최신 네트워크 보안 기술 동향 분석

오승희° 남택용
한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀
(seunghee5, tynam,)@etri.re.kr

Trend Analysis for Network Security Technologies

Seung-Hee Oh°, Taekyong Nam
Electronic and Telecommunications Research Institute,
Information Security Technology Division, Network Security Architecture Research Team
(seunghee5, tynam)@etri.re.kr

요 약

현대인의 삶에서 인터넷에 대한 의존도는 나날이 높아지고 있고 더불어 시스템의 취약성을 공격하는 해킹 방식은 대규모의 트래픽을 발생하는 형태로 네트워크 자체에 대해 위협적인 존재로 발전하고 있다. 따라서 이러한 사이버 위협을 차단하고 미연에 예방하기 위해서 다양한 네트워크 보안 제품들이 등장하고 있다. 본 논문에서는 네트워크 보안 기술의 흐름을 파악하기 위하여 현재의 네트워크 보안 기술을 트래픽 제어 기술과 네트워크 보안이 접목된 기술, 침입차단 기술, VPN 기술, 침입탐지 및 침입방지 기술, 정책 기반 관리 기술로 분류하여 동향 및 제품들을 비교하고, 이를 통해 네트워크 보안 기술의 향후 발전 방향을 예측한다.

1. 서론

오늘날 인터넷은 현대인의 삶 속에 깊숙이 연관되는 불가분의 요소가 되었다. 인터넷에 대한 의존성이 증가하면서 오프라인과 마찬가지로 온라인상에서도 다양한 형태의 사이버 위협들이 기하급수적으로 증가하고 있다. 이러한 사이버 위협으로부터 사용자 데이터, 시스템 및 네트워크 자체를 보호하기 위해서 다양한 네트워크 보안 제품들이 등장하고 있다. 현재의 네트워크 보안 관련 기술을 트래픽 제어 기술과 네트워크 보안이 접목된 기술, 침입차단 기술, VPN 기술, 침입탐지 및 침입방지 기술, 정책 기반 관리 기술로 분류하여 각 기술의 동향을 살펴보고, 관련된 대표적인 제품들에 대해 기능을 비교 분석한다.

2. 트래픽 제어 기술과 네트워크 보안이 접목된 기술

트래픽 제어 기술과 Firewall, VPN 등과 같은 네트워크 보안 기술이 통합된 제품으로는 IPSS(IP Services Switch)과 Layer 7 스위치가 있다. 대표적인 IPSS 제품으로는 CoSine의 IPSX 9500™, Quarry Technologies의 iQ8000™, Nortel Network의 Shasta 5000 BSN(Broadband Service Network)™이 있다. 현재까지 나와 있는 제품들은 ISP망과 같은 거대망에 거대망에 설치되어 만족할만한 속도와 성능을 제공해주기 위해서 최소한의 네트워크 보안기능(예: Firewall, Anti-virus, VPN, Content filtering)만 제공되며, 침입 탐지, 침입 방지, 침입 대응 및 복구와 같은 기술이 포함된 제품은 아직 없는 실정이다. 또한, Layer 7 스위치 역시 특정 트래픽의 패턴을 확인하는 방식을 통해 바이러스를 걸러내고 차단할 수 있는 anti-virus 의 기능은 가지고 있으나, 그 외에 다른 방식의 공격(예: DoS, DDoS 등)에 대한 정확한 탐지 및 실시간 대응 기능은 거의 없는 상황이다. 대표적인 Layer 7 스위치로는 Top Layer 의 Attack Mitigator IPS, Packeteer 의 PacketShaper 와 PacketSeeker, Array Network 의 Traffic Manager, Radware 의 Application Switch III 등이 있다.

3. 침입 차단 기술

방화벽(Firewall)은 침입차단시스템으로도 불리는 보안 제품으로 외부망으로부터 내부망으로 접속하는 비인가자의 침입을 차단시켜주는 소프트웨어 혹은 하드웨어를 지칭한다. 방화벽은 접근제어목록(Access Control List: ACL)에 따라 내부 네트워크의 자원들의 보호를 담당하고 있는 가장 널리 보급되어 있는 대표적인 네트워크 보안 장비이다.

현재 대표적인 침입차단시스템은 기존의 패킷 필터링과 응용레벨에서의 프록시 기능을 추가한 Stateful firewall 방식이 주를 이루고 있다.

Stateful firewall 은 동적으로 상태 테이블을 생성 및 관리하고 패킷을 전송할 때 상태 테이블을 통해 감시하므로 응용 레벨의 프록시 방식보다 빠른 장점이 있다.

방화벽 제품은 세계적으로 대표적인 Check Point 의 소프트웨어 방식의 FireWall-1 과 NetScreen 의 NetScreen 시리즈 등이 있으며, 라우터 장비 업체인 Cisco 의 PIX Firewall 시리즈도 많이 보급되어 있는 제품 중의 하나이다. 근래의 제품 동향은 초고속망의 사용 증가에 따른 고속 장비의 요구에 따라 NetScreen 사와 Cisco, Servgate 사 등에서 이미 기가급의 방화벽을 출시하였으며, Nokia 에서도 Check Point 의 방화벽 소프트웨어를 하드웨어 플랫폼에 탑재하는 기가급 솔루션을 내놓고 있다. 국내에서도 시큐아이닷컴과 리눅스 운영체제를 기반으로 한 리눅스 시큐리티에서 현재의 고속 장비 개발 추세에 발맞추어 기가급 침입차단 솔루션을 보유하고 있다.

4. VPN 기술

VPN 의 데이터가 IP 패킷 형태로 전달되는 것을 IP VPN 이라 하고, IP VPN 은 크게 CPE(Customer Premises Equipment) based VPN 과 Network Based VPN(NBVPN)으로 분류된다. NBVPN 의 터널링 메커니즘에 따라 IPSec, GRE(Generic Routing Encapsulation), L2TP, MPLS 등을 사용할 수 있고, 따라서 MPLS VPN 도 IP VPN 의 일종이다.

현재의 VPN 기술은 Internet IP VPN 과 MPLS VPN 으로 크게 구분되어 발전하고 있다. IP VPN 의 경우에는 Stand-alone 형태(Router, VPN 전용 장비)에서 최근에는 침입차단 시스템과의 통합, Dedicated hardware solution 을 통한 고속화 경향, Purpose-built IP VPN 시스템 및 대역폭 보장을 위한 로드 밸런싱 기술과 결합되는 추세를 보이고 있다.[7]

Internet IP VPN 은 전용 장비보다는 침입 차단 기능과 통합되는 추세를 나타내고 있으며, 관련 제품으로는 Check Point 의 VPN-1, Symantec 의 Enterprise VPN 7.0, 시큐아이닷컴의 secuiVPN 100 Gateway, 어울림정보기술의 Secureworks VPN, 퓨처시스템의 SecuwayGate 2000 등이 있다. Internet IP VPN 은 데이터의 암/복호화로 인한 네트워크의 성능 저하와 시스템의 부하를 줄이면서 송수신 데이터의 암호화와 복호화의 고속화를 지원하기 위한 하드웨어 방식의 전용 암호 고속화 칩이 등장하고 있다. 또한 서버의 로드 밸런싱 뿐만 아니라 일정한 네트워크 대역폭을 보장하기 위한 로드 밸런싱 기능을 제공하는 제품들이 등장하고 있다.

MPLS VPN 은 Frame Relay 를 대신해서 등장한 것으로 데이터를 교환 시 보안성을 높이기 위해 데이터에 별도의 라벨을 붙여 전송하는 MPLS 기술을 적용한 VPN 서비스의 한 종류이다. MPLS VPN 을 구현하기 위해서는 ISP 의 모든 라우터가 MPLS 기능을 요구되므로 소프트웨어 업그레이드 또는 별도의 MPLS 장비를 장착해야 하는 한계를 가지고 있다. MPLS VPN 은 ISP 가 MPLS 망을 따로 구성해 서비스를 제공하며 인터넷 연결을 원하는 고객에겐 두 망 사이에 Firewall, NAT 등과 같은 보안 기능을 지원하는 게이트웨이를 설치해 인터넷에 접속시켜 준다. MPLS VPN 은 인터넷과 별개인 MPLS 망을 구성해 서비스하므로 보안성이 좋고 QoS 보장이 가능한 장점을 가지고 있다.[8] 따라서 앞으로의 VPN 제품은 Intranet VPN 과 Extranet VPN 기능과 더불어 MPSL VPN 을 포함하고, 더불어 해킹에 대비한 네트워크 보안 기능이 추가되어야 할 것이다. 향후 VPN 전용 장비보다는 침입 차단, IDS, Anti-Virus, 등과 같은 네트워크 보안 기능이 포함된 복합 보안 장비들이 주도하게 될 것이다.

대표적인 제품으로는 Nortel 의 Contivity 시리즈, CoSine 의 IPSX 시리즈, Quarry 의 iQ 시리즈, Cisco 의 VPN 7100 시리즈 등이 있다.

5. 침입탐지 및 침입방지 기술

최근의 침입탐지시스템(Intrusion Detection System: IDS)의 기술은 네트워크 대역폭에서 동작하기 위해 처리 모듈의 하드웨어화 및 성능 개선 등의 고속 침입탐지 기술과 개별 노드에서의 감사 자료를 통합하여 전체적인 네트워크 차원에서의 효율적인 침입 탐지를 수행하기 위한 상호 협력기술에 초점을 두고 발전하고 있다. 또한, DARPA (Defense Advanced Research Projects Agency)의 지원을 받는 SRI(System Design Laboratory)는 EMERALD(Event Monitoring Enabling Responses to Anomalous Live Disturbance)라는 NIDES(Next-Generation Intrusion Detection Expert System)의 후속 시스템을 개발 중이다. EMERALD 는 네트워크 기반의 침입 분석과 상호 연동성을 증가시키고 분산 컴퓨팅 환경에 맞는 침입탐지시스템 개발을 목적으로 하고 있다.

HIDS(Host-based IDS)는 단지 침입에 대한 탐지를 위주로 하는 보안 제품으로, 탐지에 따른 부작용을 위해서 방화벽과 연동을 꾀하고 있으나 탐지 오류로 인한 부작용으로 자동적인 차단에는 한계점을 드러내고 있다. 이를 극복하기 위해 지능형 엔진을 개발하고자 다양한 연구가 진행 중이나 아직까지는 눈에 띄는 기술이 개발되지 못한 상태이다.

침입방지시스템(Intrusion Prevention System: IPS)은 공격에 대한 탐지만을 수행하는 기존 IDS 의 한계를 넘어 공격 시그너처를 찾아내고 비정상적인 행위에 대해 자동적인 실시간 대응 기능이 추가된 제품으로 차세대 IDS 라고 불리

우기도 한다. Gartner 에서는 IPS 가 2005 년까지 IDS 시장의 75%를 차지할 것으로 전망하고 있다. IPS 는 기존의 IDS 에서 발생되는 False Positive(정상을 침입으로 오해하는 행위)를 어떻게 줄일 것인지가 중요한 이슈이다.[10][11]

다음 표는 대표적인 IPS 제품 들의 침입 탐지, 방지 및 대응 방식에 대해 비교 정리한 것이다.

<표 1> 침입방지시스템의 침입탐지/방지/대응 메커니즘 비교

기능 / 제품	침입탐지/방지 메커니즘	침입 대응 메커니즘
NetScreen의 NetScreen-IDP™	- 자체 개발한 MMD메커니즘 - 시그너처 기반 - 프로토콜 비정상탐지	Patent-pending 테크닉 적용
Entercept의 Entercept ™	- 시그너처 기반 - Behavioral 규칙	실시간 방어
Top Layer의 Attack Mitigator IPS	- Forensic - Alert 기반	Rate limit와 Blocking 제공
이카디아의 EZiS	- 시그너처 기반 - 플로우 기반 - Anomaly	패킷 흐름에 기반한 대응으로 브리지모드 제공

6. 정책 기반 관리 기술

정책 기반 관리 기술은 여러 보안 장비를 통합하여 관리하는 ESM(Enterprise Security Management)에서 적용되는 기술이 대표적이며, 국외보다는 국내에서 활발히 개발중인 시스템이다. ESM 은 보안 정책을 수립한 후에 수립된 보안 정책에 따라 구현하고 모니터링 및 신속한 조치를 위한 각종 경보의 기능을 제공하는 일련의 흐름인 워크플로우(Workflow) 를 일관되게 지원하고 있다.[13]

ESM 은 워크플로우에 따라 사용자 및 정책 관리와 취약성 및 위협 평가로 분류할 수 있다.

- 사용자 및 정책 관리(User & Policy Management)

보안 또는 관리정책에 따른 사용자 및 Access 관리에 무게 중심을 둔 범주이다. 이 범주에는 인증이나 Single Sign-On의 기능을 포함하는 경우가 많고, 초기 EMS 모습이 많이 반영되어 보안적 측면보다는 시스템 관리적 측면의 성격이 강하다.

- 취약성 및 위협 평가(Vulnerability & Threat Assessment)

네트워크 및 시스템의 취약점, 위협 요소들을 분석하고 모니터링하는 관리도구의 형태를 취하며 제품에 따라 분석 또는 정책관리, 모니터링 및 경보(Alert) 등 어느 쪽에 초점을 두느냐에 따라 특성을 약간씩 다르다. 최근 ESM 기술의 주류를 이루고 있으며 기존 보안 제품들과의 통합(Integration)이 활발히 진행되는 범주이다.

대표적인 국내 ESM 시스템으로는 어울림의 Secureworks ESM, 인젠의 NeoAdmin@ESM, 이글루의 SPiDER-1, 넷시큐어 테크놀러지의 ActiveESM 등이 있고, 그 밖에 IBM 의 Tivoli, Lucent 의 LSMS, Arbor Networks 의 Peakflow 등이 있다.

7. 결론

지금까지 네트워크 보안 기술에 대해서 크게 5 가지 기술로 분류하여 각 기술의 최신 개발 동향 및 관련 제품들 특징에 대해서 살펴보았다.

대표적인 리서치 기관인 Yankee Group 와 Gartner 의 자료에 의하면 향후 네트워크 보안은 정책 기반 관리 방식을 중심으로 통합 제품으로 발전할 것이라 전망하고 있다. 또한, 네트워크 보안 장비는 고속의 트래픽 처리 능력과 더불어 보안 기능을 가지고 있는 형태와 라우팅 기능은 배제한 채 보안 기능만을 지닌 전용 장비 형태가 함께 발전할 것으로 보인다.

따라서, 앞으로는 여러 보안 기능을 포함하고 있는 통합 보안 장비 또는 복합 보안 장비들, 기가급 이상의 고성능 네트워크 보안 전용 장비들이 표준화된 정책 기반 방식을 도입하여 침입에 대한 정보 및 대응 방안을 서로 공유하여 날로 다양해지고 복잡해져 가는 사이버 위협에 대처할 것으로 예측된다.

참고문헌

[1] http://news.computer.co.kr/portal/news/news_view.asp?gno=37569&searchstring=어레이네트웍스&page=1

[2] www.packeteer.com

[3] http://www.networktimes.co.kr/search/search_view.html?cate=news&cd=13672&kw=패킷티어

[4] http://www.networktimes.co.kr/search/search_view.html?cate=news&cd=13138&kw=패킷티어

[5] http://www.secui.com/korean/body1111.asp?code=1111

[6] http://www.linuxsecurity.co.kr/sec_pro_giga_02.html

[7] "Market Trends and Forecast for Firewall and IP Virtual Private Network Equipment: Worldwide, 2001-2006", Market Trend, Gartner, Oct. 2002.

[8] "차세대 네트워크 보안 구조서", ETRI, 2002. 11

[9] 이윤철, "VPN 기술 및 국내외 시장 동향", 주간기술동향 1075 호, 2002.12.4

[10] 정연서, et al., "침입방지시스템", ETRI 기술 문서, 2002. 3

[11] 정보홍, "침입 방지 시스템 분석", ETRI 기술 문서, 2003. 4

[12] http://www.ekardia.com

[13] 이영석, "ESM 자료 조사", ETRI 기술 문서, 2002. 12

[14] http://www.oullim.co.kr/products/html/p_index.html

[15] http://www.inzen.co.kr/kor/products/esm/intro.asp