



네트워크상에서 오픈 콘텐츠 검사로 유해 트래픽 '척척' 차단

네트워크 애플리케이션 성능에 영향 없어...
딥 패킷 인스펙션 한계 극복



이종열
포타넷 코리아 부장
(jeo@fortinet.com)

네트워크 위협은 비교적 단순한 네트워크 연결을 통한 공격에서 출발해 바이러스, 웜, 트로이목마와 같은 복합적인 콘텐츠 기반 공격으로 발전해왔으며, 반면 기업들은 생산성을 저해하고 실질적인 법적 책임을 초래하는 스팸 메일과 부적합한 웹 콘텐츠 등의 콘텐츠 기반 공격에 맞서 대응하고 있다. 이러한 새로운 콘텐츠 기반의 공격은 많은 기업들이 이미 구축하고 있는 스테이트풀 인스펙션(Stateful Inspection) 방화벽으로는 감지 또는 차단되지 않아 보다 새롭고 효과적인 기술 개발이 요구되고 있다. <편집자>

최 근 많은 방화벽 공급업체들이 콘텐츠 기반 공격에 대해 우수한 보호 기능을 제공하는 딥 패킷 인스펙션(Deep Packet Inspection) 기술이 갖는 이점에 주목하고 있다. 딥 패킷 인스펙션은 특정 공격 유형에 대해서는 스테이트풀 인스펙션보다 더 효과적이지만 네트워크 및 컴퓨팅 시스템 보호를 위한 완벽한 솔루션으로 보기에는 부족한 점이 많다. 특히 딥 패킷 인스펙션은 현재 활동중인 트로이목마를 비롯한 바이러스, 웜 중 상당 부분을 검색하지 못할 뿐만 아니라 유해한 웹 콘텐츠나 스팸 메일 처리에는 전혀 효과를 나타내지 못한다. 딥 패킷 인스펙션 기술보다 더욱 효과적으로 유해 콘텐츠를 검사하는 컴플릿 콘텐츠 인스펙션(Complete Content Inspection)은 네트워크 상에서 모든 콘텐츠 공격을 검사함으로써 유해 트래픽이 데스크톱 및 랩톱, 서버 등에 도달하지 못하도록 차단한다.

또한 컴플릿 콘텐츠 인스펙션 기술은 적절한 하드웨어 기반의 플랫폼 환경을 통해 네트워크 애플리케이션 성능에 영향을 주지 않는 완벽한 고속 네트워크를 구현할 수 있다. 지금부터 스테이트풀 인스펙션과 딥 패킷 인스펙션 기술의 특성과 한계를 살펴보고 포괄적 네트워크 보안 기능을 제공하는 컴플릿 콘텐츠 인스펙션 기술이 갖는 이점에 대해 알아보자.

네트워크 위협의 발전 단계

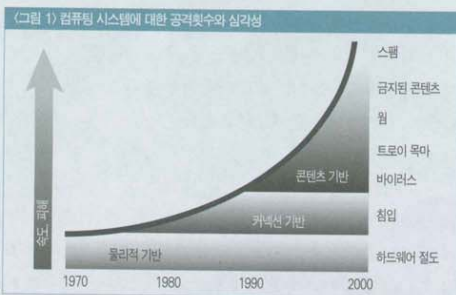
기업이나 조직들은 자사의 성공과 운영에 필요한 정보 자산 및 지적 재산이 갖는 엄청난 가치를 깨닫기 시작했다. 예를 들면, 지난 2003년 CSI/FBI CSI/FBI 컴퓨터 크레임과 시큐리티 서베이(Computer Crime and Security Survey)의 정부기관, 금융기관, 의료기관 및 대학의 컴퓨터 보안 담당자 530명을 대상으로 실시한 조사 결과에 따르면 2003년 한해 동안 미국에서 발생한 도난 당한 정보 자산의 규모는 총 800조원이 넘는 것으로 추산되어 기관당 평균 약 31조원의 손실을 입은 것으로 조사됐다.

공용 및 시설 네트워크의 확대와 네트워크 프로토콜 및 애플리케이션의 복

잠성 증가로 <그림 1>에서처럼 컴퓨팅 시스템에 대한 공격 횟수와 심각성이 급격히 증가하고 있다.

비교적 단순한 텔넷, RPC, FTP와 같은 초기 네트워크 프로토콜은 해커가 공격을 실행하기 위해선 전용선을 통해 원격 시스템에 연결된 상태에서만 가능했다. 이러한 유형에서 발생된 최초의 해킹 사건은 군 기관에 침입해 기밀 정보를 빼내려 한 것이었다. 이 같은 공격에 대응하기 위해 개발된 기술이 바로 접속 중심의 보안 시스템인 스테이트풀 인스펙션(Stateful Inspection) 방화벽이다. 이것은 송신자와 수신자의 신원을 근거로 원격 접속을 선택적으로 허용하거나 거부함으로써 컴퓨팅 리소스에 대한 접속을 통제하는 방식이다.

지난 10년 동안 애플리케이션은 훨씬 더 복잡해졌고 더욱 풍부해진 콘텐츠를 전송하기 위해 프로토콜이 사용됐다. 해커들은 이러한 변화를 이용해 접속 중심적인 보안을 피해 자동적으로 재생성 및 전파 능력을 가진 보다 효과적인 콘텐츠 기반 공격 방식을 개발했다. 콘텐츠 기반 공격은 기본적으로 인증된 접속을 통해 시도되기 때문에 접속 중심의 스테이트풀 인스펙션 방화벽을 피해갈 수 있다. 이러한 공격에는 바이러스, 트로이목마, 웜, 금지된 콘텐츠 및 스팸 등이 포함되며, 이메일이나 웹 페이지 또는 기타 실시간 통신 애플리케이션을 통해 쉽게 전파된다.



콘텐츠 기반 공격의 전파 속도와 파괴력은 상당한 영향력을 가지고 있다. 일례로 최근 북미 지역에서 월요일에 발생한 이메일 바이러스인 마이둠(MyDoom)은 단 이틀 뒤인 수요일까지 전세계 이메일 트래픽의 30% 가량을 감염시켰다. 씨넷의 지난 1월 자료에 따르면 이 바이러스는 이틀 동안 340만개 정도가 복사되어 전 세계에 전파되었다고 하는데, 이것은 12개 이메일 중 하나가 마이둠 바이러스인 셈이다.

딥 패킷 인스펙션 개선의 필요성

위에서 언급한 것처럼 대부분의 방화벽은 네트워크 레이어에서 추적하는 스테이트풀 인스펙션 기술을 사용해 방화벽의 모든 인터페이스를 통과하는 각 접속에 대한 정당성(Validity)을 확인한다. 패킷 분석을 기반으로 누구에게 내부 네트워크 컴퓨팅 시스템에 대한 접속 권한을 허용할 것인지, 아니면 정보 교환에 어떤 프로토콜을 사용할 것인지에 대한 네트워크 관리자의 정책에 따라 결정하는 것이다. 이러한 필터링 방법도 유용하지만, 이메일 메시지가 바이러스에 감염됐는지의 여부를 판단하는 데는 적합하지 않다. 왜냐하면 스테이트풀 인스펙션은 패킷에 있는 실제 콘텐츠가 유해 콘텐츠인지 혹은 유효 콘텐츠인지를 확인할 수 없기 때문이다.

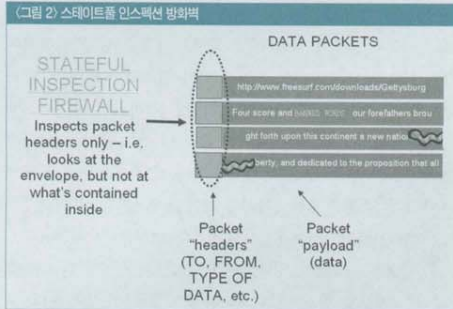
<그림 2>에서 보듯 스테이트풀 인스펙션은 발신자와 수신자의 주소, 프로토콜 유형, 패킷 페이로드에 포함된 데이터와 같은 정보를 담고 있는 데이터 패킷 헤더만 검사한다. 이러한 방법은 편지봉투 겉면에 적힌 주소만 가지고 편지 내용을 판단하려는 것과 같은 것으로, 패킷 페이로드의 콘텐츠는 검사하지 않는다.

결과적으로 스테이트풀 인스펙션 기술은 ISP의 이메일 서버나 공식 웹사이트와 같이 인증된 소스에서 발신되는 데이터가 적합한 것인지 혹은 유해한 것인지는 구별하지 못한다. 따라서 스테이트풀 인스펙션 기술은 단순 침입이나 기타 접속 기반 공격에 대해서만 효과가 있을 뿐이다.

스테이트풀 인스펙션 기술이 갖는 이러한 한계를 극복하기 위해 딥 패킷 인스펙션(DPI) 기술이 개발됐다. DPI는 스테이트풀 인스펙션 기술을 뛰어넘어 페이로드, 즉 패킷의 헤더뿐만 아니라 내용까지 검사한다. 공격이 소수 패킷에만 들어 있을 경우 DPI는 이를 효과적으로 검색하고 차단할 수 있으며, 단일 패킷에 포함되어 있는 버퍼 오버플로우(buffer overflow) 공격, 서비스 거부(DoS) 공격, 정밀 침입, 일부 웜 등의 공격에도 효과적이다.

하지만 DPI 기술의 중요한 한계는 일반적으로 인터넷을 통해 전송되는 대량 패킷에 포함된 위협을 찾아내지 못한다는 점이다. 일반적으로 단일 인터넷 패킷으로 전송 가능한 페이로드의 최대 길이는 약 1천500바이트이다. 대부분의 바이러스와 웜은 크기가 수십 킬로바이트이고, 수백 혹은 수천 패킷으로 구성되는 수백만 바이트 길이의 파일(문서, 프로그램 등)에 숨겨져(embedded) 있기도 하다. 따라서 한번에 소수의 패킷만 검사하는 콘텐츠 분석방법으로 모든 바이러스와 웜을 검색할 가능성은 매우 낮을 수밖에 없다. 이것은 마치 테러리스트가 미사일을 500개의 작은 부품으로 분리한

후 각 부품을 자동차 부품과 함께 포장해 발송하는 것과 같다. 각 포장품을 해체해 개별적으로 검사하더라도 각각의 부품이 미사일 부품으로 판명되지는 않는다. 따라서 미사일이 검색되지 않고 그대로 통과될 가능성이 높은 것과 같은 것이다.



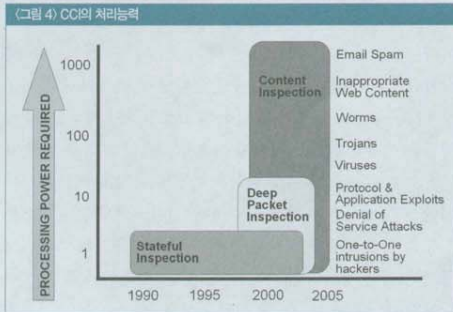
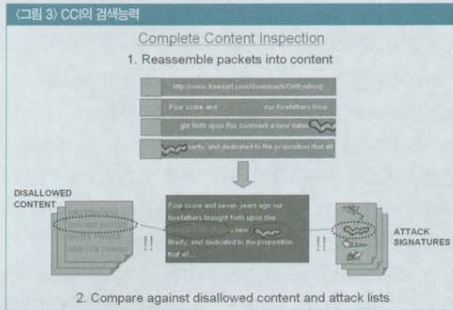
컴플릿 콘텐츠 인스펙션: 보다 향상된 접근 방법

DPI의 한계는 보다 정밀한 컴플릿 콘텐츠 인스펙션(CCI) 네트워크 보안 기술로 해결할 수 있다. CCI의 핵심은 패킷 페이로드를 파일, 문서, 프로그램과 같은 애플리케이션 수준의 개체로 재결합한 후 해당 개체를 분석해 콘텐츠 기반 공격을 검사하는 것이다. 콘텐츠 재결합 기술을 이용하면 용량이 큰 파일에 숨어있는 바이러스와 웜 같은 주요 위협을 확실히 예방할 수 있다. <그림 4>에서 보듯이 CCI 기술은 바이러스의 길이나 이를 전송하는데 사용되는 호스트 파일의 길이에 상관없이 바이러스, 웜, 트로이목마, 유해 웹 콘텐츠, 스팸 메일 등의 모든 위협을 검색할 수 있다.

· 컴플릿 콘텐츠 인스펙션과 네트워크 성능

CCI 기술이 갖는 뛰어난 장점은 컴퓨팅 성능대비 비용효과에 있다. <그림 3>에서 보듯이 CCI는 스테이트풀 인스펙션 기술이나 DPI와 비교해 백 배에서 천 배 이상의 패킷당 처리 능력을 필요로 한다.

CCI 기술을 표준 컴퓨팅 시스템(예: 서버)이나 네트워크 제품(예: 라우터, 방화벽/VPN 게이트웨이 등)에서 구현하면 시스템의 성능이 급격히 떨어진다. 또한 DPI 역시 표준 컴퓨팅 시스템과 네트워크 보안 장비에서 실행될 경우 성능이 75% 이상 저하된다. 따라서 네트워크 성능 저하 없이 CCI 기술을 제공하기 위해서는 새로운 유형의 하드웨어와 소프트웨어 아키텍처가 필요하다.



실시간 네트워크 보호 지원하는 독특한 아키텍처

포티넷은 실시간 처리가 가능한 네트워크 기반 솔루션으로 CCI를 구현하는 독특한 아키텍처를 개발했다. 포티넷은 핵심 기술을 필수 애플리케이션 및 세계 정상급 공격 대응 시스템과 연계함으로써 강력하고 비용 효율적인 실시간 네트워크 보호 솔루션을 제공하고 있다.

· 핵심 기술

포티넷의 포티게이트(FortiGate) 안티바이러스-IPS는 네트워크 레벨의 보안 기능과 더불어 네트워크 상에서 애플리케이션 레벨 콘텐츠 프로세싱을 실시간으로 처리하는 하드웨어/소프트웨어 통합 아키텍처 시스템을 기반으로 한다. 포티넷의 아바카스(ABACAS, Accelerated Behavior and Content Analysis System) 기술은 초당 1기가비트 이상의 데이터 속도로 실시간 바이러스 검색 및 콘텐츠 필터링과 같은 애플리케이션 레이어 서비스를 제공할 수 있는 플랫폼이다.

자체 포티ASIC(FortiASIC) 칩에는 하드웨어 검색 엔진과 하드웨어 암호화, 실시간 콘텐츠 분석 프로세싱이 통합되어 있다. 포티넷이 개발하고 포티게이트 시스템에서만 사

용할 수 있는 이 포티ASIC은 빠른 속도로 다음과 같은 네 가지 기능을 실행한다.

- 패킷 헤더가 유효한 소스(방화벽)에서 온 것인지 확인
- VPN 패킷(DES, 3DES, MD5, SHA-1) 인증, 암호화 및 복호화
- 콘텐츠의 패킷 조합, 공격 및 금지 요소 검색(시그니처 검색 및 학습적 검색)
- 패킷 수 계산 및 플로우 측정(트래픽 세이핑)

포티ASIC 프로세서의 처리 능력은 기존 서버나 ASIC 기반 방화벽 및 VPN 장비를 사용하면서도 CCI를 실행할 수 있다.

포티OS(FortiOS) 운영 시스템은 단일 플랫폼에서 스테이트풀 인스펙션, DPI 및 CCI 모두를 구현할 수 있는 강력하고 안정적인 고성능 운영 시스템이다. 이 플랫폼은 안티바이러스, 침입 감지 및 침입 방지 기술을 결합해 전반적인 콘텐츠 기반 공격을 차단한다.

CCI에 스테이트풀 인스펙션, 프로토콜 분석 및 DPI 기능을 추가함으로써 문제의 소지가 있는 위협을 인지 및 제거하는 시스템이 탄생했다. 다음 표는 위협의 유형과 예, 이를 검색하는 시스템을 간략하게 정리한 것이다.

(표) 위협의 유형과 검색시스템		
위협의 유형	예	검색 시스템
연결 기반 침입	텔넷 공격	스태이트풀 인스펙션
프로토콜 공격	SYN Flood, ICMP Flood	프로토콜 분석
패킷 레벨 콘텐츠 공격	버퍼 오버플로, 침입조사 단계의 일부 침	DPI
파일 레벨 콘텐츠 공격	바이러스, 대부분의 웜, 트로이목마	CCI
파일 레벨 콘텐츠 위협	부적절한 웹 콘텐츠, 스팸	CCI

실시간 대응을 위한 포티프로텍트 서비스

포티프로텍트(FortiProtect) 서비스(FPS)는 포티넷 게이트웨이 기반 네트워크 보호 솔루션의 핵심 요소이다. 포티넷은 포티프로텍트 서비스를 통해 최신 네트워크 보안 위협 정보와 신속한 바이러스 및 침입 공격 패턴 업데이트를 전 세계 포티게이트 안티바이러스-IPS 시스템에 제공한다. 포티넷의 포티프로텍트 센터(FortiProtect Center) 웹 포털은 포티넷 고객이 최신 보안 위협 정보를 제공받을 수 있도록 분 단위로 최신 정보를 업데이트하고 있으며, 포티프로텍트 분산 네트워크(FortiProtect Distribution Network)는 새로운 위협을 검색 및 차단하는데 필요한 데이터를 포티게이트 안티바이러스-IPS 시스템에 제공한다. 시스템은 다음

과 같은 세 가지 핵심 요소로 구성된다.

- 포티프로텍트 센터
 'www.fortinet.co.kr'에서 이용할 수 있는 포티프로텍트 센터는 현재 네트워크 위협에 대한 전체적인 개요, 특정 바이러스 및 취약성에 대한 정보, 최신 포티게이트 바이러스 및 침입 데이터베이스가 지원하는 위협요소에 대한 세부 정의 등을 제공한다. 포티프로텍트 센터 정보 포털은 매일 업데이트되며 읽기 및 검색이 쉬울 뿐 아니라, 최신 보안 위협에 대한 최신 정보 유지라는 포티넷의 확고한 약속을 실천하고 있다.

- 포티프로텍트 위협 대응 팀
 (TRT, FortiProtect Threat Response Team)
 포티프로텍트 위협 대응 팀은 포티프로텍트 인프라의 중추적 요소이다. 포티프로텍트 위협 대응 팀의 보안 전문가는 포티프로텍트 분산 센터에 필요한 정보를 조사 및 개발하고 새로 등장하는 위협을 24시간 모니터링 한다. 와일드 리스트(Wild List) 협회의 설립자인 조 웰(Joe Wells) 회장이 이끄는 숙련된 네트워크 보안 전문가 팀은 바이러스 샘플을 수집 및 분석하고 현재의 포티넷 안티바이러스(AV) 정의를 업데이트하기 위한 바이러스 시그니처를 개발한다. 또한 이 팀은 네트워크 취약성 시그니처를 개발하고 포티넷 네트워크 침입방지시스템(IPS)을 업데이트한다.

- 포티 리스판스 분산 네트워크
 (FDN, FortiProtect Distribution Network)
 포티 리스판스 분산 네트워크는 포티프로텍트 위협 대응 팀에서 개발한 바이러스 및 침입 시그니처 정의를 이용해 신속하게 자동으로 업데이트를 제공함으로써 전 세계 포티게이트 안티바이러스-IPS 시스템이 최신 AV 및 IPS 보호 기능을 갖출 수 있도록 지원한다.

컴플릿 콘텐츠 인스펙션 기술은 오늘날의 콘텐츠 기반 네트워크 보안 위협에 대처하기 위한 최적의 솔루션이다. 포티게이트 안티바이러스-IPS를 이용함으로써 기업은 파괴, 도난 또는 손실로부터 정보 자산 및 지적 재산을 안전하게 보호할 수 있다. 포티게이트 안티바이러스 IPS는 포티ASIC 프로세서와 포티OS 시스템을 통해 콘텐츠를 재결합하고 분석함으로써 다른 시스템과 비교할 수 없을 정도로 뛰어난 수준의 보안과 성능을 제공한다. 