IDS를 넘어서:
네트워크 침입 방지(Network Intrusion Prevention : IPS)의 본질적 요소

해가 거듭됨에 따라 기업 네트워크가 가진 중요성, 복잡성 및 취약성은 더욱 심각한 이슈로 대두하고 있다. 오늘날 모든 기업과 에이전시들은 이러한 문제를 분명하게 인식하고 있다. 네트워크 관리자 및 엔드유저는 기술, 애플리케이션 및 기능을 지속적으로 추가하고 있으며 네트워크는 이제 물리적인 공장 설비 만큼이나 중요하게 다루어지고 있다. 뿐만 아니라 물리적 설비와 마찬가지로 작업자가 해당 설비를 사용하지 못하게 될 경우 비용 손실이 발생한다. 또한 설비가 파손될 경우 수리가 비록 불가능하지는 않더라도 상당히 어려울 뿐만 아니라 많은 비용을 지출해야 하는 상황인 것이다.

탑레이어의 신념은 모든 기업들이 원치 않는 액세스를 차단하고 침입을 탐지할 수 있어야 할 뿐만 아니라 목표로 하는 타깃을 공격하기 전에 그 공격을 적극적으로 차단할 수 있는 제품을 보유하고 있어야 한다는 것이다. 공격이 네트워크의 방어망을 뚫게 되면 “침입 이벤트’가 개시된다. 이는 공격이 저지되고, 문제의 여파가 완화되어 시스템이 정상으로 복귀될 때 까지 손실 비용은 계속해서 누적된다. 시간은 조치를 취하는 동안에도 계속 흘러 침입 개시 시점부터 발생한 지연 시간은 심지어 수 시간이 될 수도 있다.

기업들은 네트워킹에 대한 보안 위협을 처음으로 경험하게 되면 마치 문과 창에 거는 잠금장치 처럼 자체 네트워크 입구에 방어벽 역할을 하는 방화벽을 설치한다. 방화벽은 특정 인터넷 프로토콜을 위한 포트인 이들 입구를 완전히 차단함으로써 그 어떤 트래픽도 입구를 통해 전혀 통과하지 못하도록 한다. 뿐만 아니라, 방화벽은 그들이 열어 놓은 포트에 대한 액세스를 엄격하게 제어함으로써 적격의 헤더를 지닌 데이터 패킷 만이 통과할 수 있도록 한다.

방화벽은 다양한 유형의 공격을 효과적으로 방어할 수 있다고 입증된 바 있다. 그러나 기업은 방화벽을 사용해 전달되는 모든 공격을 차단할 수는 없을 것이다. 기업이 외부 세계와 단절하지 않는 한 이는 불가능할 것이다. 그리고 포트를 열어 둔 상태로 둔 놓아둔다면, 공격자들이 이를 악용하게 될 것이다. HTTP 웜, DoS(denial-of-service) 공격 및 프로토콜 변형(protocol anomaly) 등으로 인해 업계 최고의 방화벽마저도 무너뜨리게 될 것이다.

따라서 기업은 건물 출입구의 폐쇄 회로 비디오 카메라를 설치하는 것처럼 제 2의 보안 디바이스 세트를 설치하게 된다. 네트워크 IDS(침입 탐지 시스템, Intrusion Detection

System)가 바로 그것이다. 이는 데이터 패킷이 들어갈 때 그 데이터 패킷을 검사하고 발견 사항을 계속적으로 기록한다.

IDS 제품은 일반 방화벽 보다 패킷의 컨텐트를 보다 철저하게 검사한다. 방화벽이 실제로 네트워크 상에 상주해 컨텐트 검사를 위해 적격의 데이터 패킷 플로우까지도 방해하는 반면 IDS 제품은 단순히 네트워크 트래픽을 심도깊게 모니터링(eavesdrop)하기 때문이다.

따라서, 비디오 카메라처럼 IDS는 사이드에 있다가 일어나는 모든 트래픽을 감시하고 보안 관리자에게 경보를 발령할 것이다.(도로에서 흔히 접할 수 있는 차량 경보처럼, 이러한 경보도 잘못 발생되는 경우가 종종 있다. 이 경우 관리자는 곧바로 대응을 중단하게 된다.)

보안 관리자가 nIDS에 대응하고 경보의 유효성 여부를 판단하고 침입을 막기 위해 조치를 취하기 시작하는 시점에는 침입자에 의해 한동안 침입이 진행된 상태이고 따라서 기업은 오랜 시간이 걸리는 (또한 비용이 많이 드는) 원상 복구(cleanup) 및 수리 작업 수행해야 할 것이다.

최근 새로운 유형의 솔루션인 IPD(침입 방지 디바이스, Intrusion Prevention Device)가 각광받고 있다. 대부분의 경우, 이들 제품은 IDS의 업그레이드가 아닌 완전히 새로운 차원의 제품으로서 구현되고 있다.

IPD 제품은 어떤 차이점이 있을까? 이들 제품은 네트워크 상에 상주하면서 트래픽을 모니터링할 뿐만 아니라 악성으로 예상되는 패킷을 드롭시키고 의심스러운 세션을 종료시키거나 공격에 대처하기 위한 기타 조치를 취하는 등 적극 개입한다는 것이다.

IPD가 전혀 새로운 차원의 제품이라는 점에서 탑레이어는 서명 탐지, 프로토콜 분석 등 구형 IDS 모드에 익숙한 기업이 아니라 실시간 네트워크 트래픽을 처리한 경험을 보유한 기업을 통해 성공적인 차세대 네트워크 보안 디바이스가 개발될 수 있다고 확신하고 있다. 본 백서는 기업이 직면하고 있는 위협, IDS가 이들 위협에 대처하기 위해 사용하고 있는 방법, 그리고 마지막으로 IPD가 이들 위협에 대처하는 새로운 방법을 설명하고 있다.

섹션 1 : 위협

보호 받은 네트워크의 많은 자원은 안전하게 유지되어야 하며 언제라도 이용할 수 있어야 한다. 공격은 기업이 의존하고 있는 파일, 프로그램, 하드웨어 또는 대역폭 등 다양한 자원에 영향을 미칠 수 있다.

다음의 보안 침입 유형은 가장 일반적인 공격 유형을 나타낸 것이다. 오늘날 특정한 카테고리의 공격이 주류를 이루고 있지만 이는 언제라도 순식간에 바뀔 수 있다는 점을 명심해야 한다. 님다(Nimda) 웜이 네트워크를 공격하는 단일 문제로서 가장 일반적인 형태로 자리잡는 데는 매우 짧은 시간이 소요됐지만 또 다른 새로운 공격이 순식간에 가장 심각한 사안으로 대두하게 될 수도 있다.

공용 프로토콜 침입. 네트워크 자원을 대상으로 가장 빈번하게 발생하는 공격은 기업이 인터넷 전반에 걸쳐 사용하는 프로코콜을 이용하기 위해 사용되는 메소드 그룹에서 시작되고 있다. 이들 공격은 네크워크 내부에서 돌아다니려고 하는 외부의 누군가에 의한 것이다. 이들 중 일부는 단순한 프로브(probe) - (예, 취약점을 발견하기 위해 포트를 스캐닝하는 것)- 일 수도 있다. 이와 같은 프로브 그 자체로서는 네트워크에 아무런 해를 끼치지 않지만 종종 로그인 시도나 IP 스푸핑(spoofing)과 같이 좀더 은밀한 메소드를 사용해 열린 프로토콜을 악용하려고 시도하게 된다. 일단 네트워크가 일차적으로 손상을 입게 되면 네트워크 프로토콜을 이용한 추가 침입이 발생할 수 있다.

마지막으로 기업 내부의 사용자가 네트워크 상에서 악의적인 행동을 시도할 수 있으며 이런 침입 형태는 그 피해가 가장 심각할 수 있다.

HTTP 공격. 웜은 자기 복제를 통해 계속 퍼져나가도록 설계된 컴퓨터 코드다. 일부 웜은 단순히 계속 퍼져나가기만 해 컴퓨터와 네트워크 공간을 꽉 채워 마비시키기도 한다. 또한 다른 웜은 이동할 때 호스트 컴퓨터를 파괴시킨다. 1년 이상 수 천 여대의 머신을 감염시킨 님다와 같은 HTTP 웜은 감염된 e-메일로부터 시작했다가, 일단 시스템에 이상이 발생하면 네트워크 공간으로 빠르게 퍼져나가게 되고, 그 다음 감염된 포스트는 취약한 웹 서버를 스캐닝한 후 감염시키는 여러 공격 메소드를 보유하고 있다. 웹 사이트를 관리하는 호스트 컴

퓨터를 이용함으로써 님다는 실제로 기업의 방화벽 뒤에서 활동을 함으로써 인트라넷 상의 또는 심지어 비즈니스 파트너와 공유하는 엑스트라넷 상에서 안전하게 여겨지는 사이트를 감염시킨다. e-메일을 스캐닝하는 안티바이러스 소프트웨어는 발생하게 될 웜의 확산을 전혀 파악하지 못한다. nIDS 센서는 단일의 감염된 호스트로부터 1천 회의 경보를 발행할 수 있지만 실제로 그 어떤 공격의 확산도 저지하지 못한다.

SYN 플러드(flood) 공격. 가끔 DoS 공격으로 인해 유명 웹 사이트가 마비 또는 중단됐다는 뉴스를 접하곤 한다. 그러나 이 DoS 공격은 실제 알려진 것보다 훨씬 더 자주 발생하며 모든 규모의 기업을 대상으로 이루어진다. 이들 공격은 서버에 엄청난 양의 트래픽을 일시에 반복적으로 보냄으로써 네트워크 속도를 느려지게 하며 적법한 사용을 막을 뿐만 아니라, 심지어 서버의 기능을 완전히 마비시킬 수 있다.

SYN 공격은 얼마나 간단하게 네트워크 장애를 일으킬 수 있는 지를 여실히 보여 주고 있다. SYN 통신은 2 대의 컴퓨터 간의 통신을 시작하기 위해 사용되는 것으로서 응답을 발생시키게 된다. 단순히 가짜 소스 주소를 사용하는 SYN 스트링을 반복적으로 끝도 없이 계속 보냄으로써, 공격하는 컴퓨터는 타깃 컴퓨터가 점점 더 많은 불완전한 커넥션을 열게 된다. 일정 순간이 되면, 시스템은 충돌하게 된다(crash). 표준 방화벽 구현으로는 SYN 플러드 공격을 효과적으로 저지하지 못한다. 비록 일부 벤더의 경우 SYN 활동을 모니터링하기 위한 추가 플러그 인을 제공하긴 하지만, 이들은 종종 방화벽의 성능을 크게 저하시키는 결과를 초래한다. 대부분의 nIDS 센서는 SYN 플러드를 감지할 수 있지만, 이들은 네트워크 외부에 존재하기 때문에 SYN 활동의 변화하는 특징을 파악할 수 없다. 예를 들어, 웹 서버는 예를 들어 파일 및 프린트 서버 보다 많은 오픈 SYN 커넥션을 만든다. NIDS 센서는 모든 호스트를 동일하게 처리해야 하기 때문에 이처럼 서로 다른 활동들 간의 차이점을 구분할 수 없게 되며 따라서 공격을 정상적인 활동으로 판단(false positive)하는 실수가 증가하게 된다.

FTP 공격. FTP(File Transfer Protocol)은 파일 공유를 위해 일반적으로 사용되는 인터넷 프로토콜이다. 그러나 설계 상의 결함 때문에 '바운스(bounce)' 공격에 취약하다. 공격자는 타깃 사용자의 IP 주소만 보유하고 있으면 된다. 공격자는 FTP 서버를 사용해 타깃 사용자와의 커넥션을 연결하고, 전혀 해롭지 않아 보이는 이 커넥션을 이용해 악성 코드가 방화벽

을 통과할 수 있도록 한다. 이 때 종종 이 코드는 공격자에 대한 직접 액세스를 설정함으로써 공격자는 타깃 사용자의 컴퓨터에 완벽한 액세스 권한을 확보하게 된다.

ICMP 공격. 네트워크에 대한 진단을 수행하기 위해, 네트워크 관리자는 일반적으로 ICMP 프로토콜을 사용한다. 당연히 해커는 이 열려진 상태를 악용한다. 해커는 기본적으로 포트를 통해 가짜 요청(핑)을 보냄으로써 내부에서 응답을 하도록 한다. 이는 정보를 얻거나, 시스템을 마비시키거나(flood), 심지어 취약성을 더욱 악화시킬 수 있는 명령어를 심는데 이용될 수 있다. ICMP 응답을 이용해 손상된 머신에 명령어를 과도하게 보내는 것(피기백, piggyback)이 그 대표적인 예가 될 수 있다.

애플리케이션 공격. 웹 서버 상에서 실행되는 애플리케이션에서 완벽하게 버그를 제거한다는 것은 매우 어렵다. 만약 한 해커가 이를 이용할 수 있는 방법을 발견하게 되면, 언더그라운드의 해커들을 통해 급속하게 알려지게 된다. 종종 공격자는 임시 메모리 파일의 과부하로 인해서 흔히 발생하게 되는 취약점인 “버퍼 오버플로우”를 집중 공략한다. 영리한 해커들이라면 이런 취약점을 이용해 웜 또는 트로이 목마(Trojan)와 같은 악성 코드가 보안 액세스를 통과할 수 있는 방법이나 시스템에 대한 ‘루트(관리자)’ 액세스 권한을 확보하는 방법을 이미 알고 있다.

공격으로 인한 기업의 피해

웹 서버 또는 네트워크에 대한 엄청난 파괴력의 공격은 그것이 비록 단 한번일지라도 기업에게는 막대한 규모의 경제적 피해를 줄 수 있다. 공격은 비즈니스 거래를 방해하거나 지연시킬 수 있을 뿐만 아니라 전용 정보를 손상시키고, 직원들이 업무를 수행할 수 없게 되는 것은 물론 시스템을 교체해야 하는 경우도 있다.

그러나 작은 규모의 공격은 쉽게 그 정도를 수치화할 수 없다라고 할 지라도 피해를 주기는 마찬가지다. 직원들의 생산성은 웜 또는 기타 공격으로 인해 네트워크에 문제가 발생할 때 저하된다. 심지어 nIDS를 사용할 경우에도, 실제로 무엇이 일어났는지 그리고 시스템이 실제로 손상됐는지 여부를 파악한다는 것은 어려운 작업일 뿐만 아니라 많은 시간을 필요로 한다. IT 부서는 문제를 추적하고 해결하는데 막대한 시간 및 자원을 투입하게 되며 그 다음으로 네트워크나 서버를 적합한 구성으로 복구하게 된다.

뿐만 아니라, 공격은 기업이 우물쭈물 하고 있는 동안 매우 큰 피해를 입힌다. 보안 담당자들은 끝도 없는 네트워크 로그를 모니터링하고 가짜 경보를 추적하느라고 시간을 허비하고 기업의 재정 비용을 소모하고 있다.

인터넷 상에 '희생 양' (예, 패치를 적용하지 않고 Windows 2000의 경우 IIS를, Linux의 경우 Apache를 디폴트로 내장)을 배치하는 단순한 실험을 통해 무엇이 일어나는지 모니터링하는 것이 효과적일 수 있다. 일반적으로 시스템은 4 시간이 채 지나지 않아(어떤 경우 불과 몇 분 만에) 피해를 입게 되며 nIDS 센서를 모니터링하는 것은 24 시간 동안 9,000 회 이상의 경보를 발행할 수 있다. '실세계' 환경에서 이들 경보 중 대다수는 시스템에 영향을 미치는지 여부를 판단하기 위해 조사해야 할 것이다.

최근 조사에 의하면, 대부부의 대기업은 지난 12 개월 내에 보안 침해 사례를 보고했다. 공격이 발생하는 것 자체는 막을 수가 없다고 하더라도 많은 공격의 경우 네트워크 운영에 침입하거나 시스템을 손상시키기 전에 저지할 수 있다. 그리고 침입이 발생할 경우, 기업이 문제를 얼마나 신속하게 해결할수록 있느냐에 따라, 손실 비용을 좌우하게 된다.

문제의 해결은 단순히 취약점을 계속 악용하지 못하도록 저지하는 것 만을 의미하는 것은 아니다. 한 번의 침입 행위는 종종 일련의 공격 활동을 유발한다. 예를 들어 네트워크에 들어 온 웜은 계속적으로 확산될 뿐만 아니라 새로운 공격을 개시한다. 모든 진행되는 침입 행위의 영향은 반드시 차단되어야 한다. 여기에 이미 입은 피해를 복구하고 시스템이 정상적으로 작동되도록 복구시켜야 하는 작업이 이루어져야 한다. 이는 수 시간, 수 일 또는 그 이상이 걸릴 수도 있으며 따라서 기업으로서는 엄청남 비용 부담이 가중된다. 대부분의 경우 님다로 인해 네트워크에 피해를 입은 경우 기업들은 모든 http 작업을 네트워크에서 중단시켜야 했다(스캔 등을 통해 생성된 트래픽 때문에). 기업들이 웹 기반 업무 처리 애플리케이션에 대한 의존도가 높아짐에 따라, 이는 해당 기업의 일일 운영에 엄청난 영향을 미칠 수 있다.

탑레이어는 기업은 공격에 의한 취약점 윈도우(여지, 가능성, window)(여기에서는 노출(exposure)이 더 적합하지 않은가?)를 최소화하는데 그 목표를 두어야 할 것으로 보고 있

다. 네트워크 또는 서버 침입은 신속하게 제어되어야 하며, 가장 바람직한 것은 공격이 저지되고 그 윈도우마저도 완전히 제거되는 것이다. 공격이 성공하게 되면 침입 이벤트가 개시된다. 침입 이벤트가 신속한 상황의 해결 및 정상화로 이어질 수 있는 연속적인 이벤트를 즉각 발동시키는 것이 중요하다.

열려 있는 윈도우를 줄일수록 침입 진행 속도를 저하시키고 시스템의 정상 복구 속도를 가속화시킬 수 있게 된다. 윈도우가 열려 있다면 신속한 조치가 매우 중요하다.

(그림)
침입 이벤트의 전체 전개 과정

개시 종료
공격 -> 저지 -> 침입 -> 탐지 -> 악용 중단 -> 영향 중단 -> 시스템 복구

섹션 2. 침입 탐지

IDS 운영 방법
방화벽의 한계는 처음 개발됐을 당시부터 분명히 드러났다. 인터넷 덕분에 작업자가 보다 작업을 수행할 수 있게 된 것은 사실이지만, 이를 위해서 작업자는 SMTP, DNS, FTP, HTTP 등 모든 방식의 프로토콜을 사용해야만 했다. 보안 관리자는 어느 정도까지는 이들 프로토콜을 사용할 수 있도록 방화벽을 구성해야 했다. 이는 곧 방화벽이 모든 공격을 차단할 수 있으리라는 기대를 할 수 없다는 것을 의미하는 것이다.

이러한 요구에 대처하기 위해 등장한 제품 카테고리가 nIDS(network Intrusion Detection System) 였다. 이들 제품은 네트워크 사이드, 대역 외에 존재하며 전달되는 트래픽 플로우를 감시한다.

초기에 이 전략은 nIDS를 통해 알려진 위협이 발생하고 있다는 증거를 발견하는 것이었지만 추후 정상적인 트래픽으로 보이지 않는 네트워크 트래픽과 같은 이상 현상을 탐지하는 새로운 메소드가 추가됐다.

패턴 매칭. nIDS 제품은 패턴 매칭 알고리즘을 사용해 진행 중인 침입을 파악한다. NIDS는 알려진 공격 패턴의 서명을 이용하며 nIDS 센서는 네트워크를 통과하는 트래픽에서 이러한 패턴의 증거를 포착하기 위해 지속적으로 스캐닝한다.

공격 서명을 검색하는 IDS 센서는 “악성 수표” 리스트를 벽에 테이프로 부착한 출납원과 같다. 이 시스템은 알려진 침입자 만을 포착하며, 이마저도 리스트가 지속적으로 업데이트 된다는 가정 하에서 가능하게 된다. 불행히도, 네트워크를 악용하려는 사람들은 결코 게으르거나 어리석지 않다. 그들은 끊임 없이 새로운 변종을 만들어 내고 새로운 공격을 개시한다. 매번 새로운 공격을 할 때 마다 새로운 서명을 IDS에게 알려줘야 한다. 시간이 지남에 따라, 이는 IDS 제품은 말 그대로 수 천 개의 공격 서명을 보유해야 하고 그 모든 서명을 지속적으로 스캔닝해야 할 뿐만 아니라 IDS의 서명 라이브러리를 끊임없이 업데이트 해야 한다는 요구가 발생하게 된다. 공격자는 IDS 제품이 어떻게 운영되는 지 정확히 알고 있기 때문에 탐지를 피하기 위해 계속해서 약간씩 변형하게 된다. 보다 정확한 결과를 도출하기 위해서는 보다 우수한 인텔리전트 서명 시스템이 요구된다.

스테이트풀 매칭(stateful matching). 인텔리전트 서명 패턴 매칭은 일반적 메소드를 크게 향상시킨 것이다. 이는 서명의 주변 상황 및 배치 상태를 관찰함으로써 공격 여부를 보다 지능적으로 판단할 수 있게 된다. IDS는 외부 엔티티와의 커넥션 상태를 계속 추적하고 커넥션 동안 시작된 모든 트랜잭션을 포함해 보다 포괄적인 상황을 고려해 판단하게 된다.

프로토콜 공격. 새로운 시스템일수록 먼저 프로토콜을 규명한 후 비정상적인 활동 또는 프로토콜과 연관된 공격 서명을 구체적으로 탐색함으로써 시간을 절약할 수 있도록 한다. 따라서 이를 통해 보다 정확하게 대상을 겨냥할 수 있을 뿐만 아니라 더욱 효과적으로 검색을 수행할 수 있게 된다. 이를 통해 IDS는 네트워크 트래픽 내에 숨겨진 공격을 더욱 효과적으로 발견할 수 있게 된다.

IDS의 한계

IDS 제품은 기업이 침입을 탐지할 수 있도록 지원하는 것은 분명하지만, 공격이 증가함에 따라, 그 한계점이 보다 분명하게 드러나고 있다. 배치 및 운영 상의 문제 역시 이 접근 방

식의 중대한 단점으로 지적되고 있다. 제품 개선으로도 이와 같은 본질적인 문제를 해결할 수 없다.

탐지는 가능하지만 방지는 불가능. nIDS는 네트워크로부터 따로 떨어져 있기 때문에 트래픽에 영향력을 행사하기 어렵다. 따라서, 진행 중인 공격을 중단시키거나 최소한 진행 속도를 늦출 수 있을 정도의 능력이 없다. 뿐만 아니라, 매우 높은 경보 오류율을 감안할 때 경보의 정확성이 보장되지 않는 한 그 누구도 nIDS에 데이터 패킷 드롭을 맡기려 하지 않을 것이다. 따라서 공격을 직접 확인하는 작업이 반드시 필요하다.

해결까지 오랜 시간 소요. 수동 개입의 필요성 그리고 엄청난 양의 데이터에 대한 세밀한 검사로 인해 침입 이벤트 시작에 대한 대응 시점이 늦춰지게 된다. 위에서 언급한 바와 같이, 취약성의 윈도우를 최소화하기 위해서 즉각적인 조치가 요구된다.

과도한 로그 데이터. IDS는 모든 공격을 적극적으로 저지하지 못하기 때문에, 비정상적이거나 또는 의심스러운 네트워크 활동에 대한 수 많은 리포트를 생성해야 한다. 네트워크 보안 관리자는 많은 시간을 들여 이들 로그들 뿐만 아니라 네트워크 트레이스 추적 및 기타 진단 메소드를 검토함으로써 실태 파악 및 조치 여부에 대한 판단을 해야 한다. IDS 벤더의 자체 MSP(Managed Service Provider) 운영을 통해 문제 정도를 나타낼 수 있다. 한 벤더의 경우 3 개월 동안 2천 1백만 개의 경보를 발령했으나 실제 공격이 일어난 사례(문제 해결을 위한 후속 조치를 요구하는)는 1천 4백 42건에 불과한 것으로 나타났다.

경보 오류. IDS를 운영해 본 사람이라면 누구나 시스템이 진행 중인 침입이 보고된 처음 몇 차례는 초긴장 상태에 돌입했다가 그 이벤트가 양성인 것으로 판명됐을 때 허탈해 했던 경험을 모두 갖고 있을 것이다. 결국 나중엔 경보가 발령되어도 늑장 대응을 하게 되고 종국에는 귀찮은 것으로 치부하기도 한다.

nIDS는 단순히 양성 트래픽을 공격으로 잘못 판단하기도 한다(판정 오류). 그러나 종종 이런 실수는 문제가 제기된 패킷을 검사하고 IDS가 잘못 판단했다는 결론을 내리기까지 많은 시간을 요구하게 된다.

때로는, IDS가 서명과 일치하는 특정 트래픽 패턴을 식별했지만, 그 패턴은 특정 해당 기업에서는 정상적인 패턴으로 판명되기도 한다(판정 오류). 이러한 경보로 인해 네트워크 관리자는 권한이 있는 트랙픽임에도 불구하고 공격으로 오인됨으로써 그 트래픽을 잠정적으로 중단시킬 수 있다.

더욱 심각한 경우, 경보 오류로 인해 사람들이 실제 침입 상황에 대해 둔감해지게 된다. 2002년 Network World Fusion 리포트는 “실제 공격이 발생할 때, 일부 (IDS) 제품은...오류 경보 리포트를 과도하게 발행함으로써 실제 공격을 놓치기가 쉽다.”고 결론을 내렸다.

개발 문제. nIDS 센서는 CCTV 카메라와 같다. 그리고 CCTV 카메라처럼 어디에나 설치되어 있는 것은 아니다(센서 비용 때문에). 따라서 센서는 네트워크의 중요한 지점에만 설치될 수 밖에 없다. 그 다음 적절하게 구성되어야 할 뿐만 아니라 끊임없이 업데이트되어야 한다. 실제로, nIDS을 운영하는 것이 무척 까다롭고 비효율적인 것으로 입증됐다. 이는 센서 운영을 위한 추가 작업 시간을 요구할 뿐만 아니라 구성이 잘못됐을 경우 성능 저하를 가져오고 공격과 침입을 제대로 탐지하지 못할 가능성이 있다.

실망스러운 결과. 벤더들이 여러 세대 제품을 거치는 동안 nIDS를 향상시키고 공격 서명에 대한 방대한 라이브러리를 컴파일했더라도, 처음 IDS 제품이 등장하기 시작했던 8년 전보다 지금이 더 안전하다고 느끼는 기업은 거의 없을 것이다. 알려진 공격 또는 일반적인 공격 등을 포함한 모든 공격은 계속해서 발생되고 있으며 또한 성공을 거두고 있다. 교묘하게 변형된 공격을 통해 이들 제품들은 무용지물이 되고 있다. 가장 중요한 것은 님다와 같은 새로운 유형의 공격은 그 전파가 너무나 급속도로 진행되기 때문에 nIDS가 탐지해 보안 관리자가 적절한 대응을 할 수 있기도 전에 엄청난 피해를 입힌다는 사실이다.

섹션 3 : 침입 방지

효과적인 보안은 네트워크 외부에 상주하면서 내부를 감시하는 것 만으로는 실현될 수 없다. 다행스러운 것은, 차세대 보안 제품에서는 수동적인 모니터링 기능이 아니라 기업의 컴퓨팅 자원을 적극적으로 보호하며 실질적인 조치를 취하는 기능이 구현되고 있다는 것이다.

탑레이어는 공격이 기업의 시스템을 위협할 때 탐지, 대응 및 리포팅 메커니즘을 통합한

IPS(Intrusion Prevention System)야 말로 진정한 의미의 효과적 보안을 제공할 수 있다고 확신하고 있다.

IPS 운영 방법

IPS 제품은 네트워크 내에 – 일반적으로 방화벽 뒤에- 상주함으로써 송수신되는 모든 패킷을 검사한다. IPS는 모든 유형의 패킷을 처리하고 각 개별 패킷 뿐만 아니라 트래픽 패턴에 대한 광범위한 탐지 분석을 수행함으로써 각 트랜잭션의 전후 상황을 포괄적으로 검토한다. 탑레이어의 Attack Mitigator IPS 솔루션은 여러 다양한 트래픽 플로우 분석 메커니즘을 사용해 의심스러운 트래픽에 대한 악성 여부를 판단한다. 탐지 메커니즘에는 주소 매칭, HTTP 스트링 및 서브스트링 매칭, 일반 패턴 매칭 및 TCP/UDP 포트 매칭이 포함된다.

만약 IPS가 패킷이 무해하다고 판단할 경우 그 패킷을 정상적으로 통과시킨다. 이 경우 엔드 유저는 아무런 영향도 의식하지 못한다. 그러나 IPS가 공격을 탐지할 경우에는 자체 대응 메커니즘 중 하나를 실행한다. 이는 트래픽을 제한할 수도 있다. 즉, 일정 수의 패킷 만을 정상적으로 통과시킨다. 또한 트래픽을 필터링할 수도 있다. 패킷에서 비정상적인 패킷만 제거한 후 패킷을 계속 통과시킨다. 다른 옵션으로는 트래픽을 제지하고 추후 공격에 대한 분석 포렌식(forensics, 공격 증거 수집 및 분석)을 위해 패킷을 검사할 수 있을 때까지 저장해 두고 통과시키지 않는 방법이 적용될 수 있다. 마지막으로 IPS는 패킷을 완전히 폐기할 수도 있다.

이들 기능과 방화벽의 기능을 차이점을 파악하는 것이 중요하다. 방화벽은 본질적으로 외부 엔티티가 데이터 포트를 통해 연결을 시도할 때 승인 또는 거부의 기능을 수행하는 네트워크 트래픽에 대한 액세스 제어 디바이스다. 방화벽은 네트워크 상에서 여러 클래스의 트래픽을 방지하는 데 매우 중요한 역할을 한다. 그러나 방화벽이 일단 연결 요청을 승인하면, 그 이후 통신을 구성하는 개별 패킷에 대해서 그 어떤 조치도 거의 취할 수 없다.

물론 IPS 역시 광범위한 리포팅 메커니즘을 보유하고 있어야 한다. 그러나 이는 단순한 로그 활동에 대한 리포트 만으로 그치지 않을 것이다. IPS는 경보를 생성해 적합한 목적지로 전송할 수 있다. IPS는 보안 직원이 즉각적인 분석 및 진단을 수행할 수 있도록 포렌식(forensic) 포트를 통해 실제 트래픽 복사본을 발송할 수 있다. 심지어 진행 중인 전체 세션

트래픽에 대한 “플로우 미러(flow mirror)”를 생성해 미러 포트로 보냄으로써 써드 파티 보안 디바이스를 통해 분석할 수 있도록 할 수 있다. 마찬가지로, IPS는 실제로 네트워크에 들어가지 않는 가짜 세션으로 해커를 유인해 공격자가 자동으로 덫에 걸려들도록 할 수 있을 뿐만 아니라 그 근원지를 추적할 수 있다. (정말 그렇습니까?)

네트워크 보안 관리자는 기업의 요구 및 정책 수준에 따라 이와 같은 탐지, 대응 및 리포팅 메커니즘을 구성할 수 있다. IPS가 네트워크 성능에 대한 부작용 없이 이 모든 것을 수행할 수 있다고 관리자가 확신하게 되면, 모드 설정을 통해 “비활성” (탐지 비활성, 대응 비활성, 리포팅 비활성), “모니터링” (탐지 및 특정 리포팅 메커니즘 활성, 대응 비활성) 및 “문제 해결”(탐지 및 특정 대응 및 리포팅 메커니즘) 단계까지 상향 조정할 수 있다. 이는 특정 유형의 공격에만 국한되는 것이 아니며, 다른 호스트 그룹에도 여러 세밀한 설정을 적용할 수 있다.

탐지 메소드

IPS는 위에서 설명한 IDS 스캐닝 메소드를 훨씬 능가하는 일련의 탐지 메소드를 사용한다. 탑레이는 모든 유형의 공격을 검색할 수 있도록 4 단계의 탐지 프로세스를 통합시켰다. (사실과 다르므로 이렇게 쓰지 않아야 않는 것이 바람직)

인텔리전트 서명. 탑레이어의 Attack Mitigator가 인텔리전트 서명을 어떻게 이용하고 있는지에 대해 설명하고자 한다. Attack Mitigator는 일반 패턴 매칭을 사용할 수 있다는 점에서 nIDS와 같지만 공격 서명 검색을 위해 패킷의 모든 부분을 더욱 깊숙이 탐색할 수 있다는 고유의 특징을 가지고 있다. 본 제품은 또한 인텔리전트 매칭 메커니즘을 사용함으로써 여러 변종들을 식별할 수 있지만 일반적인 매칭의 경우 새로운 서명을 통해서만 탐지할 수 있다. 여기에 대한 좋은 예로는 URI 탐지를 들 수 있다. 대부분의 nIDS는 각 공격 변종에 대한 다른 서명을 요구한다. 즉 단순한 디렉토리 위반 공격의 경우에도, 이는 각 유니코드 변종에 대한 10~20개의 다른 서명을 요구한다. Attack Mitigator IPS는 실제로 URI를 디코딩해 그 결과를 검토하고 ‘../..’ 악용이 포함되었는지 여부를 판별한다. 이는 nIDS가 ‘../..’를 처리하기 위해 10~20개의 서명을 요구하는 것과는 달리 Attack Mitigator IPS는 오직 단일 서명 만을 요구한다는 것을 의미하는 것이다.

DoS/Ddos 엔진. Attack Mitigaor는 겉으로 보기에는 각기 다른 소스를 가진 일련의 무해한 개별 패킷처럼 보이도록 함으로써 보안 구성을 교란시키는 분산 공격을 포함해 서버에 대한 DoS 공격을 식별할 수 있도록 하는 통합 메소드를 사용한다. 통합 패킷 필터, 패킷 시퀀스 서명 및 TCP, UDP 및 ICMP 커넥션 또는 플로우 카운터(flow counter)를 사용함으로써, Attack Mitigator는 공격이 임의의 다중 소스 주소에서 시작된 것이라 하더라도 SYN 플러드 공격, UDP 폭탄(bomb), FTP 바운스, PoD(Ping of Death) 및 IP 조각 플러드를 탐지할 수 있다.

안티 웜 및 포트 엔진. 탑레이어는 TCP/UDP 포트 매칭 서명을 사용해 정기적인 서명 패턴 매칭 뿐만 아니라, 미심쩍은 포트 연결 시도를 식별한다. 웜을 나타내는 문자 스트링을 검사하는 HTTP URI 필터가 중요한 컴포넌트이다. 이를 통해 IPS는 네트워크에 유입되거나 머신을 감염시키지 못하도록 방지함으로써 웜이 처음부터 확산되지 못하도록 한다. 탑레이어는 업계 최고로 문자 스트링 매칭 및 길이 검사 기능을 이용해 HTTP 공격을 정확하게 탐지할 수 있는 메소드를 개발했다.

트래픽 변형(anomaly) 엔진. 인텔리전트 트래픽 분석 시스템을 이용해, Attack Mitigator는 프로토콜 이상 탐지 및 서명 탐지 뿐만 아니라 트래픽 변형 탐지까지 수행한다. 이는 수상한 패킷을 식별하는 수준을 넘어 네트워크를 통과하는 의심스러운 트래픽 패턴을 포착한다는 것을 의미한다.

이점

향상된 탐지 기능. 뛰어난 탐지 메소드를 사용하고 네트워크 트래픽과 동일선 상에 위치한다는 이점을 활용함으로써, IPS 제품은 IDS가 가능했던 그 어떤 수준보다 훨씬 많은 유형의 공격을 탐지할 수 있다.(표현 수위를 약간 낮추는 것이 바람직). 서명에 대한 의존도는 낮추는 대신 인텔리전트 탐지 메소드를 보다 적극 활용함으로써 IPS는 경보 오류 발생율을 낮춘다. 이를 통해 기업은 실제적인 위협에 대처하는데 시간과 노력을 투입할 수 있게 되는 것이다.

적극적 방지. IDS는 단순히 수상하거나 또는 비정상적인 트래픽을 보고하는 반면, IPS는 앞서 기술한 바와 같이 다양한 차단 전략을 수행할 수 있다. 이는 네트워크 보안 관리자가 많

은 시간을 소요해야 하는 필요성을 없애며 신속하게 위협을 해결할 수 있도록 한다.(논리적이 않음). IPS는 IDS보다 정확도가 훨씬 뛰어나기 때문에 기업은 IPS 제품이 양성 트래픽을 드롭시킬 가능성에 대해 전혀 걱정을 하지 않아도 된다. 뿐만 아니라 제품의 성능과 기능을 효과적으로 수행하고 위험한 패킷을 유연하게 제거할 것이라는 사실을 믿고 안심할 수 있다.

신속한 침입 차단. 앞서 논의된 바와 같이, 침입 이벤트는 기업 컴퓨팅 자원에 피해를 입히는 프로세스로서 향후 법적 책임을 지게 될 가능성도 가지고 있다. 탐지 시점에 개입함으로써, IPS는 침입을 신속하게 저지하고 네트워크가 정상으로 돌아가는데 드는 전체 소요 시간을 최소화하게 된다.

IPS의 요구 사항

IPS 접근 방식이 최상의 탐지 메소드를 보유하고 있으며 최고의 성능을 통해 정상적인 트랙픽을 네트워크 상에서 전달할 수 있을 때 IPS 접근 방식은 IDS 보다 많은 이점을 실현하게 된다.

IPS 제품의 프로그램이 위에서 언급한 바처럼 단순한 패턴 매칭을 넘는 강력한 메소드를 사용할 경우 제품을 인라인으로 배치함으로써 탐지 기능을 향상시킬 수 있다. (센서가 모니터링 디바이스다라는 마이크의 설명에 반대한다. IDS RMON 프로브(probe), AV 등과 같은 IDS는 그렇게 말 할 수 있을 것이다. 따라서 그냥 센서라고 하는 것이 나을 것이다). 일반적인 IDS의 탐지 방법이 IPS에서 사용될 경우 IDS와 같이 많은 오류 경보를 발행하게 될 것이다. 따라서 IPS는 패킷 인라인을 감시할 수 있는 능력을 이용하는 새로운 기술을 포함하고 있어야 한다.

그러나 IPS 센서를 인라인으로 배치함으로써 만약 솔루션이 뛰어난 네트워크 성능 표준에 맞춰 개발되지 않은 경우 새로운 문제를 일으킬 가능성이 있다. 기업은 모든 제품이 네트워크의 트래픽과 동일선 상에 상주하면서 패킷을 검사하고 통과시키는 등 제대로 그 기능을 수행하도록 요구하게 될 것이다. 따라서 IPS 벤더의 자체 개발 팀은 네트워크 가용성 및 성능 요구를 추후 추가하는 것이 아니라 제품 개발 시작 단계에서부터 설계에 반영할 수 있도록 네트워킹 엔지니어링 경험을 갖춰야 할 것이다.

탑레이어는 기업이 정확성, 완벽성, '네트워크 시민권(network citizenship)' 및 관리 등 주요 4개 카테고리에서 우월성을 입증하는 IPS 솔루션을 선택하도록 권장한다.

정확성. 앞서 언급한 바와 같이, 지금까지 IDS 제품의 가장 중요한 문제는 탐지 메소드에 의해 발생된 수 많은 오류 결과라고 할 수 있다. 이는 IDS의 경우 매우 심각한 문제가 되지만, IPS의 경우 절대 허용될 수 없는 사항이다. 부정확한 탐지는 적격의 트래픽에 영향을 미치는 대응 메커니즘을 실행시키는 결과를 초래함으로써 사용자의 업무를 방해하고 불평을 일으킬 수 있다. 탑레이어는 IDS 센서가 사용하는 메소드를 능가하는 통합 탐지 메소드를 통해 필수적인 뛰어난 정확성을 달성할 수 있다고 확신하고 있다.

완벽성. IDS 제품에서 완벽성은 제품의 라이브러리 내의 많은 서명을 통해 측정되었다. 이러한 측정 방법은 이제 낡은 방식이다. 완벽성의 핵심은 모든 클래스의 공격을 인식하고 적절하게 대응함으로써 그 공격으로부터 보호할 수 있는 능력에 있다. 완벽성이란 모든 가능한 대응 메커니즘을 최대한 포함하고 있다는 것을 의미한다. 완벽한 IPS는 특정의 새로운 공격 서명 뿐만 아니라 전혀 새로운 클래스의 공격은 물론 적절한 대응을 펌웨어 업그레이드를 통해 업데이트할 수 있는 방법을 내장하고 있어야 한다는 것을 의미한다. (펌웨어를 사용할 필요가 있나요? 인텔 플랫폼 상에서 개발된 IPS는 어떤가요? 그게 중요한가?). 탑레이어는 탐지, 대응 및 리포팅에 대한 광범위하고 철저한 접근 방식이 탑레이어의 IPS 솔루션의 차별화된 강점이라고 자신할 수 있다.

네트워크 시민권. IPS는 네트워크의 주변부가 아니라 네트워크의 핵심 부분을 구성하고 있다. 따라서 IPS는 기업에게 부과되는 그 어떠한 압력도 견딜 수 있도록 해야 한다. 이는 성능, 신뢰성 및 가용성에 의해 평가되는 우수한 네트워크의 구성 요소이다. 성능은 네트워크 상에서 트래픽의 흐름을 유지시킬 수 있는 IPS 능력을 가리킨다. 과도한 트래픽 환경 하의 낮은 성능은 결국 트래픽 성능의 저하를 초래할 뿐만 아니라 심지어 패킷 손실을 가져 올 것이다. 신뢰성이란 네트워크 상의 다른 시스템에 지장을 주지 않으면서 그 기능을 올바르게 수행할 수 있는 IPS의 능력을 의미한다. 가용성은 폐쇄, 다운 또는 수리로 인한 제품의 정지 시간으로 나타낼 수 있다.

탑레이어는 세계 최대 규모의 기업들을 위한 강력한 네트워킹 제품을 설계한 풍부한 경험을

보유하고 있는 네트워크 보안 기업으로서 주요 영역에서 확고한 경쟁 우위를 고수하고 있다. 탑레이어는 IPS 솔루션 구매를 고려하고 있는 기업이라면 벤더가 대규모 트래픽 네트워크 상의 패킷 처리 분야에서 입증된 경험을 보유하고 있는지의 여부를 주의깊게 검토해야 한다고 조언한다.

관리. IPS는 많은 네트워크 보안 관리 기능을 수행할 수 있게 때문에 네트워크 보안 관리자에게 많은 옵션을 제공한다. 따라서 IPS는 관리자가 손쉽게 센서 구성을 설정하고 변경할 수 있는 인테페이스를 제공해야 할 것이다. 탑레이어는 손 쉽게 사용할 수 있는 관리 인터페이스를 제공한다.

뿐만 아니라, 진정한 IPS 솔루션은 독립적으로 존재하는 것이 아니라, 통합 보완 관리(Security Integrated Management) 스위트의 중앙 허브로서 역할을 수행함으로써 궁극적으로 방화벽, IDS, 안티바이러스 및 취약성 평가 제품 및 기능을 모두 통합할 수 있어야 한다.

탑레이어의 Attack Mitigator IPS는 레이어 2 디바이스로서 기존 라우팅 인터페이스에 대한 그 어떠한 변경도 요구하지 않는다. 본 제품은 거의 탐지가 불가능하기 때문에 공격 그 자체로부터 안전하게 시스템을 보호할 수 있다.

탑레이어 제품은 여러 중요한 보안 관리 특징을 제공한다. 전용 관리 포트는 3개의 유지 보수 포트와 독립되어 있다. 유지 보수 포트로는 기업이 네트워크 분석기(analyzer)를 배치할 수 있는 구성 가능한 '플로우 미러' 포트, 안전한 오프라인 검사를 위해 필터링된 패킷을 복사할 수 있는 포렌식 디스카드(forensic discard) 포트 및 세션 리포트를 위한 구성 가능한 포트 등을 들 수 있다. 복잡한 로그를 들여다볼 필요 없이 전체 개요를 한 눈에 파악할 수 있도록 하는 Summary Security Report(보안 개요 리포트)가 제공된다. 뿐만 아니라 HTTP, SSH, 암호 보호 로컬 시리얼 콘솔 및 시스로그(syslog) 메시지와 같은 보안 프로토콜을 통해 디바이스 관리가 제공된다. 보안 강화를 위해 SNMP, HTTP 및 텔넷은 기본값으로 비활성 상태로 설정되어 있다.

결론

IPS(Intrusion Prevention System)은 차세대 네트워크 보안 솔루션으로서 기대를 모으고 있

다. 이제 곧 IPS 자체의 배치 여부가 아니라 어떤 IPS를 선택해야 하는지가 중요한 문제가 될 것이다. IDS 벤더 역시 이를 인정하기 시작했으며 따라서 자체 IPS 제품을 준비하고 있다.

탑레이어는 기업이 IPS을 구매하고자 할 경우 제품의 네트워크 기능을 면밀히 검토해야 한다고 확신한다. IPS는 네트워크 상에 상주하게 될 것이며 IPS가 다운되거나 또는 성능이 저하될 경우 네트워크에 직접적으로 영향을 미치게 된다.

뿐만 아니라, IPS 제품은 네트워크 상의 위치를 최대한 활용함으로써 새로운 첨단 탐지 기술을 구현함은 물론 다양한 개입 메소드를 제공할 수 있어야 한다. 제품에 있어 무엇보다 중요한 것은 기업들이 제품에 대한 확신을 가지게 되거나 자체 네트워크 보안 정책을 변경하게 될 때 마음 놓고 선택할 수 있도록 모니터링에서 문제 해결에 이르기까지 “포괄적인 (ramp-up)” 일련의 옵션을 제공할 수 있어야 한다는 것이다.

이와 같은 모든 옵션을 보유하고 있는 IPS라면 기업이 서버와 네트워크에 대한 위협에 노출되는 취약성을 획기적으로 줄일 수 있을 것이다. 기업의 그 어떠한 방어 조치도 IPS가 없다면 완벽하지 않다고 할 수 있다.