방화벽기반 통합 멀티코어 DLP(정보유출방지) 시스템 개발

조현규, 신동진, 한승철*
*㈜엔피코어
e-mail : hgcho1@npcore.com, hansc1@npcore.com

A Development of the Multicore DLP System based on Firewall

Hyun-Kyu Cho, Dong-Jin Shin, Seung-Chul Han*
*NPCore , Inc.

요약

본 제품은 RFC(Recursive Flow Classification) 알고리듬의 네트워크 접근제어를 구현한 방화벽 기반의 정보유출방지 솔루션이다. 네트워크 단에서의 정보유출은 대부분 이메일, 메신저, 웹하드, P2P 등을 통해 이루어진다. 따라서 본 제품은 업로드 트래픽의 크기를 제한하고 사용자가 송수신하는 모든 메일을 필터링하여 저장한다. 웹상에서는 정보유출 가능성이 있는 URL을 등록, 사용을 제한하는 기능을 통하여 네트워크를 통한 정보유출의 가능성을 원천적으로 차단한다. 동시에 사용자 중심의 인터페이스와 성능이 뛰어나면서도 저렴한 통합 플랫폼을 제공함으로써 중소기업환경에 최적화된 네트워크 정보보안의 대안을 제시한다.

1. 서론

경찰에 따르면, 2010년 경찰이 적발한 산업기술 유출사건은 40건, 피해액은 9조 2000억원에 달한다. 또 지난해 국정감사에서는 2004년부터 2009년까지 국내 산업기술의 유출 시도가 203건 발생해 235조원의 막대한 피해추정액이 발생한 것이 지적되었다. 특히 대기업에 비해 보안이 취약한 중소기업에서의 정보유출이 많아 국가정보원은 중소기업의 산업기밀 유출이 지난 2003년 2건에서 2009년 29건으로 10배 이상 급증했다는 결과를 발표했다. 또 중소기업청은 기술유출 기업의 건당 피해액이 평균 10억 2000만원에 이른다는 집계자료를 발표하기도 했다. 그럼에도 불구하고 기술력에 비해 자금여력이 많지 않은 중소기업들은 고가의 기존 DLP 솔루션을 도입하는데 부담이 큰 것이 사실이다. 본 제품은 이러한 상황을 감안하여 중소기업환경에 적합하면서도 뛰어난 네트워크 정보유출방지 기능을 가지도록 설계되었다.

2. 주요기능과 특징

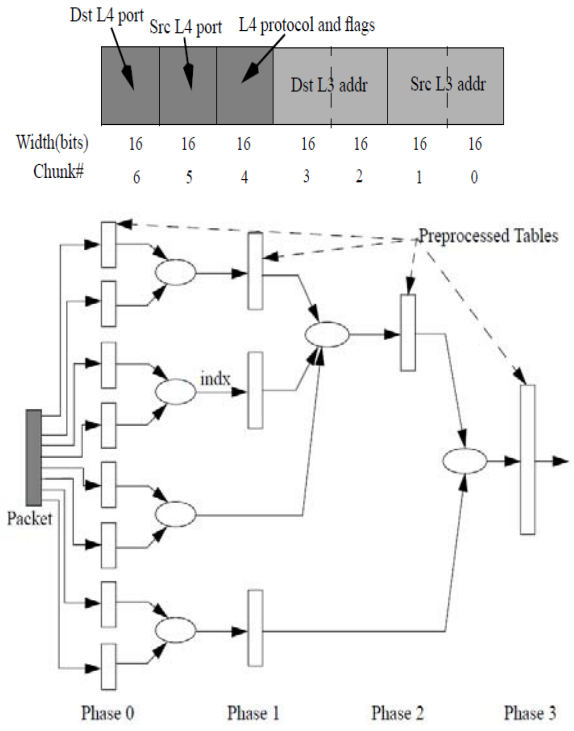
2.1 네트워크 DLP

DLP 솔루션은 동작방식에 따라 네트워크 DLP, 엔드포인트 DLP, 서버 DLP의 세 가지로 분류할 수 있다. 네트워크 DLP는 게이트웨이 단에서 외부로 전송되는 데이터를 감시하며, 중요 데이터가 포함될 경우 트래픽을 차단한다. 엔드포인트 DLP는 개별 사용자단에서 네트워크 외부 혹은 PC 외부로 이동되는 데이터를 감시한다. 구축과 함께 PC등 개인이 사용하는 기기에 저장된 중요 데이터를 찾아 보안정책에 따라 관리한다. 서버 DLP는 중요 데이터가 저장된 서버 혹은 Storage 단에서 데이터의 상태를 모니터링한다. 본 제품은 네트워크 DLP이며 방화벽으로 기능함과 동시에 모든 이메일을 필터링하고, 등록된 URL로의 접속을 차단하며 네트워크를 통과하는 업로드 트래픽이 지정된 용량을 초과할 경우 차단하는 기능을 갖추고 있다.

2.2 네트워크 접근제어

본 제품의 접근제어는 RFC(Recursive Flow Classification) 알고리듬을 기반으로 구현되었다. RFC 알고리듬은 패킷을 프로토콜, 목적주소와 목적포트, 출발주소와 출발포트 필드로 분류하고 사전처리를 통해서 해쉬맵을 만들어 둔 다음, 패킷이 들어왔을 때 항상 동일한 비교에 의해 패킷을 분류하는 고속처리 알고리듬이다. RFC의 가장 큰 특징은 ACL 목록이 수 만개에 이를 정도로 증가했을 때에도 그보다 적은 수의 목록이 있을 때와 동일한 처리속도를 제공한다는 점이다. 따라서 본 제품은 Quad-Core 하드웨어 플랫폼과 RFC 알고리듬을 사용하여 여러 통합 기능을 제공하면서도 100Mbps

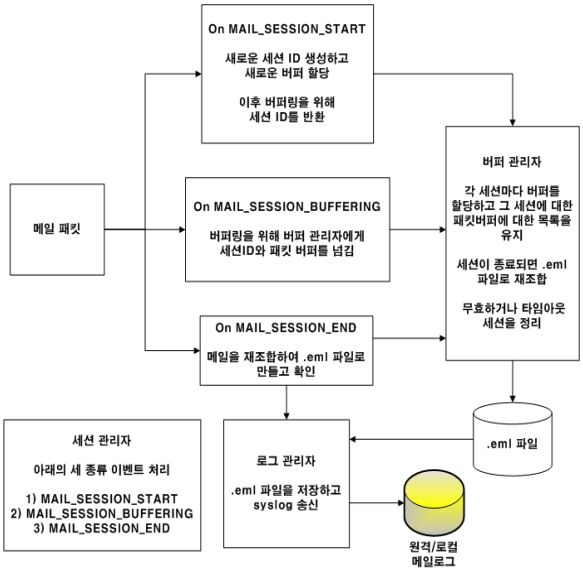
의 성능을 보장한다.



(그림 1) Recursive Flow Classification: 다중 필드 패킷 분류 알고리듬

2.3 메일 필터링

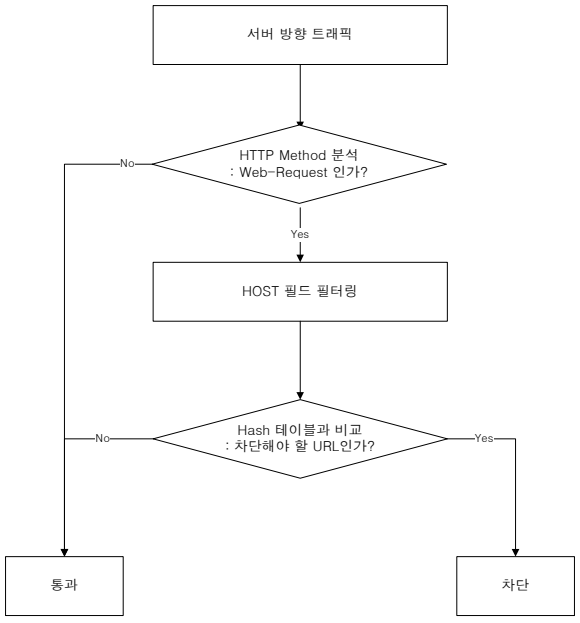
네트워크를 통과하는 패킷 중에서 SMTP 프로토콜을 사용하는 패킷을 따로 수집하여 세션을 만들고 재조합의 과정을 거치면 eml파일을 생성할 수 있다. 이 eml 파일은 실제로 보내는 이메일과 같은 것이며 Microsoft의 Outlook으로 열어서 확인할 수 있다. 본 제품의 메일 필터링 과정은 다음과 같다.



(그림 2) 메일 필터링 알고리듬

2.4 URL 필터링

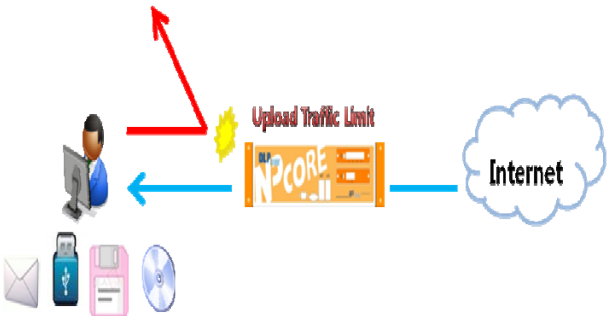
네트워크 내부 사용자가 외부 URL에 접속을 시도할 때 HTTP는 GET이나 POST 메서드를 사용하며 해당 URL 정보는 패킷의 payload에 HOST 필드로 저장되어 있다. 따라서 HOST 필드를 필터링하여 미리 저장된 차단대상 URL과 비교하면 특정 URL을 차단할 수 있다. 본 제품은 URL 비교 프로세스에 해쉬 테이블을 사용, 처리속도를 향상시켰다.



(그림 3) URL 필터링 Process

2.5 업로드 트래픽 제한

본 제품은 네트워크 내부 사용자(클라이언트)와 외부 서버 간 세션을 저장하고 감시한다. 클라이언트가 외부 서버로부터 정보를 요청하는 경우(업로드) 통상적으로는 동일 세션에서 많은 데이터를 보내지 않는다. 그러나 일반적인 용량 이상의 데이터를 보낸다면 파일 업로드로 판단할 수 있으며, 이러한 특성을 이용하면 이메일의 파일첨부, 웹하드, P2P 등을 통해 중요 데이터가 담긴 파일이 유출되는 것을 사전에 방지할 수 있다.



(그림 4) 업로드 트래픽 제한 모식도

2.6 통합 플랫폼

본 제품은 위에서 언급된 네트워크 접근제어, 메일 필터링, URL 필터링, 업로드 트래픽 제한 외에 방화벽의 기본기능인 라우팅, 주소변환, 포트포워딩 기능을 갖추도록 개발되었다. 여기에 모든 기능에 대한 정책을 설정하고 보안사항을 모니터링할 수 있는 ESM 웹서버를 기본 탑재하고 있어서 네트워크 관리자뿐 아니라 비전문가가 관리하기에도 용이한 통합플랫폼이다.

3. 결론

뛰어난 기술력을 보유하고 있는 기업의 경우 기술유출을 방지하기 위해 여러 대책을 마련해야 한다. 인원보안과 시설보안은 물론이고 이메일, 웹하드 각종 P2P 사이트 또는 메신저 등 인터넷을 통한 정보유출에도 만전을 기해야 한다. 본 장비는 기본 방화벽 기능 외에 메일 필터링, URL 필터링, 업로드 트래픽 제한 기능을 갖추고 있으므로 사내 네트워크에서 외부로 향하는 모든 트래픽을 감시하고 제어할 수 있다. 특히 고가의 네트워크 장비를 여럿 구매하여 설치하기 어려운 기업에 적합하도록 설계, 제작된 All-in-One 제품이므로 중소기업에 특화된 네트워크 보안 및 정보유출 방지 제품이라 할 수 있다.

본 개발은 중소기업청의 “산업보안기술개발사업”의 지원을 통해 수행되었다.

참고문헌

[1] Pankaj Gupta, ALGORITHMS FOR ROUTING LOOKUPS AND PACKET CLASSFICATION, 2001
[2] Pankaj Gupta and Nick Mckeown, Algorithms for Packet Classification, 2001
[3] 이진석, 다중필드 패킷분류 알고리듬의 효율적 구현, 경북대학교, 2002
[4] 月刊 NETWORK TIMES & DataNet, 기업정보보호가이드 V.6, 2011.2
[5] 月刊 NETWORK TIMES, 2011.3
[6] Charles M. Kozierok, TCP/IP 완벽가이드, 에이콘, 2007
[7] Douglas E. Cormer, TCP/IP 인터네트워킹, 피어슨에듀케이션코리아, 2005
[8] 정상목, 한병래, 송기상 공저, 전자메일의 이해와 Windows Mail Server 구축, 경성문화출판, 2005