. 감염은 각기 다른 상황에서 발생된다. 첫 번째, 신종 악성코드 발생시 백신엔진 업데이트시 까지 방역누락이 계속된다. 두번째, 침입차단시스템에 불구하고 또 다른 침투가 등장하는데 바로 백도어 경로의 악성트래픽이다. 침입차단시스템을 우회하는 악성트래픽이 존재하기 때문이다. 세번째, 내부 경로상에서 확산되는 악성코드이다. 이는 침입차단시스템에서 방역누락 패킷의 기동 때문이다. 네번째, 서버군, 클라이언트에 대한 침투이다. 내부 게이트웨이 필터링에서 방역 누락된 악성코드는 서버군과 클라이언트 군으로 진입한다. 다섯번째, 내부 매체 감염이다. 서버와 클라이언트에서 매체 감염을 일으킨 악성코드는 내부 네트워크 경로상에서 감염 악순환을 반복한다[1, 4].

Ⅲ. multi-level 보안 도메인의 통합 아키텍쳐 설계방법

3.1 네트워크 보안 도메인의 개념

네트워크 보안도메인은 물리적, 논리적 네트워크 경로를 보안목적으로 트래픽 소통영역과 그룹을 구분, 구성하는 방법론이다. 도메인별로 효율적인 방역위치를 설정하고 도메인 특성에 따라 차별화된 보안 메커니즘을 적용한다. 본 연구는 네트워크 도메인결정을 위해 네트워크는 어떤 구조와 기준으로 설계되어야 하는가에 대한 방법론을 개발한다. 이를위해 형상(topology) 결정요소 선정, 보안도메인 설정기준 결정, 구조도 선택기준 결정, 차단위치 결정, 경로방역망 구성기준을 도출하여 통합화 도메인 아키텍쳐를 설계하고 메커니즘을 적용한다. 네트워크 경로 취약점 진단결과를 토대로 차단단계 도출과 단계별 방역 매커니즘을 설계한다. <표1>은 보안도메인 개념을 네 가지 관점에서 정리한 것 이다[2-4].

<표1> 보안도메인 개념

유형	내 용
A	보안 기술의 적용이 가능 영역
B	보안 기술의 적용이 필요한 영역
C	경로와 트래픽 성격이 타도메인과 차별화 가능 영역
D	보안 기술과 적용시 타영역의 보안 기능으로 기능 중복이 발생치 않는 영역

3.2 네트워크 보안도메인의 형상 결정요소

네트워크 보안도메인 형상은 네트워크 구조상의 어느 접속점, 어떤 경로상에, 어떤 종류의 보안 기능을 배치하고 연계 시키는가에 따라 그 형상적 의미와 종류를 결정하는 방법이다. 보안도메인은 <표2>와 같이 네트워크구조 분류기준, 즉 트래픽 경로 설정 방법, 외부 네트워크 그룹간 접속방법, 내부스테이션 배치방식, 즉 서버와 클라이언트 배치방법에 따라 구조와 형상이 결정될 수 있다. 또한 보안기능 관점에서 트래픽경로, 경로방역 구조, 거점방역 구조, DMZ구성 등을 기준으로 삼을 수 있다. 기타 스위칭구조, 침입차단시스템 필터링구조, 게이트웨이 필터링구조, 서버방역 구조, 클라이언트 방역 구조를 기준으로 할 수도 있다. <표2>는 네트워크 형상 결정요소를 저자가 국내사례를 대상으로 조사한 기준이다[5-6].

<표2> 네트워크 형상(Topology) 결정요소

분류 요소			판단 기준
유 형		항 목	
트래픽경로설정방식	내부	· 공용 경로 사용	· 인트라넷 접속 경로 단일경로
		· 분리경로	· 서브 네트워크 별 경로 분리
	외부	· 복수경로	· 인터넷, 비 인터넷 구간 분리·인터넷 구간 복수 경로
		· 단일경로	· 인터넷, 비인터넷 미 분리
외부네트워크와의 접속		· 다중화 접속	· 단일게이트웨이상 복수 네트워 크 · 동종 프로토콜과 전송표준사용
		· 분리 접속	· 네트워크 그룹간 별도의 게이트웨이나 접속점 관리
내부스테이션배치방식		· 서버 Farm 클라이언트분리	· 서버 Farm 별도 구성 · 클라이언트 네트워크 별도 구성
		· 서버, 클라이언트 동일레벨	· 서버, 클라이언트 동일 레벨 배치 후 인터네트워킹 장비로 분리

3.3 네트워크 보안도메인의 설정기준

네트워크 도메인은 정상적 트래픽처리 기능과 보안 취약성에 의한 보안침투 기능을 동시에 갖고 있다. 따라서 보안 취약성 대처를 위해 각 도메인 상황에 맞는 보안대책이 강구되어야 한다. 이때 형상 결정요소를 기반으로 보안도메인을 설정 하여야 한다[4, 7].

<표2> 네트워크 형상(topology) 결정요소 기준을 검토한 결과 보안도메인은 <표3> 보안 도메인 설정기준 영역별 구분 항목에서 1번 항목을 제외한 5개 영역이 설정되었다. 1번 항목을 제외한 이유는 외부 네트워크와 외부 라우터 구간은 인트라넷 외부 영역으로서 보안기능 적용이 불필요하며, 보안 기능은 인트라넷내의 스위칭 단계부터 적용해도 가능하기 때문이다[6].

3.4 보안 차단위치 검토

트래픽 통과지점을 기준으로 차단위치를 점검하되 효율성을 고려한다. 인트라넷 전방 인터넷 접속지점에 exterior라우터가 가동되고 있고 이어서 패킷필터링 시스템, 그리고 interior라우터가 가동된다. 이어서 두번째 interior라우터에 의해 내부 클라이언트 group 또는 서버군 group 네트워크로 다시 분류된다. 네트워크 트래픽 소통경로상 이상 5개지점을 검토한다. 5개소는 일반적인 인프라 구조로 활용하고 있는 위치로서 이 진단을 통해 차단위치에 대한 일차적 판단이 가능하다. <표4>는 차단위치 검토 요소에 대한 기준이다[8, 12].

<표3> 보안도메인 설정기준

네트워크 구간	도메인명	검토 결과			
		A	B	C	D
1. 외부 네트워크-외부 라우터	외부 라우터 구간	○	×	○	○
2. 외부 라우터-외부 스위치	외부 스위치 구간	○	○	○	○
3. 외부 스위치-침입차단	침입차단 구간	○	○	○	○
4. 침입차단-내부 게이트웨이	내부 게이트웨이	○	○	○	○
5. 내부 게이트웨이-서버팜	서버 구간	○	○	○	○
6. 내부 게이트웨이-클라이언트	클라이언트 구간	○	○	○	○

<표4> 차단위치 검토요소

기 준	선 정 사 유
· 상위 구조의 트래픽 전량 유입 유일 하위 지점	· 방역 차단시 통제와 종합관리 효과
· 네트워크 구조상 상위구조 트래픽 분기 유일 하위 지점	· 방역장치 설치와 방역 유연성 절대 유리
· 기존 구조에서 현재 패킷 검색, 컨텐츠 판독, 라우팅 지점	· 기존 네트워크 구조에서 수행되는 트래픽 컨트롤과 연동
· 기존 인프라 구조상 없는 차단 지점신설로 Performance 지연이 초래되지 않아야 함	· 응답시간 등 Performance 지연 가능. 생산성, 가용성 저하 가능성
· 기존 인프라 구조의 백본, 게이트웨이 구간의 설계를 근본적으로 변경치 않는 구간	· 백본이나 게이트웨이 근본 구조 변경시 시스템 안정성 훼손우려

3.5 보안도메인의 아키텍쳐

보안도메인 프레임워크 설계는 소프트웨어 기술방역의 취약점과 한계점을 보강할 수 있는 인프라구조 이다.

제반 검토과정을 거쳐 도출된 보안도메인 구간은 외부망 ↔ 스위치, 스위치 ↔ 침입차단시스템, 침입차단시스템 ↔ 내부망, 내부망 ↔ 서버, 내부망 ↔ 클라이언트이다. 보안도메인은 경로방역 구조로 설계된 5 tiers 방역 분담 구조이며 각 계층마다의 특성을 고려하여 계층별 방역기능을 설계한다. <표5>는 이상의 과정을 거쳐 도출한 보안도메인 설계내용 이다[10, 13].

<표5> 보안도메인 아키텍쳐

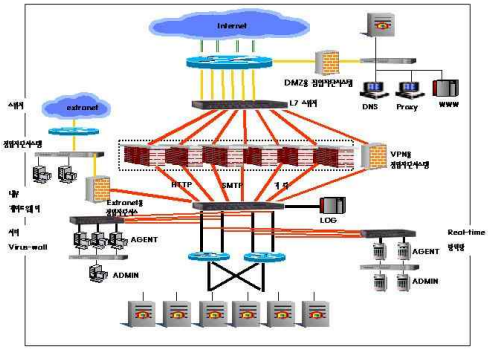
구간	도메인	메커니즘
외부망 ↔ 스위치	외부 스위칭	외부유입 감염차단
스위치 ↔ 침입차단 시스템	침입차단 시스템	내부관문 감염방역
침입차단시스템 ↔ 내부망	내부 게이트웨이	내부경로 확산차단
내부망 ↔ 서버	서버 방역	· 내부 감염차단 · 매체 감염차단
내부망 ↔ 클라이언트	클라이언트 방역망	· 내부 감염차단 · 매체 감염차단

3.6 보안도메인의 방역 메커니즘

3.6.1 Multi-level 보안도메인 구성

5단계의 각 보안 도메인별로 multi-level 차별화 방역을 적용한다. 메커니즘은 <표4>, <표5>의 도메인 특성을 고려한 차별화 방식 이다. 정교한 부하분산과 유해트래픽 차단, 데이터 필터링을 통해 네트워크 환경을 최적화 한다. 스위칭기능은 deep inspection, 전체적인 트래픽 모니터링을 실시하므로서 종래의 로드밸런싱 위주의 L4 기능에서 보안기능을 구현하는 차세대형 L7스위칭 기능이 가동된다. 도메인마다 차단기능이 구현되고 차단기능은 도메인간 상호 연동되어 종합적 효율을 도모 한다.

보안도메인별 방역 분담 메커니즘은 <표5> 보안도메인 아키텍쳐, <표6> 보안도메인 방역 분담구조와 같다. 방역 메커니즘은 5개 도메인별로 차별화 되었지만 이 기능은 독립적으로만 수행되지 않고 스위칭, 침입차단, 내부게이트웨이, server's바이러스월, real-time 방역 상호



<그림1> Multi-level 보안도메인 구성도

연동 구조이며 전체 도메인간 상호 유기적 연동을 목표로 한다. <표6>은 설계된 방역분담 기능이다.

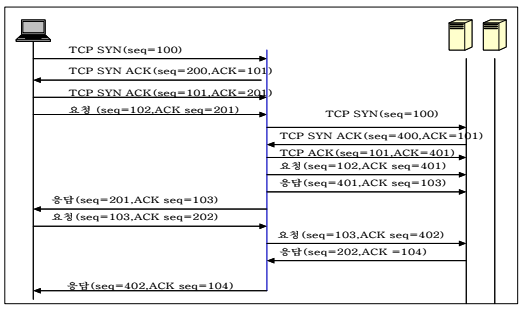
<표6> 보안도메인 방역 분담구조

솔루션	차단	방역 메커니즘
스위칭 솔루션	유입 차단	· 유입 바이러스 1차 차단 · L7delayed binding 스위칭
침입차단 필터링솔루션	유입 차단	· 유입 악성코드 1차 차단 · 특정 발신IP, 수신IP · Deep inspection · Store-and-forward 애플리케이션 레이어 분석 차단
내부 게이트웨이 필터링솔루션	유입 차단 유출 차단	· 유입 악성코드 2차 차단 · Application게이트웨이방역 · 유입 불건전 컨텐츠 차단 · 유출 악성코드 차단
Server's 바이러스월	유입 차단	· 내부유통 악성코드1차차단 · 유입 바이러스 2차 차단
Real-time 방역솔루션	유입 차단	· 내부유통 악성코드2차차단 · 클라이언트 자동화 방역

3.6.2 L7 delayed binding 스위칭

인트라넷 유입 트래픽은 exterior라우터를 통해 경로배정후 스위칭 단계로 유입된다. Exterior라우터 후방 방역은exterior라우터 보다 좀 더 정제된 공격 정보가 탐지된다. 전통적 부하분산 외에 컨텐츠 인식 L7스위칭을 적

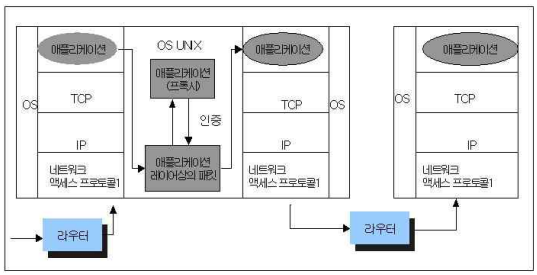
용하여 컨텐츠기반 패킷필터링과 앤티바이러스기능, 응용레벨 미러링 (mirroring)을 수행한다. L4스위칭이 IP 주소, TCP 포트번호를 기준으로 하지만 L7스위칭은 패킷의 URL정보, 제목, 내용을 나타내는 검색어 등 소위 컨텐츠 분석 스위칭이므로 문자열, HTTP콘텐츠 URL, FTP파일 제목, 쿠키정보 판독으로 악성코드 분석을 수행한다. L7스위칭은 TCP세션 보류 상태에서 요청정보가 전송되어 왔을때, 서버쪽과 TCP 세션을 중계하는 역할을 하는데 이 기능이 delayed binding기능, TCP splicing 기능 또는 TCP termination 기능 이다. TCP SYN에 대한 요청은 L7스위치가 TCP세션을 형성하며 클라이언트 요청 데이터를 L7스위치는 요청 데이터 정보를 참조해 리얼서버로 할당 한다 [10-11].



<그림2> L7스위치 TCP delayed binding

3.6.3 Application proxy 패킷 필터링

L7스위칭 이후단계 도메인에서 정교한 패킷필터링 방역이 필요하다. 정밀한 패킷필터링은 패킷타입의 조사분석 기능을 프록시나 애플리케이션 서비스로 구현한다. 프록시 서버를 클라이언트와 원격의 애플리케이션 서버 사이에 삽입한다. 이때 적용 침입차단기능은 deep inspection 서비스로서 www, 텔넷, FTP, mail 등서비스 기준의 네트워크 환경에서 해당 서비스를 요청한 호스트의 주소 와 포트번호 그리고 사용자 인증 등 기능을 기반으로 통제를 수행한다. 허용되지 않은 사용자 서비스를 차단하여 내부 네트워크 접근을 통제한다. 패킷필터링 주요기능은 내부 외부 네트워크의 유일한 연결점으로서 기능을 수행하면서 서비스 허용 및 차단, 사용자 인증 그리고 내·외부 상호 접속된 네트워크에 대한 트래픽 모니터링이다[8-9].



<그림3> 응용게이트웨이 처리과정

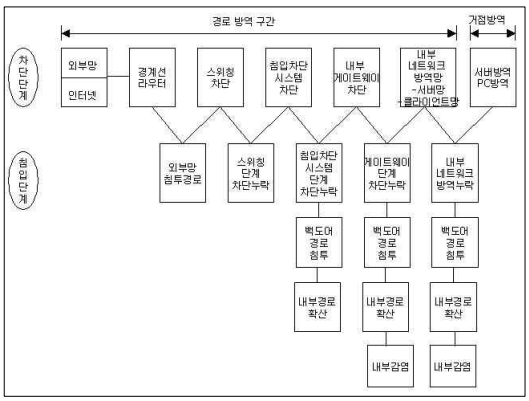
3.6.4 내부 게이트웨이 레벨 필터링

이 구간은 내부네트워크 진입경로 방역이다. 유해 트래픽이 네트워크 핵심 중요정보에 도달하기 전에 실시하는데 웹 트래픽과 SMTP 트래픽을 중점으로 한다. 통계에 의하면 일반적으로 전체 트래픽중 웹 트래픽이 80%, SMTP 트래픽이 10% 수준이다. 따라서 이 두개 종류의 트래픽에 대한 사전 방역 은 차단과 performance 향상 두가지 측면에서 긴요하다. 게이트웨이 방역의 기본 기능은 필터링 기능이다. 게이트웨이 적용 필터링은 바이러스 필터링, 컨텐츠 필터링, 이메일 필터링, 파일 필터링, 스팸 필터링 등으로 구분할 수 있다. 바이러스 필터링은 패킷단위로 바이러스 감염여부를 점검 삭제하며 컨텐츠 필터링은 이메일의 제목과 본문내용에서 특정 키워드가 발견되는 경우 차단기능 이다. 이메일 필터링은 이메일 통과 허용 size를 제한하는 기능이며, 파일 필터링은 특정 첨부파일명이나 확장자를 미리 검사해 차단한다 [9-10].

3.6.5 Real-time 방역누수 연동

도메인 마다 방역기능이 구현되고 방역기능은 도메인간 연동된다. 모든 도메인상에는 전단계 도메인으로부터

발생되는 방역 누락 요소와 당해 도메인 상에서의 직접 감염 등 두가지 유입 유형의 감염이 발생한다. 방역연동이란 전단계 도메인 방역 누락을 다음 단계에서 차단하고 이같은 방역을 5단계 전 과정에서 연동하는 매커니즘이다. 방역누락은 Ⅱ. 네트워크보안 방역 누락요소에 열거된 다섯가지 패턴으로 발생되며 5개의 도메인을 대상으로 반드시 5단계 차단이 필요하고 만일 1단계 또는 3단계 차단 구조는 그만큼 미차단 도메인이 발생하여 위험을 증가시킨다. <그림4>는 차단기능을 도메인간 연동과정 측면에서 보여주고 있다[6-7].



<그림4> 보안도메인 방역누수 연동과정

Ⅳ. 통합 아키텍쳐에 대한 효율성 측정방법

4.1 검증목표

검증목표는 현장의 운용실적을 토대로 하는 제안구조의 효율성 측정이다. 이를위해 제안 네트워크 인프라의 기능과 효율성을 검증한다. 검증방법은 운용실적 데이터를 토대로 검증분야별 정량적 측정과 정성적 측정을 시행한다. 검증분야는 5개도메인 통합 아키텍쳐에서의 악성코드 방역실적, 게이트웨이 performance, 도메인 형상별 종합효율이다.

4.2 검증환경

검증을 위해 설계 도메인과 동일한 구조의 인프라 환경을 구성해야 하지만 실험만을 위해 네트워크 인프라 전반의 환경을 바꾸는 일은 현실적으로 매우 어려우므로 기존 운용시스템을 최대한 활용한다. 기존 운용시스템에 측정용 소프트웨어 자원과 설비를 추가한 후 트래픽 측정구간을 구성하여 트래픽 처리실적을 측정한다.

4.2.1 트래픽 측정구간 구성

사용자 단말에서 시작된 트랜잭션이 사내 네트워크 구간을 거쳐 인터넷 구간을 통과하고 다시 사내 네트워크로 복귀하는 구성도이다. PC 출발 트랜잭션은 outbound 트래픽으로 사내 클라이언트 → 서버 → 내부 게이트웨이 → 침입차단시스템 → 스위치 → 라우터 통과후 인터넷 구간으로 접속된다. Inbound 트래픽은 인터넷구간 서버를 거쳐 인트라넷 구간 외부라우터 → 스위치 → 침입차단시스템 → 내부 게이트웨이 까지 접속된다.

4.2.2 데이터 수집 및 분석 방법

성능평가를 위해 사용된 임의의 로그파일 표본을 추출하여 data set으로 이용하고 실험은 RR(Round Robin) 스케줄링, LC(Least Connection) 스케줄링 방식으로 비교 실험한다. 데이터 수집 분석용 화면과 메뉴상에 검증조건이 설정된다. 데이터는 단순 텍스트 기반 정적 HTML문서와 C++언어로만든 간단한 CGI 동적문서 이다. 측정시스템은 운용 시스템 기존 인프라를 사용하되 별도로 측정용 에이전트PC, 서버장비와 측정도구, 측정화면을 준비하여 Linux7.0운영 체제에서 네트워크 시뮬레이터 NS2. 1b8a를 사용한다.

4.3 성능검증 항목

준비된 환경에서 트래픽처리를 기준으로 클라이언트

<표7> 데이터 수집 및 분석 자원

자원별	용도	장비명	수량
장비	데이터 수집 및 집계	· 제어 콘솔 · 데이터 수집서버 · 망 관리용 서버 · 중앙제어용 서버	1식 1식 1식 1식
	에이전트	· 에이전트 PC	3식
소프트웨어	데이터수집 분석	· IT 측정 시스템	1식
	Latency측정	· Latency측정시스템	1식
	네트워크관리	· NMS	1식

request의 초당 응답시간, 서버시스템 performance, 악성코드차단을 검증한다. 설계 도메인 성능측정을 위해 성능 정보를 구성하고 정의한다. 성능정보는 방역성능과 performance로 구분되는데 방역성능은 악성코드 차단실적, performance는 차단시의 CPU부하, latency, 응답시간이다.

<그림5> 데이터 수집 및 분석 화면

4.3.1 시스템 performance

• Performance

보안기능 부작용(side effect)으로서 발생 되는 시스템 부하수준 으로서 응답시간(responsetime), CPU부하율(CPU utilization) 이다.

• Latency

송신한 패킷이 측정 구간을 통과하는 소요시간이다. 측정작업에는 32bytes ICMP ping 패킷을 전송하여 구간까지 통과시간을 측정한다.

- 측정단위 : micro second

• 응답시간(response time)

단말에서 응답요구 패킷을 송신하고 호스트로부터 응답시간 패킷 수신 완료시까지 시간이다. 응답시간 = 네트워크 전송시간 + 서버 처리 시간 + 클라이언트 처리 시간

- 측정단위 : 초(second)

4.3.2 악성코드 차단 성능

차단이 이루어진 실적을 계량화한 수치로서 차단건수와 차단율로 구성한다.

- 차단건수 : 차단된 악성코드 건수
- 차단율 : 차단건수/총발생건수
- 미차단율 : 미차단건수/총발생건수

4.3.3 종합 효율

악성코드 차단실적과 차단 행위 원인으로 performance 부작용 발생 비율. 차단실적은 정(+), performance는 부(-)가 지향 목표

- 측정단위 : 차단율, 응답시간 지연율(%) 상호 비교 분석 지수

4.4 실제 측정결과

성능측정에 사용된 시스템은 ISP인 S기업 인트라넷이며 통신장비 성능, 침입차단시스템 소프트웨어 기능, 바이러스 월 기능은 기존 운용시스템이다. 인트라넷은 서버 1,000대, 워크스테이션급 PC 50,000대, 내부사용자 40,000명이며 생산, 재무, 인사, MIS, 등 20종 업무가 수용되어있다. 다수 기종 서버가 혼재되고 OS는 Unix, Solaris, VMS, AIX, HP-UX, NCR 등 다양하며 수시로 최신버전으

로 업데이트 된다. DBMS는 Oracle과 SQL을 사용하고 시스템구성은 클라이언트-Tuxedo-서버 3단계이다. 측정기간은 7일간 80회로 총 41시간이 소요되었다.

<표8> 측정작업 시행기간

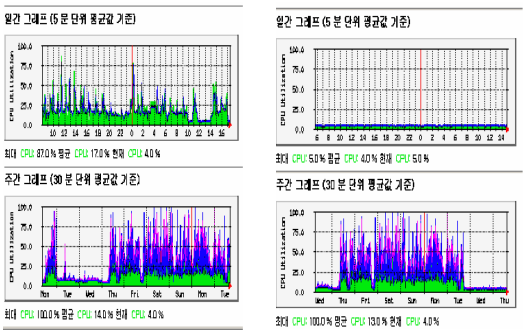
측정 기간	측정시간(시:분)	측정 소요시간 (시:분)	측정횟수 (회)	트랜잭션 (건)
1일차	08:00~14:00	04:00	11	2,198
2일차	09:00~14:00	05:00	11	2,665
3일차	09:00~16:00	07:00	12	2,992
4일차	08:00~16:00	08:00	12	3,523
5일차	08:00~12:00	04:00	11	1,752
6일차	08:00~14:00	06:00	12	2,482
7일차	08:30~15:30	07:00	11	3,209
계		41:00	80회	18,821

4.4.1 시스템 performance

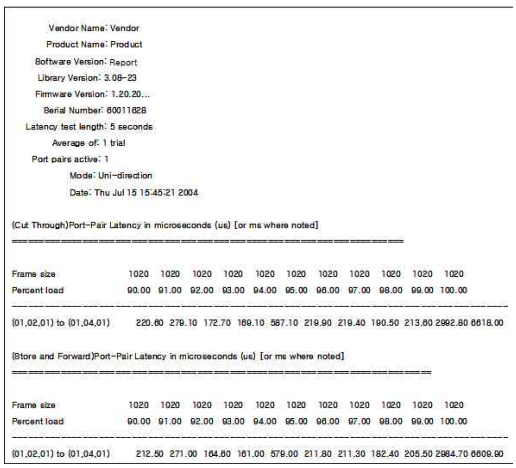
측정기간 동안 측정시스템의 인트라넷 내부게이트웨이 스위치를 설치하고 backbone switch CPU상에 게이트웨이 CPU 부하율 변화를 측정했다. 내부게이트웨이 설치전 급증하던 CPU 부하는 내부게이트웨이 설치후 하향되었다. 다음 <그림6>은 측정 기간중 유해 트래픽으로 인한 백본 스위치의 CPU 사용율 변화에 대한 화면이다. 그림에서 월간 CPU 사용율 17% 수준은 7%로 축소되고, 주간 단위 측정에서도 평균 14% 수준에서 13% 수준으로 하향 조정 되었다. 이는 정확한 형태를 알 수 없는 유해 트래픽이 네트워크를 통과하고 있음을 보여주는 것이다.

4.4.2 Latency 테스트

패킷단위 데이터의 latency 를 측정할 수 있는 경우로서 스위칭 구간을 조사 하였다. 서버처리 부하성능을 평가하기 위해 온라인 작업부하 특성을 파악하고 이에 맞는 latency 테스트를 실시했으며 request 요청에 따른 초당 응답시간을 실측했다. <그림7>은 latency 테스트 측정 결과표 이다.



<그림6> 내부게이트웨이 CPU부하율



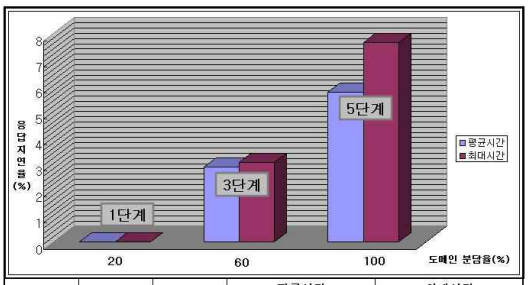
<그림7> 레이턴스테스트 측정결과

Performance 측정은 프레임 단위의 처리 시간 측정이 가능한 경우만을 조사하고 그 결과치를 다른 과정에 논리적으로 응용 참조할 수 밖에 없다. 측정 결과에 의하면 하나의 트랜잭션 처리시 latency 소요시간은 6,609 마이크로세컨드로 나타났다. 같은 기준에 의한 측정이 불가능한 나머지 단계는 스위칭 단계 latency를 참고할 수 있다.

4.4.3 응답시간(Response Time)

측정대상은 에이전트 단말PC에서 발신된 트랜잭션이 외부 네트워크 구간까지 왕복할 수 있도록 구성된 업무용 6개시스템 이다. 총 측정횟수는 10회이며 트랜잭션

카운트횟수는 총 12,775건으로 집계되었다. 보안도메인은 5개 영역이지만 차단단계는 유입 트래픽 4개단계로 구성된다. 즉 유입 트래픽의 경우 스위칭 → 침입차단 → 게이트웨이 → 서버 단계이거나 또는 스위칭 → 침입차단 → 게이트웨이 → 클라이언트 과정으로 처리된다. <그림8>는 1단계, 3단계, 5단계 차단 단계별로 도메인별 응답시간 변화를 보여주고 있다. 도메인 처리시간을 평균시간과 최대시간별로 구분하여 시간 증가율을 측정한 결과 평균시간 경우 1단계 차단시 0.8474초가 소요되고 3단계 차단은1.695 초, 5단계 차단은 3.39초가 소요된다. 시간 증가율은 3단계에서 2.875% 증가, 5단계 차단에서 3.06% 증가 수준이다.



구조	차단단계	패킷처리횟수	평균시간		최대시간	
			시간(초)	증가율(%)	시간(초)	증가율(%)
기존구조	1단계	1	0.8475	0	1.91825	0
통합구조	3단계	2	1.695	2.875	3.8365	3.06
	5단계	4	3.39	5.75	7.673	7.65

<그림8> 응답시간 측정결과

4.4.4 악성코드 차단

L7 컨텐츠 필터링으로 query 대상 및 DDoS 공격에 대한 사전 차단과 신규 인터넷 웜 바이러스를 차단했다.

악성코드 방역 유형은 감염된 URL의 접속 차단, 웜유입 차단, 악성코드 감염 트래픽 과 site 추적, 악성 코드 감염 IP 추출 및 차단, DDoS 방지이다. 이 기간중 발생한 악성코드 종류는 Blaster, Welchia, Agobot, Mydoom으로 채집 되었다. 악성코드 발생량과 차단실적은 조사가능 방법으로 집계된 것이며 조사된 사항은 발생실적 대비 98% 차단을 나타냈다.

<표9> 악성코드 종류별 차단실적

구분	Blaster	Welchia	Agobot	Mydoom. A	Mydoom. B
방역조치	▪ URL차단 ▪ Windows 업데이트 ▪ COM차단 ▪ DDoS방지 ▪ 웜 차단	▪ URL차단 ▪ www.microsoft.com 차단 ▪ 감염 IP 추출 및 차단 ▪ DDoS방지 ▪ 웜 차단	▪ URL 차단 ▪ Dunghole. myqld.com접속 시도 IP 추출 ▪ DDoS방지 ▪ 웜 차단	▪ URL 차단 ▪ www.sco. com 차단 ▪ 감염 IP 차단 ▪ DDoS방지 ▪ 웜 차단	▪ URL차단 ▪ www.microsoft. com 차단 ▪ DDoS방지 ▪ 웜차단
발생	710,100건	103,000건	9,000건	280,000건	190,000건
차단실적	▪ 710,000 건 차단 ▪ 감염 트래픽과 Site 추적	▪ 102,900건차단 ▪ 감염 IP 4,063개 추출	▪ 8,900 건 차단 ▪ 감염 IP 추이 분석	▪ 278,000 건 차단 ▪ 감염IP추출	▪ 189,000건 차단 ▪ 감염IP추출

V. 결 론

종합효율은 performance, latency와 차단실적간 상관관계 이다. 도메인별 종합효율 분석이 이상적이지만 악성코드 차단실적을 도메인별로 구분한 집계는 기술적으로 어려우므로 대안으로서 도메인별로 방역메커니즘기능이 적용돠는 도메인수를 기준으로 종합효율을 산출한다. 그 결과 5단계의 다단계 차단일수록 방역효율은 높고 latency는 증가 한다. Performance 지연은 3단계 차단에서 평균 1.695초, 최대 3.8365초 정도 이며 5단계 차단에서도 평균 3.39초 미만, 최대 7.673초 미만 수준이다. 도메인 수 증가에 따른 latency 증가는 우려한 수준이 되지 않고 있는 것 으로 분석 되었다.

종합효율은 다단계 차단구조 적용시 전체적 performance에 지장을 초래하지 않고 차단 기능이 수행된다. 즉 performance 지연은 종전의 1단계 차단, 3단계 차단연구와 비교하여 5단계 차단 연구결과 두드러지게 증가하지 않았다. 차단 완전성은 1단계보다 3단계가, 3단계보다는 5단계가 상대적으로 유리하다. 5단계 차단은 전방위의 zone으로 차단영역 확대로 차세대형 차단 구조로서 강력한 방역기능 실현이 가능하다. 결론적으로 보안도메인은 5단계까지는 방역효율을 높이면서

<표10> 도메인별 효율분석

도메인유형	방역메커니즘	도메인수		응답시간(%)
		방역	미방역	
3단계 방역	스위칭, 침입차단	1	2개영역 (40%)	평균 2.875% 최대 3.06%
	서버 방역	1		
	클라이언트 방역	1		
	소계	3		
5단계 방역	스위칭	1	없음	평균 5.75% 미만 최대 7.65% 미만
	침입차단필터링	1		
	내부 게이트웨이	1		
	서버 방역	1		
	클라이언트 방역	1		
	소계	5		

performance는 심각하지 않은 수준이다. 보안도메인은 새로운 설계사상을 기반으로 프레임워크 도출과 기능 메커니즘을 구성했으며, 통합구조, 다단계 차단, 차별화 차단 구조이다. 제안 방식은 보안 스캐너와 백신등 방역 소프트웨어 적용을 전제로 하고 있으며 신·구 백신간 신속한 업데이트 과정이 필수적이다. 본 제안 방법론은 향후 업무운용 현장에서 응용될 수 있을 것으로 기대한다.

참고문헌

[1] Mart Bishop, “Computer Security,” Addison Wesley, 2000.

[2] Timothy P. Appleby, “Building a Virus Protection Infrastructure,” CHI Publishing Ltd, 2000.

[3] Sichoon Noh, Dong Chun Lee, and Kuimam J. Kim, “Improved Structure Management of Gateway Firewall Systems for Effective Networks Security,” Springer, 2003.

[4] Sichoon, Noh, Dong Chun Lee, “Multi-Level Protection Building for Virus Protection Infrastructure,” SCIE LNCS 3036, 2004. 6.

[5] Sichoon, Noh, Dong Chun Lee, “Assurance Method of High Availability in Information Security Infrastructure System,” SCIE LNCS 3794, 2005. 12.

[6] Sichoon, Noh, Kuimam J. Kim, “Building of an Integrated Multilevel Virus Protection Infrastructure,” IEEE Computer Society, 2005. 12.

[7] Sichoon, Noh, “A Securing Method of Multispectral Protection Infrastructure for Malicious Traffic in Intrnet System,” DCS, 2006. 02.

[8] Sichoon, Noh, Dong Chun Lee, Kuimam J. Kim “Protection Structure Building for Malicious Traffic Protecting in IntrnwtSystems,” SCIE LNCS 3981, 2006. 05.

[9] Sichoon, Noh, “Active-Active High Availability of Information Infrastructure System for Effective Network Security,” IEEE Computer Society, 2008. 01.

[10] Sichoon, Noh, “MSPI(Multi-Spectral Protection Infrastructure) System for Optimal Network Security,” IEEE Computer Society, 2008. 08.

[11] Nortel Networks Korea, “애플리케이션스위치를 이용한 네트워크 보안,” 2003.

[12] 나병윤, “시스템 및 네트워크 트래픽 모니터링,” (주) PGPnet, 2003.

[13] 장윤정, “L7스위치로 네트워크 활용도를높여라,” 네트워크타임스, 2003.

■ 저자소개 ■

나 상 엽
Na, Sang Yeob

1996년~현재 남서울대학교 컴퓨터학과 교수
2005년 Carnegie Mellon University School of Computer Science MSIT(Master of Information Technology)
2001년 동국대학교 컴퓨터공학과 (공학박사)
1995년 동국대학교 컴퓨터공학과 (공학석사)

관심분야 : 정보보호, 정보검색, 데이터 마이닝
E-mail : nsy@nsu.ac.kr

노 시 춘
Noh, Si Choon

2005~현재 남서울대학교 컴퓨터학과 교수
2005 경기대학교 정보보호기술(박사)
2004 KT 충청전산국장
2002 KT 시스템보안부장
1987 고려대학교 경영정보학(석사)

관심분야: 차세대통신, 컴퓨터네트워크, 정보보호
E-Mail: nsc321@nsu.ac.kr

논문접수일 : 2009년 10월 12일
수 정 일 : 2009년 11월 11일
게재확정일 : 2009년 11월 17일