MSPI설계를 통한 유해 트래픽 차단

노 시 춘*

요 약

이 논문에서는 기존 정보보안체계의 취약성에 대처하고 보다 강력한 침입차단을 위해 통합화된 인프라스트럭처 구조를 제안했다. 제안된 인프라스트럭처는 정보보안 프레임워크, 기능메커니즘, 통합화구조에 기반한 정보보호스킴으로 구성되었다. 이 논문은 오늘날의 바이러스방역환경에서 악성트래픽을 효과적으로 차단하기 위해서는 인프라스트럭처를 기본으로 구조개선과 스캐닝툴의 효과적인 결합을 통한 대응이 최적의 접근방법임을 제시하고 있다. 본 논문을 통해 인프라스트럭처상에서의 성능분석모델을 제시했으며 이 분석모델을 통해 1단계, 3단계, 5단계 차단단계별 성능측정이 가능함을 실험을 통해 보여줬다. 최적의 정보보호를 위한 효율적인 인프라스트럭처 구조는 사용자 또는 사용자조직에 의해 계속적인 진단과 평가 및 튜닝이 필요함을 본 연구에서는 결론으로 강조했다.

Malicious Traffic Protection through MSPI Designing

Si Choon Noh*

ABSTRACT

In this paper, we proposed an integrated infrastructure for optimal information security to resolve these kinds of problems and to implement more powerful protection. The proposed infrastructure presents a security framework, provides a functional mechanism, and implements a scheme for information security based on the design concept of integrated structures. In order to ensure effective malicious traffic blocking, this paper emphasizes that a comprehensive approach through infrastructure improvement and combination of scanning tool is the only measure for preparing against today's environment of virus infiltration. The proposed model is a measure developed at a time when a permanent technological solution to virus is yet to be developed. A performance analysis model is developed and the performance is evaluated through the case studies for the proposed methodology. The effectiveness of the infrastructure for optimal information security needs the continuous diagnostic evaluation and tuning through the users or the organizations.

Key words : MSPI(Multi Spectral Protection Infrastructure)

* 남서울대학교 컴퓨터학과

1. 서 론

현재의 방역 환경하에서 PC나 서버 단위로 바이러스를 삭제, 차단하는 소위 거점(Station 또는 Traffic Node) 방역은 어느 정도 기능적 속성상의 취약 요소가 내재되어있다. 순간적으로 전파되는 바이러스를 모든 서버나 PC단위로 일일이 삭제하고 차단하게 되므로 비록 백신기술이 뛰어나고 자동화 방식이라 해도 정보 시스템별 특성에 따라 발생할 수 있는 일정 부분의 방역 누수가 그것이다. 두 번째의 취약점은 특히 심각하게 문제되는 부분으로 소위 인트라넷 내부네트워크 경로(Traffic Route)를 따라 바이러스가 확산하는 것인데 거점 상에서의 바이러스 진단, 삭제, 유입 차단이라는 방역망을 통과한 바이러스가 네트워크 내부경로를 통해 확산되는 경우이다. 수많은 서버와 PC에서 바이러스를 삭제해도 네트워크 상에 바이러스가 존재하는 것은 거점방역기능 자체가 가진 속성에 기인한 방역 누수가 원인이고, 백신기술 발전에도 불구하고 바이러스의 네트워크 확산이 계속되는 것은 거점 방역은 원래 임무 자체가 네트워크 경로상의 확산 차단 용도가 아니기 때문이다.

이제 바이러스 방역 개선책은 완전예방과 완전차단 대신 현실적 대안으로서 유통 바이러스를 인트라넷의 트래픽 주요 통과경로에서 차단 삭제해야 한다. 이를 위해 현재의 거점 방역 조를 사용하면서도 네트워크 경로 상 확산차단을 추가하는 것이다.

본 연구는 오늘날의 방역체계 환경에서 바이러스를 비롯한 각종 악성코드 공격 패턴에 대응할 수 있는 방역인프라는 어떤 구조로 구성되어야 하는 가에 대한 대안을 제시하기 위해 널리 사용되고 있는 일반적인 방역 체계 구조의 성격과 취약점을 진단하고 이를 개선할 수 있는 개선된 방역 체계를 제안했다.

2. 기존방역체계의 취약성

일반 방역 체계는 바이러스 발생시 이를 진단, 차단할 수 있는 대응 소프트웨어를 개발하여 방역 대상 자원에 설치, 방역에 임하고, 향후 추가의 유사 바이러스가 나타나면 장착된 백신엔진을 업데이트하는 방법이다. 이는 예방기능이라기 보다는 사후대처 기능에 속하고, 구조적으로 다음과 같은 한계점이 나타나고 있다.

- 신종바이러스는 백신엔진 개발전에 이미 네트워크에 침투해 버리고 네트워크상에서 각종자원에 유입되어 버린다.
- 바이러스백신 설치과정에서는 인트라넷내 모든 서버와 PC자원에 일시에 완벽한 백신 장착이 어렵고 여러 가지 원인으로 방역 누수가 발생한다.
- 외부에서 반입된 오염된 플로피디스크, CD 등의 매체를 통해 인트라넷 내부를 감염시킨 경우 네트워크 관문 방역에 관계없이 내부망 감염이 계속된다. 백신중심 방역 매커니즘에서는 이상과 같은 요인으로 네트워크에 이미 침투해버린 웜, 바이러스, 트로이 목마로 인한 바이러스 기동과 삭제라는 악순환이 불가피하게 반복되고 있다. 현재 모든 조직, 모든 인트라넷 시스템에서는 이상의 문제점을 근본적으로 해소하지 못한 채 정보시스템이 운영되고 있다.

3. MSPI 설계

3.1 인프라구조설계

보안인프라 구조는 인트라넷, LAN 등 네트워크 상에서 보안기능과 관점에서 네트워크 구조를 정의하고 분류하는 개념이다. 보안 인프라 구조는 일반 네트워크 구조상의 어느 접속점, 어떤 경로상에, 어떤 종류의 보안 장치를 배치하고 연계시키는가에 따라 그 형상적 의미와 종류가 결정된다. 보

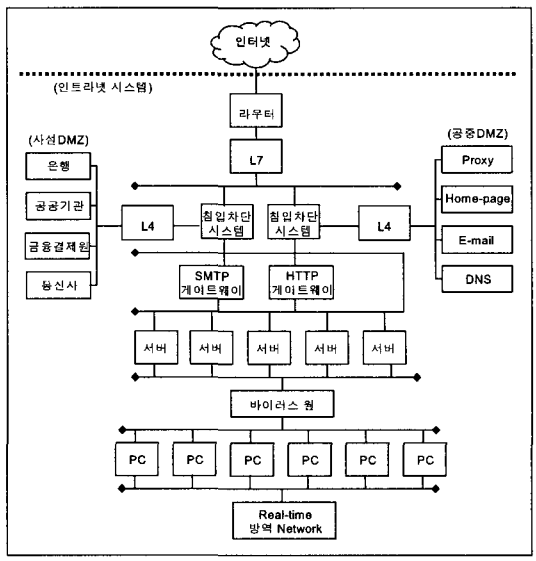
안 네트워크는 일반적인 네트워크 구조분류 기준, 즉 트래픽 경로 설정방법, 네트워크 그룹간 접속방법, 서버와 클라이언트 그룹 배치방법에 따라 구조와 형상이 결정될 수 있다.

또한 보안기능 관점으로 분류해 본다면 다음 표와 같이 트래픽 경로, 외부네트워크 접속점, 내부 스테이션배치 등을 기준으로 구조를 검토 할 수 있다.

〈표 1〉 인프라구조 설계 도출 방법

유 형		항 목	판단 기준
트래픽 경로 설정 방식	내부 경로	• 공용 경로 사용	• 인트라넷 접속 경로를 단일경로로 구성 -모든 트래픽이 공용 경로로만 소통
		• 분리경로 구성	• 서브 네트워크 별로 경로를 분리하는 방식
	외부 경로	• 복수 경로 구성	• 인터넷, 비 인터넷 구간을 분리 • 인터넷 구간 복수 경로
		• 단일 경로 사용	• 인터넷, 비 인터넷 미 분리 공동 사용
외부 네트워 와의 접속방법		• 다원화 접속	• 하나의 게이트웨이 상에서 복수의 네트워크 그룹을 접속 • 동종의 프로토콜과 전송 표준 사용시 가능
		• 분리 접속	• 네트워크 그룹간 별도의 게이트웨이나 접속점을 관리
내부 스테이션 배치 방식 -서버, 클라이언트 배치		• 별도 서버 Farm 설치 • 서버, 클라이언트 분리	• 서버 Farm 별도 구성 • 클라이언트 네트워크 별도 구성
		• 서버, 클라이언트를 동일 레벨로 배치	• 서버, 네트워킹 장비로만 분리

논문에서는 스위칭 구조, 침입차단시스템 필터링 구조, 게이트웨이 필터링 구조, 서버 방역 구조, 클라이언트 방역 구조를 기준하여 일차적 구조를 설계했다. 이때 업무특성, 네트워크 인프라 구조, 보안 환경, 트래픽 볼륨, 트래픽 특성 등을 고려하여 구조가 검토되어야한다. MSPI 종합 구조도는 네트워크 인프라상의 5단계 차단 구조와 각 Tiers 별 개별 구조도를 결합하여 실용화할 수 있는 구조를 도출했다. 종합 구조도는 네트워크 인프라와 바이러스 차단 보안 장치를 결합했고 각 부분을 실용화 구조로 설계했다. 외부 네트워크와의 접점에서부터의 트래픽 경로는 일반 PSTN 구간, 인터넷 구간을 분리구성하며 경계선 라우터에서는 내부 네트워크와 DMZ 구간을 구분하였다. 내부 네트워크는 침입차단시스템 구간을 HTTP, SMTP, 기타 구간으로 3원화 분리했고 침입차단시스템 이후 게이트웨이 구간 또한 침입차단시스템 구간과 동일한 방식으로 트래픽을 볼륨 규모 기준으로 경로를 구분했다. 게이트웨이 하부의 내부 네트워크 구간에서는 각종 서버팜을 대상으로 서버스 바이러스 월을 구축하고 클라이언트 대상으로 하는 리얼타임 방역망을 구성하였다. 다음 그림은 이 같은 기준으로 도출한 구조도이다.



(그림 1) MSPI인프라 구조도

3.2 기능구조 설계

MSPI기능구조는 차단기능이 어떤 영역, 어떤 종류로 구성되는가에 대한 기능설계이다. 차단기

능은 인프라구조상에서 영역별로 패킷스위칭, 패킷필터링, 차단(Protection)등으로 우선분류 되는데 실제 현장에서는 이 같은 차단기능이 순수한 차단기능으로 구성되기도 하고 네트워킹 기능과 결합하거나 연동하여 구현되기도 한다. 따라서 오늘날의 차단기술을 보안기능과 네트워킹 기능으로 엄격하게 분리하기가 어렵고 상호 연동작용을 통해서 기능이루어지는 것을 반영했다. 이 구성에 따른 세부 기능의 종류는 <표 2>와 같다.

〈표 2〉 차단기능구성도

기능 영역	네트워크 기능	보안 기능	
		차단 기능	효율성 기능
스위칭	• 네트워크 로드 밸런싱 • 캐시 리다이렉션 • 서버 로드 밸런싱 • 침입차단시스템 로드 밸런싱	• 웜 바이러스 차단 • 해킹 공격 차단 • 컨텐츠 스위칭 • 컨텐츠 필터링	• 서버 로드 밸런싱 • 침입차단시스템 로드 밸런싱 • 네트워크 로드 밸런싱 • 고가용성 구조 • 실시간 방역
침입차단 시스템 필터링	• 패킷 필터링 • 접근 제어 -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 • 바이러스 차단	• 실시간 방역 • 자동화 방역
서버 방역		• 바이러스 유입 차단 • 백신 업데이트 • 바이러스 감염 진단 • 바이러스 삭제	• 실시간 방역 • 자동화 방역
클라이언트 Real-time 방역		• 바이러스 유입 차단 • 바이러스 감염 진단 • 바이러스 삭제 • 백신 업데이트	• 실시간 방역 • 자동화 방역

먼저 트래픽 경로는 설계 프레임워크에서 제시한 바와 같이 트래픽 경로를 기준으로 방역존이 설정되면 그 결과를 토대로 차단 기준정보를 구성하고 이어서 차단단계를 구성한다. 이 같은 제반 단계의 결과는 차단 기능 구성으로 나타난다. 차단기능 구성을 통해 실제적인 차단기능이 구현되도록 설계하였다. MSPI 방역알고리즘은 구조 설계를 통해 구성된 종합구조, 트래픽 소통경로, 경로방역망 구조, 단계별 방역기능 분담구조를 기반으로한 바이러스 차단기능 수행 매커니즘 구성에 관한 것이다. 다시 말하면 네트워크 차단구조를 가동했을 때 각 구조별로 작동되는 기능의 수행원리이다. 따라서 방역 알고리즘의 구성은 영역별 단계별 차별화된 고유한 기능이 수행된다. 설계된 방역 기능을 적용했을 때 단계별로 방역 구간이 설정되며 각 구간마다 방역을 수행할 수단인 보안 인프라가 필요하고 아울러 각 보안 인프라가 수행하는 방역 기능이 존재한다. 이상과 같은 매커니즘은 다섯 단계의 방역 구간, 보안 인프라, 방역 기능이 상호 연동되어 전체적인 방역 알고리즘을 형성한다.

3.3 동작 메커니즘 설계

MSPI동작 매커니즘 구조는 네트워킹기능, 효율성 기능, 침입차단기능 3단계로 계층화된다. 네트워킹계층은 보안 인프라가 구성, 설정되는 기본틀인 네트워킹 계층의 기능을 말한다. 네트워킹 기능은 OSI 7 레이어별로 차별화된 네트워킹 기능 구조를 형성하고 이 구조상에서 라우팅, 스위칭, 브로드캐스팅 등 인터네트워킹 기능, 데이터전송 기능 그리고 패킷처리 기능을 수행한다. 다이어그램으로 표현해 본다면 이 같은 네트워킹기능의 영역 내에 효율성 기능과 침입차단 기능이 존재한다. 효율성 기능은 네트워킹 기능을 토대로 하지만 침입차단 기능 구현시 적용되어야 할 필수적인 지원 기능 또는 연관기능이다. 효율성 기능은 성격상 3

개 세부 영역으로 분류되는데 고가용성 기능, 통합 관리 기능 및 자동화 처리와 실시간 처리 기능이다. 침입차단 기능은 인프라 구조의 목적에 해당되는 바이러스와 각종 악성코드 침입차단 기능이다. 침입차단 기능은 OSI 계층별 차단, 트래픽 소통 경로별 차단, 방역 존별 차단으로 분류될 수 있다. OSI 계층별 차단은 OSI 레이어 2에서 레이어 7까지의 계층별로 수행되는 차단기능이다. 경로별 차단은 외부 라우터에서부터 최종 클라이언트까지의 트래픽 경로별로 수행되는 차단이다. 방역 존별 차단 기능은 각종 리소스별로 차단 기능이 수행되는 것이다.

3.3.1 동작단계 설정

차단 기능 기본구도는 방역 존별 차단, 차단 기준 정보별 차단, 차단 단계별 차단, 차단 기능별 차단으로 구성된다. 방역 존별 차단이란 방역을 해야할 영역별로 어떤 기준으로 범위를 설정하는가에 관한 것이다. 일반 구조는 하드웨어 리소스별 기준으로 방역 존을 구성했다. 일반 구조의 하드웨어 리소스 기준은 각종서버와 클라이언트를 방역 대상으로 삼는 것이다. MSPI에서는 방역 존을 트래픽 경로별로, 정보 자원별로, 하드웨어 리소스별로 세 개의 카테고리로 구분하여 설정했다.

〈표 3〉 기능아키텍쳐

방역 zone	차단 기준 정보	차단 단계	차단 기능
• 트래픽 경로 • 정보 자원 • 하드웨어 리소스	• MAC 주소 • IP 주소 • 프로토콜 종류 • TCP, UDP 서비스 종류 • 컨텐츠 기반 • 트래픽 볼륨	• 외부 관문 • 내부 관문 • 내부 게이트웨이 • 내부 네트워크	• 진단 • 삭제 • 거점 차단 • 치료 • 경로 차단

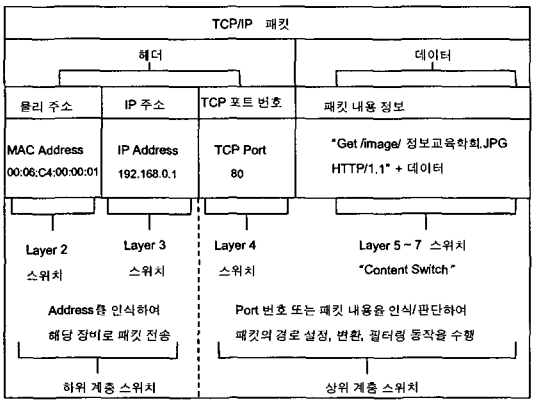
먼저 트래픽 경로는 설계 프레임워크에서 제시한 바와 같이 트래픽 경로를 기준으로 외부라우터 - 외부스위치, 외부라우터 - 침입차단시스템, 침입차단시스템 - DMZ, 침입차단시스템 - 내부 네트워크 등 4개 영역으로 편성한다. 그중 내부네트워크는 게이트웨이 구간, 서버 구간, 클라이언트 구간으로 더 세부적 설정이 된다. 정보 자원별 존이란 저장 매체, 공유폴더, 뉴스그룹, 그룹웨어 등으로 사용하는 정보 영역별 구분을 하는 것이다. 하드웨어 리소스는 웹 서버, Exchange 서버, SMTP 서버, 파일 서버, 클라이언트 등으로 나눠서 설정한다. MSPI 기능 기본 구도 중 두 번째 카테고리는 차단 기준정보별 기능이다. 차단 기준 정보별 기준이란 차단을 어떤 기준정보, 어떤 키값으로 시행하는냐 하는 방법이다.

고전적인 IP 주소 또는 포트 스캔에서 이제는 자신의 MAC이나 IP 주소를 바꾸어서 침입을 시도하는 도구들이 사용되고 있다. 또한 SYC, RST, ACK 공격과 같은 여러 가지 형태의 서비스거부를 유발시키는 공격패턴이 많이 알려져 있다. 이러한 침입시도(Intrusion)나 공격(Attack)이 대부분 고의적으로 발생하겠지만 최근에는 트로이 목마 유형의 바이러스에 의해 발생하기도 한다. 2계층 차단 기준 정보는 MAC 주소, 3계층 차단 기준 정보는 IP 주소, 4계층의 경우 하위 계층 기준 정보를 포함 TCP, UDP, ICMP 프로토콜 종류, TCP, UDP 포트 번호로 설정된다. 5계층에서부터 7계층까지의 기준 정보는 컨텐츠 기반 정보를 기본으로 한다. 컨텐츠 기반정보는 제목, URL을 비롯 컨테츠 내용 중 키워드(Key Word) 기준으로 설정할 수 있고 이 경우는 보안솔루션별로 선택기능을 부여한다. 마지막으로 트래픽 볼륨이란 트래픽의 양적 기준을 참조하여 악성 트래픽 여부를 판단하는 것이다.

3.3.2 트래픽 경로설정

단위 네트워크 룹에 유입되는 트래픽은 내부, 외부 경계선에 위치한 외부 라우터(Exterior Router)를 통해 경로 배정과 포워딩이 이루어진 다음 스위칭 단계로 유입된다. 스위칭 단계에서는 네트워

킹 기능, 보안 기능이 수행되고 더불어 효율성 기능이 구현된다. 본 절에서 설명하는 내용은 보안 기능 중 스위칭 단계 기능 구성 내용이다. 스위칭 기능은 L2에서 L7까지 수행된다. L2~L3까지의 기능은 일반적인 네트워킹 처리과정의 트래픽 경로 배정과 부하 분산 기능을 위주로 수행한다. 즉 물리 주소, IP 주소, TCP 포트 번호를 기준으로 스위칭 기능이 수행된다. 해킹, 바이러스 차단 기능으로서의 본격적인 방역 기능은 L4, L7 스위칭 기능을 통해 구현되는데 그 이유는 L4 이상의 상위 계층 스위칭은 IP 주소, TCP 포트 번호를 기준으로 가동되고 특히 L7 스위칭은 패킷의 특정 URL 정보, 제목, 내용을 나타내는 검색어 등 소위 컨텐츠를 기준으로 스위칭 되기 때문이다. 따라서 L7 스위칭을 상위 계층 스위칭이라고 분류하며 해킹, 바이러스 침투를 차단하는 기능으로서는 특히 L7 스위칭 기능을 채택한다.



(그림 2) OSI 레이어별, 스위치별 스위칭 기능

3.3.3 트래픽 스위칭

외부 라우터(Exterior Router) 이후 침입차단시스템 전단에서 트래픽스위칭을 실시한다. 스위칭 목적은 전통적 기능인 부하 분산(Load Balancing) 기능 외에 컨텐츠 인식 기능을 갖는 레이어 7 스위칭을 추가 수행하기 위해서 이다. 이 기능을 통해서 컨텐츠 기반 패킷 필터링과 앤티바이러스 기능, 응용 레벨의 미러링(Mirroring)을 추가 수행한다. 컨텐츠 기반 패킷필터링 기능은 앤티바이러스 기능의 근간이 된다. 네트워크상에서 기승을 부리는 님다, 코드레드, 마이둠 등 바이러스는 기존의 침입차단시스템 기능만으로는 해결하기 어렵고 스위치 단계에서 강력한 패킷 처리 능력과 인지 능력을 통해 보안 기능을 제공으로 차단하게 된다.

3.3.4 패킷검증

전계층 스위칭을 통해 URL기반으로 웹 서버를 분리해 웹 서비스가 가능하게 된다. 특정 URL에 대해 특정 웹서버가 처리할 수 있도록 전계층 스위칭을 적용하는 것이다. 예를 들면 동적으로 변경되는 페이지는 서버 1 웹 서버에 저장하고 정적인 HTML 텍스트나 이미지 등은 서버 2에 저장해 웹 서버 관리를 효율적으로 할 수 있다. 이렇게 서로 특성이 다른 웹 페이지를 별도로 관리하고 웹 서버에 특성을 조절함으로서 최대의 성능을 낼 수 있다. 이러한 기능은 특히 캐쉬 서버(Cash Server)의 리디렉션이나 침입탐지 시스템(IDS : Intrusion Detection System)상에서 서버 로드 밸런싱을 수행할 경우에 매우 효과적으로 웹 서버의 성능을 극대화시키게 된다.

3.3.5 악성 트래픽 차단

NBAR(Network-Based Application Recognition) 기능은 QoS(Quality of Service)의 큐잉(Queuing) 방법 중에서 CBWFQ(Class-based Weighted Fair Queuing)기능에 포함된다. CBWFQ는 특정 기준에 의해 트래픽을 분류(Class-map)하고 분류한 트랙픽에 대해 하나 또는 그 이상의 정책을 적용(Policy-map)하여 라우터의 인터페이스에 Policy-map을 적용(Service Policy)한다. 따라서 Class-map을 어떻게 분류하는지 Policy-map을 어떻게 적용하는

지, 인터페이스에 적용할 때는 어떻게 적용하는지 등 경우의 수가 많기 때문에 폭넓은 설정과 세심한 조정이 동시에 가능한 방법이다. NBAR는 CBWFQ를 이용해서 라우터에서 구현하기 어려운 여러 가지 기능을 제공한다. NBAR는 동적 TCP/UDP 포트를 사용해서 분류하기 힘든 프로토콜이나 웹 기반의 프로토콜 등과같이 다양한 애플리케이션을 인식할 수 있는 분류 엔진(Classification Engine)이다. NBAR는 다음과 같이 몇 가지 분류 기능이 있다. 동적으로 할당된 TCP, UDP 포트번호를 가진 애플리케이션 분류, URL, HOST, MIME (Multipurpose Internet Mail Extension)타입에 의한 HTTP 트래픽의 분류, 애플리케이션 이름에 의한 ICA(Independent Computing Architecture)분류이다. 이 중에서 'URL, HOST, MIME 타입에 의한 HTTP 트래픽의 분류' 방법을 이용해 코드레드, 님다 등과 같은 웜 바이러스 형태의 공격을 라우터에서도 차단할 수 있다. NBAR는 애플리케이션 트래픽을 TCP/UDP 포트번호 이상으로 분석할 수 있다. 이것은 서브포트 분류(Sub-port Classification)방법이다. NBAR는 TCP/UDP 페이로드 자체를 판독하고 트랜잭션 식별자, 메시지 타입, 다른 유사한 데이터와 같은 내용물에 따라 패킷을 분류한다. URL, HOST 또는 MIME 타입 등은 HTTP 트래픽에서 Get 요청시 URL이나 HOST 필드내에 있는 규칙적으로 나오는 텍스트에 의해 HTTP 트래픽을 분류할 수 있다. L7스위칭은 TCP/IP 서비스 포트 0~65,535까지 지원한다. 따라서 MAC 주소, IP 주소 또 프로토콜 대상 하위계층 스위칭을 포함하여 트래픽의 모든 헤더정보와 데이터를 판독하므로 소위 말하는 컨텐츠 스위칭이 가능하다. 모든 입력데이터는 이상과 같은 기준으로 패킷 프로세싱 처리단계를 거쳐 큐잉되거나 포워딩된다. 동작과정에서는 설정된 정책(Rule)과 세션데이터 및 애플리케이션 정의(Application Definition) 라이브러리가 스위칭 기능의 정보로 활용된다.

4. 성능분석

성능 즉 통신 장비의 성능, 방화벽 소프트웨어 기능, 바이러스 월 기능 등은 MSPI구조 설계 전후 모두 동일한 환경이다. 따라서 각 자원은 자체적인 성능개선을 통해 차단 성과 제고가 있을 수 있으므로 본 논문에서는 이 같은 관련자원의 성능을 동일한 것으로 전제하고 다만 차단 인프라 구조 개선시의 방역 효율만을 검증한다. 본 논문에서 제시한 5가지 영역의 구조도 즉 네트워크 구조도, 스위칭 구조도, 침입차단 구조도, 게이트웨이 구조도, 서버 바이러스 월 및 리얼타임 방역망 구조도 중 인프라 구조 개선 전후 성과 비교가 가능한 네트워크 구조도를 대상으로 효율성을 검증한 것이다.

4.1 측정환경

분석 환경은 A기업 인트라넷 시스템 상에서 실제 업무를 대상으로 검증을 실시했다. 본래의 네트워크 구조가 MSPI 설계 사상으로 사전구비된 것은 아니므로 본 검증 작업을 위해 측정 목적의 보강과 환경 준비 단계를 거쳤다. 인용된 A기업 업무 환경과 인트라넷의 트래픽 처리 환경은 각종서버 1,000대, 워크스테이션급 PC 30,000대, 내부사용자 규모 40,000명으로 구성되었다. 네트워크 구조는 인트라넷과 외부망 연결은 310Mbps 속도의 복수회선으로 구성되었고, 인트라넷입구에 침입차단시스템이 설치되었으며 침입차단시스템 이후구간에는 인트라넷이 구성되었다. 인트라넷 내부구조는 서버 전단에 별도의 메일 검색시스템이 설치되었으며 PC자원을 대상으로 개별 단위 바이러스 백신이 설치되어 있다. 트래픽 규모는 일간 약 10억 패킷이 처리되는 대규모 볼륨(Volume)이고 상시 10만 정도의 네트워크 세션(Session)이 접속되고 있다. 전반적인 인터넷 관련 트래픽은 최근 4년간 약 5배가 증가되었으며 기업의 업무규모 비대화와 함께 네트워크 규모도 증가 속도가 빠르게 진행되고 있다.

4.2 측정 항목 대상

차단 실적은 최초 차단 단계(스위칭 단계)와 최종 차단 단계(클라이언트)의 차단 실적이 측정 목표 항목이다.

- 최초 차단 단계는 인트라넷 관문의 차단으로서 바이러스를 비롯한 악성트래픽은 도메인 진입 전인 관문에서 1차적으로 최대한 차단이 이루어져야 하므로 1차 관문의 1차 차단 실적을 측정한다.
- 최종 차단 단계는 악성코드가 실제적으로 사용자 자원에 직접 침투하는 구간으로서 MSPI 구조 차단 성과는 이 도메인에서 반드시 구현되어야함으로 이 단계의 차단 실적을 측정한다.
- 내부 게이트웨이 구간은 바이러스를 비롯한 악성 트래픽을 여과시키는 구간이다. 악성 패킷은 침입차단시스템 상에서 IP 주소, 프로토콜, TCP 서비스 번호 등을 기준으로 1차적 필터링이 이루어져서 패킷의 주소와 형태적으로 정상이지만 패킷의 컨텐츠 상으로 비정상 트래픽을 구분하는 것이다. 따라서 이 구간에서는 모든 악성 트래픽 차단 실적을 일반 구조와 MSPI 간 시스템 부하율 변화을 통해 측정한다.

〈표 4〉 측정항목

구 분	측정 구간	측정 항목	측정 단위
바이러스 발생량	5개 구간	바이러스 및 악성 트래픽 발생	• 건수
바이러스 차단실적	스위칭 구간	구간 바이러스 차단 실적	• 건수
	5개 구간 합계	총 구간 차단 실적	
퍼포먼스	내부 게이트웨이	CPU 부하율	• %
	서버 구간	CPU 부하율 시스템 프로세스수	• % • 건수
	스위칭 구간	Latency	• micro second • mili second • second
	5개 구간 합계	응답 시간	
고가용성	3개 구간	부하부산율, Data-loss율	• %

- 서버 방역 구간 방역의 특징은 이메일 바이러스 차단이다. 일반적인 악성코드와 바이러스 중 이메일을 통한 바이러스가 절대 다수 비율을 점유하고 있음으로서 이메일 바이러스 차단 실적을 통해 서버 레벨의 방역 성과를 측정한다. 이때의 측정은 바이러스 차단 전후 성능을 다각적으로 비교 측정한다.

4.3 실제 측정결과

4.3.1 퍼포먼스 측정결과

응답시간 측정은 조사 기간 7일간 총 60시간 10분이 소요되었다. 측정 대상 시스템은 에이전트 PC에서 발신된 트랜잭션이 외부 네트워크 구간까지 왕복할 수 있도록 구성된 업무용 6개 시스템이다. 총 측정횟수는 10회이며 트랜잭션 카운트 횟수는 총 12,775건으로 집계되었다.

5단계 구조일 경우 보안 도메인은 5개 영역이지만 차단 단계는 유입 트래픽 4개 단계로 구성된다. 즉 유입 트래픽의 경우 스위칭 → 침입차단 → 게이트웨이 → 서버 단계이거나 또는 스위칭 → 침입차단 → 게이트웨이 → 클라이언트 과정으로 처리된다. 그러나 유출 트래픽일 경우에는 클라이언트 → 서버 → 게이트웨이 → 침입차단 → 스위칭으로 5개 단계를 거친다. 유출 트래픽의 경우 보안처리를 수행하지 않으므로 응답시간에 영향을 주지 않는다. 통합구조는 유입 트래픽 구간을 기준으로 설계되기 때문이다. 이 같은 환경에서 응답시간 측정 결과는 기존 구조에서 통합구조로의 증가 시간을 비율로 보면 평균 증가율은 5.75%이고 순간 최대 증가율은 10%까지 증가했다. 순간 최대 증가율이 10% 수준까지 증가한 것은 어느 일정 순간의 최대 증가치이며 측정 당시의 네트워크 구간, 서버, 클라이언트 중 시스템부하 증가 요인이 발생했던 환경에서 기인한 것으로 추정할 수 있다. 다음 표는 차단구조별 응답시간 변화를 보여주고 있다.

〈표 5〉 응답 소요 시간 분포

(단위 : 초)

측정	대상 시스템수	트랜잭션 카운트	기존 구조		통합구조	
			평균	최대	평균	최대
1	6개 시스템	1,198	3.28	7.120	3.350	7.630
2	6개 시스템	1,359	3.51	8.940	3.700	9.460
3	6개 시스템	1,183	2.496	6.350	2.630	6.570
4	6개 시스템	1,369	3.168	6.860	3.350	7.200
5	6개 시스템	1,219	3.622	6.830	3.840	6.690
6	6개 시스템	1,404	3.176	7.250	3.330	7.580
7	6개 시스템	1,352	2.554	6.230	3.730	6.550
8	6개 시스템	1,358	3.367	6.590	3.510	7.160
9	6개 시스템	1,084	3.670	6.870	3.830	7.450
10	6개 시스템	1,249	3.448	8.960	3.630	10.440
총 평균		1,277.5	3.229	7.128	3.390	7.673

설정한 측정 기준과 방법에 따른 측정 작업은 통계의 신뢰 수준을 높이기 위해 10회에 걸쳐 실시하였다. 기존 구조와 통합구조간 응답시간 차이만을 단순 비교하므로 주기별, 요일별, 시간대별 추이라던가 응답시간의 변동 추이, 시간 분포도 등은 조사하지 않았다. 조사 결과는 통합구조하에서 응답시간 평균 소요 시간은 전체적인 퍼포먼스의 6% 이상을 점유하지 않고 있다. 이 같은 결과는 시스템 퍼포먼스측면에서 5단계 차단 구조의 부담이 예상보다 높지 않음을 입증하고 있다. 게이트웨이가 개별 스테이션에서의 보안 필터링을 일괄 수행한다는 면에서 대기 시간 기준으로 경제적인 방안이 되고 있음이 입증되었다. 대기 시간 지연 원인은 많은 변수가 존재하지만 인프라 구조상에서의 추가적 필터링으로 인한 지연 가능성 또한 상존한다. 그러나 이 같은 부작용에 대해서는 네트워크 보호 차원에서 어느 정도 불가피한 현상이고 대신 네트워크 성능 및 가용성을 높이는 노력과 보안 솔루션 통합 노드 적용이 병행되어야 한다. 그리고 어떤 방법을 통해 이를 해결해야 하는가에 대한 방법론 도출은 별도의 추가적 연구를 통해서 좀더 체계적으로 규명해야 한다.

4.3.2 차단 단계별 방역 효율

차단 단계별 방역 효율성이란 통합구조에서 설정한 보안 도메인을 기준으로 차단 단계를 구성하고 방역을 시행시 각 단계의 유형별 보안 효율을 의미한다. 설정된 차단 유형은 차단 단계를 기준으로 1단계, 3단계, 5단계 경우 등 3가지 유형을 설정했다. 3가지 유형을 설정한 이유는 현재 우리나라 기업의 보안 인프라 구축 실태는 기본적 보안 인프라인 침입차단 시스템을 설치한 사례도 50% 미만으로서 기본 인프라가 미비한 상황에서 다단계 차단 구조를 적용하는 사례가 현실적이지 못하므로 차단 유형을 하향 설정한 것이다.

1단계 차단은 일반적으로 보안이 활성화되지 못한 불완전한 보안 대책으로서 스위칭, 침입차단, 서버 방역, 클라이언트 방역중 하나만을 시행한 경우이다. 3단계 차단이란 경로 차단 구조로서 스위치, 서버 방역, 클라이언트 방역의 구조를 택하거나 또는 침입차단 시스템, 서버 방역, 클라이언트 방역을 선택하는 경우이다. 5단계 차단이란 설계한 구조대로 스위치, 침입차단 시스템, 서버 방역, 클라이언트 방역망을 모두 갖춘 경우를 말한다.

(1) 1단계 차단

1단계 차단은 스위치, 침입차단 시스템, 서버 방역망, 클라이언트 방역망 중 하나만을 가동했을 경우 방역 성취도를 나타낸다. 네 가지의 경우 중 어느 경우든 5개 도메인 중 하나의 도메인만을 방역 대상으로 하고 있음으로서 나머지 4가지 도메인에 대해서는 경로 차단 기능 적용이 불가능하게 된다.

각각의 경우 차단 가능한 부분과 차단 불가능한 부분은 <표 6>과 같다. 어느 경우는 1단계 차단에 의한 방역은 방역에 치명적인 위험이 된다. 다만 국내의 많은 기업, 대학, 연구소 등에서 1단계 차단 장치인 침입차단 시스템 설치율마저 매우 저조하다는 사실은 우리나라 방역 대비가 매우 불안한 상황임을 나타내주고 있다.

(2) 3단계 차단

3단계 차단의 경우는 스위치를 기준으로 하는 3단계 차단과 침입차단 시스템을 기준으로 하는 3단계 차단 두 종류가 있다. 어느 경우든 1단계 차단보다 방역 성취도가 높지만 경로 차단을 시행치 못하는 도메인이 발생한다. 경로 차단이 미시행되는 도메인은 스위칭, 서버, 클라이언트 방역의 경우 패킷 필터링에 의한 침입차단 방역이 이루어지지 못하여 패킷의 IP주소 기준, TCP 포트 기준, TCP 프로토콜 기준의 세션 검사와 관리가 이루어지지 못하는 문제가 있다. 또 내부게이트웨이 단계에서의 방역 미시행으로 내부 경로상 유통 바이러스에 대한 대책은 서버 방역망과 클라이언트 방역망으로 대처해야 한다는 필요성이 대두된다. 한편 침입차단, 서버 방역, 클라이언트 방역 방식을 채택하는 경우 스위칭 단계의 차단이 이루어지지 못하므로 많은 웜 바이러스가 내부 네트워크에 진입하게 된다는 위험성이 있다. 이 같은 위험은 스위칭 단계 차단에서 나타난 방역 성과를 참조해보면 그 위험성이 어느 정도인지를 알 수 있다.

(3) 5단계 차단

5단계 차단 경우는 통합구조에서 구성한 보안 도메인을 모두 적용하여 방역 처리하고 있다. 5단계 차단의 경우는 구현하고자하는 차단 기능이 모두 구현될 수 있다. 1차적으로 외부 경계선에서의 침입을 레이어 7 스위칭에서 97% 이상 걸러주며 2차적으로는 패킷 필터링 과정에서 패킷 자체의 여과를 거치면서 메일 바이러스 위주의 차단이 시행된다.

만일 그 단계에서 누락된 부분이 있다하더라도 내부 게이트웨이 단계에서 내부 경로상 확산 차단을 시행하므로 안전한 도메인을 형성하고 내부에서 매체 감염으로 새로운 침입이 발생하더라도 내부 게이트웨이 방역망에서 차단이 이루어진다. 한편 서버 방역망과 클라이언트 방역망은 3개 구간의 전단계 방역 누락 부분을 다시 한번 걸러주게 되므로 방역 안전성을 최종 노드에서 보장하게 된다.

(4) 종합효율

통합구조 적용후 평균 쓰르풋타임은 5.7% 수준으로 증가했지만 프로세스 상 퍼포먼스는 30~40%의 불필요한 메일을 걸러줌으로 서버에 주는 부하는 오히려 상당량 감소되었다. 예를 들면 Sobig 바이러스가 시간당 3,000여 통씩 쏟아질 때 차단 장치에서 먼저 걸러주면서 트래픽 부하를 축소시켜 전체적으로는 별다른 영향 없이 동작할 수 있었다. 유입 패킷을 먼저 수신해 악성 트래픽과 바이러스 검사를 수행함으로 유해 트래픽 유입을 차단하고, 1차적으로 걸러진 메일을 다시 첨부 파일명, 제목, 본문, 필터링 형태로 검색함으로서 비정상적인 메일을 네트워크 전송 과정에서 차단한다. 또한 스팸메일이나 바이러스 오염 메일로 분류된 메일을 곧바로 삭제하지 않고 일정 기간 보관해 정상적인 메일이 스팸메일로 분류되는 폴스 포지티브(False Positive) 메일은 재발송이 가능하여 필터링으로 인한 중요 메일 유실 문제 해결이 가능하다.

이상의 차단 결과와 레이턴시소요 시간 조사 결과를 토대로 하여 차단 유형별로 종합적인 방역 효율을 분석했다. 효율 분석은 1단계 차단, 3단계 차단, 5단계 차단 유형별로 차단 효과와 레이턴시를 각각 분석하고 그 결과를 종합 효율로서 평가하는 것이다. 이상적인 차단 구조 모델은 차단율은 높을수록 유리하고 레이턴시는 낮을수록 유리하다. 따라서 크게 세 가지 유형과 세부적으로는 일곱가지 차단 경우의 수별로 차단율과 레이턴시를 모두 감안했을 때 가장 이상적인 모델을 찾아보는 것이다. 1단계 차단의 경우는 1개 도메인의 방역만 가능하고 나머지 4개 도메인의 방역은 불가하다. 차단 단계가 다단계일수록 방역율은 높고 레이턴시는 증가한다. 다음 표는 차단 유형별 방역 효율 종합 분석 결과를 보여주고 있다.

〈표 6〉 차단 유형별 방역 효율 종합 평가표

차단 유형		차단 장치	방역 도메인		응답시간 지연(%)
			차단	미차단	
1단계 차단		스위칭	1	4개 영역 (80%)	평균 0% 최대 0%
		침입차단 시스템 필터링	1		
		서버 방역	1		
		클라이언트 방역	1		
3단계 차단	스위칭 기반	스위칭	1	2개 영역 (40%)	평균 2.875% 최대 3.06%
		서버 방역	1		
		클라이언트 방역	1		
		소계	3		
	침입 차단 시스템 필터링 기반	침입차단 시스템 필터링	1	2개 영역 (40%)	평균 2.875% 최대 3.06%
		서버 방역	1		
		클라이언트 방역	1		
		소계	3		
5단계 차단		스위칭	1	없음	평균 5.75% 미만 최대 7.65% 미만
		침입차단 시스템 필터링	1		
		내부 게이트웨이 방역	1		
		서버 방역	1		
		클라이언트 방역	1		
		소계	5		

종합 효율을 분석해보면 5단계 차단 구조 적용 시 전체적인 퍼포먼스에 큰 지장을 초래하지 않고 차단 기능이 수행된다. 즉 퍼포먼스지연은 1단계 차단, 3단계 차단에서 미미한 정도이며 5단계 차단에서도 두드러지게 나타나지 않았다. 적어도 5단계 차단 구조까지는 퍼포먼스영향을 걱정하지 않아도 된다. 차단의 완전성은 1단계보다 3단계, 3단계보다 5단계 차단이 절대 유리하다. 5단계 차단에서는 전방위의 존으로 차단 영역이 확대됨으로서 차세대형 차단 구조로서 가장 강력한 방역 기능 실현이 가능하다. 결론적으로 차단 단계를 추가시 일정단계까지는 퍼포먼스에는 업무 불편을 초래할 만큼의 지연이 발생치 않는다. 이 같은 분석 결과는 퍼포먼스부담으로 인하여 다단계 차단 구조를 적용하기가 어려울 것이라는 일반적인 우려에 대해 시사점을 주는 것으로서 향후 현장 보안시스템 구축시 참고되어야 할 사항이다.

5. 결 론

현재 인트라넷 시스템 운용 현장에서는 갈수록 빨라지는 바이러스 침투 시간, 침투한 웜 바이러스의 급속한 내부 네트워크 재감염, 다수 서버와 클라이언트 차원에 대한 개별 방역 처리 시간의 과다 소요 등 사용하고 있는 방어 메커니즘으로는 극복하기 어려운 문제점들이 노출되고 있다. 본 논문에서는 이러한 문제점을 해결하고 보다 강력한 방어를 수행하기 위하여 통합구조의 정보보호 인프라스트럭처를 제안했다. 제안 인프라스트럭처는 새로운 설계사상을 기반으로 하여 프레임워크를 도출하고 기능 메커니즘을 구성했으며, 기반 구조도를 설계했다. 통합구조 인프라스트럭처는 다원화 차단, 다단계 차단, 차별화 차단을 실행하는 구조이다. 본 논문에서는 제안된 방법론에 대하여 성능분석 모델을 개발하고 사례연구를 통하여 성능분석 및 검증을 실시했다. 정보보호 인프라스트럭처의 효율성 여부는 사용자 또는 사용부서의 지속적인 진단과 튜닝을 필요로 한다. 본 논문으로 제안된 방법론은 향후 업무 현장에서 참고 되고 응용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] Andrew Cook, "Building High Performance Firewall and Security Infrastructure", Nortel Networks, 2002.

[2] CCIMB, "Common Methodology for Information Technology Security Evaluation,

Part1 ~ Part3. Version2.1", 1999.

[3] CCIMB, "Common Methodology for Information Technology Security Evaluation, Part2, Version1.0", 1999.

[4] C. Edward Chow, "Introduction to Content Switch", University of Colorado, 2000.

[5] CIAO/VAF, "Vulnerability Assessment Framework 1.1", Critical Infrastructure Assurance Office(CIAO), 1999. 10.

[6] David Baer, "Towards Compatibility with Firewall and Keyword search", Distributed Computing Group, 2002.

[7] David Harley, "Virus Bible", Kyohaksa, 2004.

[8] David Harley, "Virus Revealed", Kyohaksa, 2002.

[9] David Mitchell and Katherine Carr, "Best Practice for Multi-tier Virus Rrotection", Oxford University, 2002.

[10] Department of Defense Computer Security Center, "Department of Defense Trusted Computer System Evaluation Criteria", August 1983.

[11] D. Peeples, "The Foundations of Risk Management", 20'th National Information Security Conference, 1990. 10.

[12] Dr. Thomas W. Shinder, Debra Littleejohn Shinder, "ISA Server 2000", Syngress Media, 2001.

[13] E. Amosoro, "Fundamentals of Computer Security Architecture, Design, Depolyment & Operations", Osbourne/McGraw-Hill, 2001.

[14] Edward J. Rhode, "An Introduction to Load Balancing with planet Application Server", Soun Developer Network, 2000.

[15] Emily Gladstone, "Sans GCFW Practical Assignment(V 1.6)", Glac Enterprise, 2002.

[16] E. Zwicky, S. Cooper, and D. Chapman, "Building Internet Firewalls", O'reilly, 2000.

노 시 춘

2000년 고려대학교 경영학과 (경영학석사)

2005년 경기대학교 정보보호 기술공학(공학박사)

2006년 ~ 현재 남서울대학교 컴퓨터학과 교수