# 네트워크 경로상에서의 정보보호기능 연동 메커니즘 구현 연구

노시춘 · 송은지
남서울대학교 컴퓨터학과

# A Securing Method of Relational Mechanism Between Security Technologies on Network Ruote

Sichoon Noh · Eunjee Song
Dept of Computer Science, Namseoul University
E-mail : nsc321@nsu.ac.kr

요 약

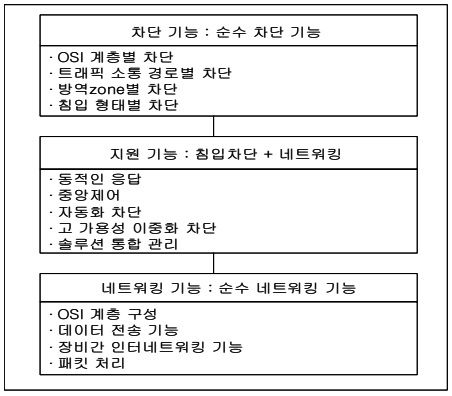
네트워크보안에서 네트워킹기능과 정보보호기능을 분리하여 관리하지 않고 연계하여 종합 메커니즘을 구성 및 적용할 경우 종합적인 정보보호 효율은 시너지효과로 나타난다. 본 연구는 네트워킹 기능과 정보보호기능을 연계하여 정보보호기능을 적용했을 경우의 연동메커니즘 구현방법을 제안하기 위한 것이다. 연동 메커니즘에 의한 보안차단성과는 분리상황의 성과보다 증대되어 나타나므로 네트워크 인프라상에서의 정보보호기능 구현은 반드시 네트워킹기능과 정보보호기능을 연계하여 구성하고 그 성과를 측정, 관리하는 것이 정보보호 성과 관리에 효율적 방법임을 본 연구를 통해 제시하고자 한다.

## 1.서 론

정보보호기능 연동이란 네트워크트래픽 처리과정에서 전단계 네트워크 도메인 차단 시 방역 누락되는 누수 바이러스를 다음 단계 도메인에서 차단하고 이 같은 방역 누락을 다음 단계 도메인에서 차단해주는 기능 매커니즘을 말한다. 방역 누락은 방역 도메인별로 각기 다른 상황에서 발생된다. 각 도메인 상에서 단 한건의 감염도 전체 도메인으로 확산된다. 따라서 각 도메인마다 차단 기능이 구현되고 차단 기능은 도메인 간 연동되어야 한다.

## 2. 설계방향

종합 매커니즘 구조는 [그림 1]과같이 네트워킹기능, 지원기능, 정보보호기능 3단계로 계층화된다. 네트워킹기능은 네트워크 인프라상의 통신트래픽 처리 기능이다. 네트워킹 기능은 OSI 7 layer별로 차별화된 네트워킹 기능 구조를 형성하고 이 구조상에서 라우팅, 스위칭, 브로드캐스팅 등 인터네트워킹 기능, 데이터 전송기능 그리고 패킷처리 기능을 수행한다. 다이어그램으로 본다면 이 네트워킹 기능 영역 내에 지원기능과 침입차단 기능이 존재한다.




[그림 1] 연동기능 종합메커니즘

## 3. 종합메커니즘 설계

### 3.1 스위칭과정 연동

1) 컨텐츠 스위칭(Contents Switching)

단위 네트워크 그룹에 유입되는 트래픽은 내부 외부 경계선에 위치한 외부 라우터( Exterior Router)를 통해 경로 배정과 포워딩이 이루어진 다음 최초로 스위칭 단계로 유입된다. 스위칭 단계에서는 네트워킹기능, 보안기능이 수행되고 더불어 효율성 기능이 구현된다. 스위칭기능은 L2에서 L7까지 수행된다. L2 - L3까지의 기능은 일반적인 네트워킹 처리 과정의 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 방역기능은 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 스위칭되기 때문이다.

2) 유입 트래픽의 스위칭 연동

외부 라우터(Exterior Router) 이후 침입차단시스템 전단에 스위칭을 구성한다. 스위칭 목적은 전통적 기능인 부하 분산(Load Balancing) 기능 외에 컨텐츠 인식 기능을 갖는 Layer7 스위칭을 수행하기 위해서 이다. 이 기능을 통해서 컨텐츠 기반 패킷 필터링과 앤티바이러스 기능, 응용 레벨의 미러링(Mirroring)을 수행한다. 컨텐츠기반 패킷필터링 기능은 앤티바이러스 기능의 근간이 된다. 최근 기승을 부리는 님다, 코드레드, 마이둠 등 바이러스는 기존의 침입차단시스템 기능만으로는 해결하기 어렵고 스위치 단계에서 강력한 패킷 처리 능력과 인지 능력을 통해 보안 기능을 제공한다.

3) URL 분리(URL Partitioning) 연동

L7 스위칭을 도입함으로서 URL기반으로 웹 서버를 분리해 웹 서비스가 가능하게 된다. 특정 URL에 대해 특정 웹 서버가 처리할 수 있도록 L7 스위칭을 사용하는 것이다. 동적으로 변경되는 페이지는 서버1 웹 서버에 저장하고 정적인 html 텍스트나 이미지 등은 서버2에 저장해 웹 서버 관리를 효율적으로 할 수 있다. 이렇게 특성이 다른 웹 페이지를 별도로 관리하고 웹 서버에 특성을 조절함으로서 최대의 성능을 낼 수 있다. 이러한 기능은 특히 캐쉬 서버(Cash Server)의 Redirection이나 침입탐지 시스템(IDS:Intrusion Detection System) 서버의 로드 밸런싱을 수행할 경우에 매우 효과적으로 웹 서버의 성능을 극대화하는 방법을 제공한다.

4)바이러스필터링연동

NBAR(Network-BasedApplicationRecognition) 기능인 QoS(Quality ofervice)의 큐잉(Queuing) 방법 중에 CBWFQ(Class-based Weighted Fair Queuing)기능이 있다. CBWFQ는 특정 기준에 의해 트래픽을 분류(Class-map)하고 분류한 트래픽에 대해 하나 혹은 그 이상의 정책을 적용(Policy-map)하고 라우터의 인터페이스에 Policy-map을 적용한다. 따라서 Class-map을 어떻게 분류하는지 Policy-map을 어떻게 적용하는지, 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 등과 같이 다양한 애플리케이션을 인식할 수 있는 분류 엔진(Classification Engine)이다.

### 3.2 침입차단 필터링 연동

광범위하게 바이러스를 진단하고 보다 정교한 수준의 필터링 기능을 수행하기 위해서는 패킷 타입을 조사하고 분석 작업을 수행할 수 있어야 한다. 이러한 기능은 일반적으로 프록시(Proxy)나 애플리케이션 서비스 (Application Service)로 제공된다. 프록시 서버는 클라이언트와 원격의 애플리케이션 서버 사이에 삽입된다. 그러나 이러한 침입차단시스템은 필터링과 프록시 서비스 모두 유지 가능하다. 일반적으로 침입차단시스템은 서비스(www, 텔넷, FTP, Mail 등)를 제공하는 네트워크

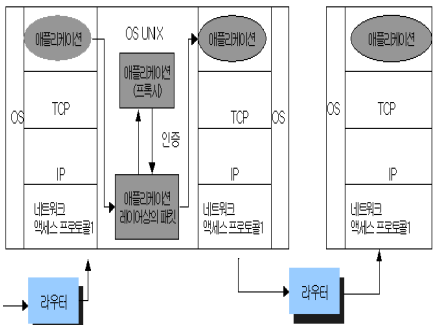
환경에서 해당 서비스를 요청한 호스트의 주소와 포트번호 그리고 사용자 인증 등의 기능을 기반으로 통제하게 된다.

1) 프록시 서버(Proxy Server) 기능연동

프록시 기능을 이용하는 침입차단시스템은 애플리케이션 침입차단시스템과 서킷 게이트웨이 침입차단시스템이 있다. 프록시 서버 동작 과정은 클라이언트가 침입차단시스템으로 접속을 요구하면 침입차단시스템상의 프록시 서버는 접속 허용 규칙을 이용하여 클라이언트의 접속 여부를 결정한다. 프록시는 클라이언트로 접속 요청에 대한 응답을 보내어 클라이언트와 프록시 서버간의 연결을 맺는다. 이렇게 연결이 설정된 프록시는 클라이언트와 서버 사이에서 전달자 역할을 수행하게 된다. 프록시 침입차단시스템은 바이러스 스캐너(양쪽 프로그램의 타입은 기본적으로 필터)와 같은 기능을 수행한다. 그러나 침입차단시스템에 의해서 이루어지는 분석은 입력 스트림을 바이트 단위로 읽는 스캐너가 하는 것과 같지는 않다.

2) 애플리케이션 레이어 트래픽 분석과 차단기능 연동

프록시 서버에서는 패킷 필터링을 통과한 패킷에 대해 Store-and-forward 트래픽 뿐 만 아니라 쌍방향 트래픽을 처리하게 되며 이때 애플리케이션 레이어에서 트래픽을 분석할 수 있도록 프로그램이 된다. 따라서 사용자 단계와 응용 프로토콜 단계에서 액세스 제어를 제공할 수 있고 응용 프로그램의 사용에 대한 기록을 통해 감사 추적(Audit)을 할 수 있게 된다. 응용 게이트웨이는 사용자 단계에서 유입 유출 모든 트래픽에 대한 기록을 관리하고 제어할 수 있게 되며 인증을 받지 못한 사용자를 위해서는 별도의 인증 기법이 필요하게 된다.




[그림2] 응용 게이트웨이에서의 처리 과정

### 3.3 내부 게이트웨이 레벨기능 연동

바이러스 감염으로부터 데이터를 보호하기 위해서는 바이러스가 네트워크 상 핵심 중요 정보에 도달하기 전에 실시하는데 웹 트래픽과 SMTP 트래픽을 대상으로 한다. 게이트웨이 방역의 기본 기능은 필터링 기능이다. 게이트웨이에서 적용할 수 있는 필터링 종류는 바이러스 필터링, 컨텐츠 필터링, 이메일 필터링, 파일 필터링, 스팸 필터링 등으로 구분할 수 있다. 바이러스 필터링은 패킷 단위로 바이러스 감염 여부를 점검 삭제하며 컨텐츠 필터링은 이메일의 제목과 본문내용에서 특정 키워드가 발견되는 경우 이를 차단하는 기능이다.

## 4. 결 론

모든 네트워크 도메인 상에는 전 단계 도메인으로부터 발생되는 방역 누락 요소와 당해 도메인 상에서의 직접 감염 등 두 가지 유입 유형의 감염이 발생한다. 내부 게이트웨이는 내부 도메인 진입로 초기에서 악성코드 접속을 차단한다. 연동 메커니즘에 의한 보안차단성과는 분리상황의 성과보다 증대되어 나타난다. 네트워크 정보보호기능 구현은 반드시 네트워킹기능과 정보보호기능을 연계하여 구성하고 그 성과를 측정, 관리하는 것이 필요하다. 본 연구를 통해 제시된 네트워크 경로상에서의 정보보호기능 연동 메커니즘 구현은 네트워크 보안 인프라를 설계하는 산업현장에서 적용할 수 있을 것으로 기대한다.

## 참고 문헌

[1] 김귀남, 노시춘, "다단계 바이러스 차단 구조 설계", 2004 한국 사이버테러 정보전 컨퍼런스, 2004.

[2] P.Denning, "Computer Under Attack Intruders, Worms and Virus", ddison Wesley, 1990.

[3] F.Cohen, "A short Course on Computer Viruses", ASP Press, 1990.

[4] 한명국, "바이러스의 동작 원리 및 대응", (주) 하우리, 2003.

[5] 최의인, "악성코드의 분류 및 탐지 기법", 한남대학교, 2003.

[6] Lan Browde and Camille Smith, "Virus Protection", In De Sense, Inc, 1999.

[7] Rainer Link, "Server-Based Virus rotection on Unix/Linux", University of Applied Science Furtwamgan, Germany, 2003.