최신 네트워크 보안 기술 동향 분석

오승희② 남태용
한국전자통신연구원 정보보호연구본부 네트워크보안기술연구팀
(seunghlee5, lynam)@etri.re.kr

Trend Analysis for Network Security Technologies

Seung-Hee Oh②, Taeyong Nam
Electronic and Telecommunications Research Institute,
Information Security Technology Division, Network Security Architecture Research Team
(seunghlee5, lynam)@etri.re.kr

요 약

현대인의 삶에서 인터넷에 대한 의존도는 낭만가지고 있고 더욱이 시스템의 취약성을 공격하는 해킹 방식은 대규모의 테러를 발생하는 형태로 네트워크 자체에 대해 위협적인 존재로 발전하고 있다. 따라서 이러한 사이버 위협을 차단하고 민간에 예방하기 위해서 다양한 네트워크 보안 제품들이 등장하고 있다. 본 논문에서는 네트워크 보안 기술의 홍보를 파악하기 위하여 현재의 네트워크 보안 기술을 트래픽 제어 기술과 네트워크 보안이 결합된 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 연관되며 불가분의 요소가 되었다. 인터넷에 대한 의존성이 증가하면서 오프라인과 마찬가지로 온라인상에서도 다양한 형태의 사이버 위협이 기하급수적으로 증가하고 있다. 이러한 사이버 위협으로부터 사용자 데이터, 시스템 및 네트워크 자체를 보호하기 위해서 다양한 네트워크 보안 제품들이 등장하고 있다. 현재의 네트워크 보안 관련 기술은 트래픽 제어 기술과 네트워크 보안이 결합된 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 결합된 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 CoSline의 IPSX 9500TM, Quarry Technologies의 iQ8000TM, Nortel Network의 Shasta 5000 BSN(Broadband Service Network)TM이 있다. 현재까지 나온 제품들은 ISP망과 같은 가대망에 거대망에 설치되어 안측악한 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 걸리거나 차단할 수 있는 anti-virus 기능은 가지고 있으나, 그 외 다른 방식의 과정(예: DoS, DDoS 등)에 대한 정확한 탐지 및 실시간 대응 기능은 거의 없는 상황이다. 대표적인 Layer 7 스위치로는 Top Layer의 Attack Mitigator IPS, Packeteer의 PacketShaper와 PacketSeeker, Array Network의 Traffic Manager, Radware의 Application Switch III 등이 있다.

3. 침입차단 기술

방화벽(Firewall)은 침입차단시스템으로서 불법의 보안 제품은 외부망으로부터 내부망으로 접속하는 비인가자의 접속을 차단시키주는 소프트웨어 혹은 하드웨어를 지칭한다. 방화벽은 접근제어목적(Access Control List: ACL)에 따라 내부 네트워크의 자원들의 보호를 담당하고 있는 가장 넓리 보급되어 있는 대표적인 네트워크 보안 장비이다.

현재 대표적인 침입차단시스템은 기존의 빈틈 필터링과 응용계열에서의 포록시 기능을 추가한 Stateful firewall 방식이 주를 이루고 있다.
Stateful firewall은 동적으로 상태 데이터를 생성 및 관리하고 패킷을 전송할 때 상태 데이터를 통해 감시하므로 응용 레벨의 프록시 방식보다 밀은 장점이 있다.

방화벽 제품은 세계적으로 대표적인 Check Point의 소프트웨어 방식의 FireWall-1과 NetScreen의 NetScreen 시리즈 등이 있으며, 라우터 장비 업계인 Cisco의 PIX Firewall 시리즈도 많이 보급되어 있는 제품 중의 하나이다. 근래의 제품 동향은 초고속망의 사용 증가에 따른 고속 장비의 요구에 따라 NetScreen시와 Cisco, Servoy 시등에서 이미 기기급의 방화벽을 출시하였으며, Nokia에서도 Check Point의 방화벽 소프트웨어를 하드웨어 플랫폼에 탑재하는 기기를 출시하였고 있다. 국내에서도 시가격의 둔화와 리눅스 운영체제를 기반으로 한 리눅스 시큐리티에서 현재의 고속 장비 개발 추세에 맞추어 기기가 집중된 경우가 측면을 보이고 있다.

국내에서도 시가격의 둔화와 리눅스 운영체제를 기반으로 한 리눅스 시큐리티에서 현재의 고속 장비 개발 추세에 맞추어 기기가 집중된 경우가 측면을 보이고 있다.

4. VPN 기술

VPN은 데이터가 IP 패킷 형태로 전달되는 것을 IP VPN이라고 하고, IP VPN은 크게 CPE(Customer Premises Equipment) 기반 VPN과 Network Based VPN(NBVPN)으로 분류된다. NBVPN의 데모형 테마에 따라 IPSec, GRE(Generic Routing Encapsulation), L2TP, MPLS 등을 사용할 수 있고, 따라서 MPLS VPN도 IP VPN의 일종이다.

현재의 VPN 기술은 Internet IP VPN과 MPLS VPN으로 크게 구분되어 발전하고 있다. IP VPN의 경우에는 Stand-alone 형태(Router, VPN 전용 장치)에서 최초에는 퀵프리미엄 시스템과의 동형; Dedicated hardware solution을 통한 고속화 경향, Purpose-built IP VPN 시스템 및 대역소 보장을 위한 로드 밸런싱 기술과 결합되는 추세를 보이고 있다. [7]

Internet IP VPN은 전용 장비보다는 집합 장비 기능과 통합되는 추세를 나타내고 있으며, 관련 제품으로는 Check Point의 VPN-1, Symantec의 Enterprise VPN 7.0, 시가격의 커뮤니티의 secuVPN 100 Gateway, 이음없이정보기술의 Secureworks VPN, 체크시스템의 SecucrayGate 2000 등이 있다. Internet IP VPN은 데이터의 암호화로 인한 네트워크의 성능 저하가 시스템의 부하를 증가하면서 송수신 데이터의 암호화와 복호화의 과학화를 지원하기 위한 하드웨어 방식의 전용 암호화 장치가 등장하고 있다. 또한 서버의 로드 밸런싱뿐만 아니라 일정한 네트워크 대역폭을 보장하기 위한 로드 밸런싱 기능을 제공하는 제품들이 등장하고 있다.

MPLS VPN은 Frame Relay를 대신하여 등장한 것으로 데이터를 고화시 보안성을 높이기 위해 데이터에 별도의 별도 주변을 통한 전송하는 MPLS 기술을 적용한 VPN 서비스의 한 종류이다. MPLS VPN을 구현하기 위해서는 ISP의 모든 라우터 가 MPLS 기능을 요구되므로 소프트웨어 업그레이드 또는 별도의 MPLS 장비를 장착해야 하는 한계를 가지고 있다. MPLS VPN은 ISP 가 MPLS 맵을 따로 구성하여 서비스를 제공하며 인터넷 연결을 원하는 고객에게 전 망 사이에 FireWall, NAT 등과 같은 보안 기능을 지원하는 게이트웨이를 설치해 인터넷에 접속시켜 준다. MPLS VPN은 인터넷과 별개의 MPLS 맵을 구성하여 서비스하므로 보안성이 좋고 QoS 보장이 가능한 장점을 가지고 있다.[8] 따라서 앞으로의 VPN 제품은 Intranet VPN과 Extranet VPN 기능과 더불어 MPLS VPN을 포함하고, 더불어 해킹이 대비되는 네트워크 보안 기능이 추가되어야 할 것이다. 향후 VPN 전용 장비보다는 집합 장비, IDS, Anti-Virus, 등과 같은 네트워크 보안 기능이 포함된 복합 보안 장비들이 주도하게 될 것이다.

대표적인 제품으로는 Nortel의 Contivity 시리즈, CoSine의 IPSec 시리즈, Quarry의 IQ 시리즈, Cisco의 VPN 7100 시리즈 등이 있다.

5. 침입탐지 및 침입방지 기술

최근의 침입탐지시스템(Introspection Detection System: IDS)의 기술은 네트워크 대역폭에서 동작하기 위해 처리 모듈의 하드웨어화 및 성능 개선 등의 고속 침입탐지 기술과 개발 노드에서의 장바가를 통합하여 전략적 네트워크 자원에서의 효율적인 침입 탐지 수리기 위한 사상 협력기술에 초점을 두고 발전하고 있다. 또한, DARPA(Defense Advanced Research Projects Agency)의 지원을 받은 SU(System Design Laboratory)는 EMERALD(Event Monitoring, Enabling Responses to Anomalous Lin Disturbance)라는 NIDES(Next-Generation Intrusion Detection Expert System)의 후속 시스템을 개발 중이다. EMERALD는 네트워크 기반의 침입 분석과 상호 안정성을 증가시키고 분산 컴퓨팅 환경에 맞는 침입방지시스템 개발을 목적으로 하고 있다.

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

침입방지시스템(Introspection Prevention System: IPS)은 공격에 대한 탐지만을 수행하는 기존 IDS의 한계를 넘어 공격 시그널을 찾아내고 비정상적인 행위에 대해 자동적인 실시간 대응 기능이 추가된 제품으로 차세대 IDS라고 불리
우리도 한다. Gartner에서는IPS가 2005년까지IDS 시장의 75%을 차지할 것으로 전망하고 있다. IPS는 기존의IDS에서 발생하는 False Positive(정상을 침입으로 오해하는 행위)를 어떻게 줄일 것인지가 중요한 이유이다.[10][11]
다음 표는 대표적인IPS 제품 등의 침입 탐지, 방지 및 대응 방식에 대해 비교 정리한 것이다.

<table>
<thead>
<tr>
<th>제품</th>
<th>기능</th>
<th>침입 탐지/방지</th>
<th>침입 대응</th>
<th>메커니즘</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network-I</td>
<td>- 자세 개발 MMD메커니즘</td>
<td></td>
<td></td>
<td>Patent-pending</td>
</tr>
<tr>
<td>Enterprise 2</td>
<td>- 시그니처 기반</td>
<td></td>
<td></td>
<td>네트워크 접속</td>
</tr>
<tr>
<td>Enterprise 3</td>
<td>- 프로토콜비정상형태</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TopLayer 4</td>
<td>- Forensic/ Aler 기반</td>
<td></td>
<td></td>
<td>Rate Limiting/Blocking 메커니즘</td>
</tr>
<tr>
<td>EZIS 5</td>
<td>- 시그니처 기반</td>
<td></td>
<td></td>
<td>패킷 헤더에 기반</td>
</tr>
<tr>
<td></td>
<td>- 요소 기반</td>
<td></td>
<td></td>
<td>호환성 검사</td>
</tr>
</tbody>
</table>

6. 정책 기본 관리 기술

정책 기본 관리 기술은 여러 보안 장비를 통합하여 관리하는 ESM(Enterprise Security Management)에서 적용되는 기술이 대표적이며, 국외보다도 국내에서 활발히 개발중인 시스템이다. ESM은 보안 정책을 수립한 후에 수릴 수 있는 보안 정책에 따라 구성하고 모니터링 및 신속한 조치를 위한 각종 경보의 기능을 제공하는 일련의 훈련된 워크플로우(Workflow)를 일관되게 지원하고 있다.[13]

ESM은 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 두며 복수이자. 이 범주에는 인증이나 Single Sign-On의 기능을 포함하는 경우가 많고, 초기 ESM 모델이 많이 반영되어 보안적 수준보다는 시스템 관리적 수준의 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 주요들은 가용성과 통합(Integration)이 활발히 진행되는 범주이다.

대표적인 국내 ESM 시스템으로는 이동통신사의 Secureworks ESM, 인스턴트의 NeoAdmin@ESM, 이글루의 SPIDER-I, 넷서커처 테크놀러지의 ActiveESM 등이고, 그 밖에 IBM의 Tivoli, Lucent의 LMSA, Arbor Networks의 Peakflow 등이 있다.

7. 결론

지난 몇 년간 네트워크 보안 기술에 대해서 크게 5 가지 기술로 분류하여 각 기술의 최신 개발 동향 및 관련 제품들 특성에 대해서 살펴보았다.

대표적인 리서치 기관인 Yankee Group와 Gartner의 자료의에 의하면 최근 네트워크 보안은 정책 기반 관리 방식을 중심으로 통합 제품으로 발전할 것이라 전망하고 있다. 또한, 네트워크 보안 장비는 고속한 전략적 처리 능력과 더불어 보안 기능을 가지는 형태와 타율의 기능은 훈련된 채 보안 기능은 전반적인 일련의 장비 형태를 함께 발전함으로 보인다.

따라서, 앞으로는 여러 보안 기능을 포함하고 있는 통합 보안 장비 또는 복합 보안 장비들이 점차 보편화되며 네트워크 보안 전용 장비들의 표준화된 정책 기반 방식을 도입하여 침입에 대한 경보 및 대응 방안을 서로 공유하여 난로 다양해지고 복잡해지는 사이버 위협에 대처할 것으로 예측된다.

참고문헌
searching=어메이트워크스&page=1
=13672&low=패키티어
=13136&low=패키티어
[9] 이용철, “VPN 기술 및 국내외 시장 동향”, 주간기술동향 1675 호,
2002,12,4