제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

차세대 네트워크(NGN)을 위한 네트워크 보안 구조 제안

오승희, 남택용
한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀
e-mail : (seunghee5, tynam,)@etri.re.kr

Proposal of Network Security Architecture for Next Generation Networks

Seung-Hee Oh, Taekyong Nam
Electronic and Telecommunications Research Institute, Information Security Technology Division, Network Security Architecture Research Team

요 약

현재 네트워크는 유• 무선이 통합되는 차세대 네트워크(NGN), 유비쿼터스 시대로 발전하고 있다. 현대인의 네트워크에 대한 의존도가 커질수록, 네트워크 취약점을 악용한 사이버상의 위협과 새로운 공격 유형이 급증하고 있다. 보다 안전하고 신뢰할 수 있는 네트워크 환경을 위해 다양한 보안 제품들이 등장하고 서로의 기능들을 통합하여 더 나은 보안 서비스를 제공하고자 노력하고 있으나, 기존의 대표적인 보안 제품들로는 그 한계가 있다. 따라서 네트워크 자체가 취약점과 공격을 받더라도 지속적으로 서비스를 제공할 수 있고, 빠른 보안 업데이트를 통해 네트워크 자체의 붕괴를 미연에 예방 가능한 새로운 네트워크 보안 구조가 요구된다. 본 논문에서는 차세대 네트워크 발전 방향에 적합한 네트워크 보안 구조를 제안하고, 제안하는 구조에서 네트워크 보안 시나리오를 제시하여 검증한다.

1. 서 론

인터넷이란 현대인에게는 하루 일과를 시작하고 마무리하는 핵심 매체라고 해도 과언이 아닐 만큼 일상 생활 속에 깊이 자리잡고 있다. 이처럼 인터넷을 통한 여러 가지 업무가 가능한 장점과 더불어 인터넷의 기본적인 보안 취약 구조로 인하여 개인의 정보가 쉽사리 노출되고 있고, 심지어는 네트워크 자체가 마비되는 1.25 대란과 같은 사건이 발생하고 있다. 즉, 인터넷이란 가상공간에서 발생하는 위협요소 및 범죄 행위들이 날로 다양해지고 복잡해지며 지능적으로 변해가고 있다.

개별적인 보안 제품(예: 항 바이러스 제품, PC 용 방화벽, 호스트 IDS, 등)의 설치나 통합 보안 제품들의 적용만으로 이러한 사이버 위협으로부터 안전하게 보호되기에는 한계가 있다. 이제는 근본적으로 네트워크 자체가 안전하고 신뢰할 수 있는 구조로 발전해야만 한다. 따라서 본 논문에서는 ALL IP 를 기반으로 하는 차세대 네트워크(NGN)를 위한 차세대 네트워크 보안 구조를 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서 현재의 네트워크 보안에 대한 관련 연구를 네트워크 보안 접근 방식에 따라 분류하여 다루고, 3 장에서는 제안하는 차세대 네트워크 보안 구조를 설명하고, 4 장에서는 제안하는 네트워크 보안 시나리오를 제시하여 본 구조를 검증한다. 마지막으로 5 장에서는 결론 및 향후 연구 방향에 대해서 논의한다.

2. 네트워크 보안 동향 연구

본 장에서는 네트워크 보안 관련 제품을 개발하는 업체를 분류하여 최신 동향을 분석해 보고, 이를 통해 현재 네트워크 보안 구조의 문제점과 한계를 살펴본다.

네트워크 보안 장비는 네트워크와 보안이라는 두 가지의 기능이 통합된 것으로, 보안 장비에서의 접근 방식과 네트워크 장비에서의 접근 방식이라는 주요 흐름과 고객 그룹별로 차별화된 high-touch 서비스를 제공하기 위해 새롭게 떠오르고 있는 IPSS(IP Service Switch)[1], 트래픽 흐름 분석을 통해 침입 탐지 및 예방을 지원하는 트래픽 제어 장비로 분류할 수 있다.

2.1 보안 장비 업체의 네트워크 보안 접근 방식

보안 장비 업체가 네트워크 보안 장비를 개발하는 대표적인 회사로는 FireWall-1 과 VPN-1 을 통해 높은 시장 점유율을 가지고 있는 Check Point 와 NetScreen-5000 시리즈로 firewall 과 VPN 기능을 통합한 NetScreen, RealSecure 시리즈의 ISS(Internet Security Systems), Entercept 와 Intrushield 를 통합하여 최근 McAfee 시리즈를 IPS(Intrusion Prevention System) 형태로 선보인 NAI(Network Associate) 등이 있다.

보안 전문 장비 업체들은 제품은 보안 성능 자체에 있어서는 뛰어난 기능을 지니고 있으나, 기존에 설치된 네트워크 장비와의 호환성과 네트워크 성능 저하라는 문제점으로 인해 ISP 로부터 크게 주목 받지 못하는 실정이다. 이를 극

복하기 위해서 네트워크 장비 업체와 파트너쉽을 맺고 있는 추세이다. 대표적인 예로 Nokia 는 Firewall 과 VPN 은 Check Point 사와 IDS 는 ISS 사와 파트너 관계를 맺고 있다[2].

2.2 네트워크 장비 업체의 네트워크 보안 접근 방식

네트워크 장비에 보안 기능이 추가된 경우 최대 장점은 ISP 와 같은 거대망 및 기업망에서의 주요 요구사항인 기존에 설치된 대부분의 네트워크 장비와의 호환 또는 대체가 용이하다는 것이다.

네트워크 장비 업체에서 네트워크 보안으로 접근하는 주요 업체로는 Cisco Systems 의 Catalyst 6500[3], Nokia 의 IP Series, Nortel Networks 의 Contivity 시리즈[4], Juniper Networks 의 J-Protect Security Solution 연계 제품 등이 대표적이다. 네트워크 장비 업체의 경우 보안 기능을 추가하기 위해 주요 보안 장비 회사와 파트너쉽을 맺거나, 합병 및 인수를 통해 자체적으로 보안 기술을 획득하여 자사의 주요 장비에 수용하는 방식을 사용하고 있다.

그러나 앞서 언급한 보안 기능을 가진 네트워크 장비는 네트워크의 성능을 저하시키지 않는 한도에서의 보안 기능만을 지니고 있어서 Firewall, VPN(IP VPN 과 MPLS VPN), ACL(Access Control List), Content filtering 정도만 제공한다. 따라서 침입 탐지 및 침입에 대한 동적인 대응, 침입으로부터의 네트워크 및 시스템 복구, Deep packet inspection 등과 같은 차원 높은 보안 기능이 미약하다.

2.3 IPSS 장비의 네트워크 보안 접근 방식

IPSS 는 트래픽 제어 기술과 Firewall VPN 등과 같은 네트워크 보안 기술이 통합된 제품으로는 현재 고속의 스위칭 기술을 제공함으로써 주목 받고 있는 제품이다. IPSS 제품의 주요 특징은 사용자 그룹별로 가장 적합한 IP 서비스를 고속으로 제공하는 것이다. 대표적인 제품으로는 CoSine 의 IPSX 9500™ Service Processing Switch[5], Quarry Technologies 의 iQ8000™ Service Edge Switch[6], Nortel Networks 의 Shasta 5000 BSN(Broadband Service Node)[7] 등이 있으며 Dacom, KT 와 같은 국내 주요 ISP 에서도 IPSS 제품의 설치를 고려 중에 있다.

IPSS 제품들은 ISP 망과 같은 거대망에 설치되어 만족할 만한 속도와 성능을 제공해주기 위해서 최소한의 네트워크 보안 기능인 Stateful firewall, VPN, ACL 등만 제공되며, 항 바이러스, 침입 탐지, 침입 방지, 복구와 같은 기능이 포함된 제품은 아직 없는 실정이다.

2.4 트래픽 제어 장비의 네트워크 보안 접근 방식

Layer 7 스위치와 같이 트래픽 흐름을 제어하는 장비에서 다량의 트래픽 폭주로 인한 네트워크 침입을 감지하고 이에 대응하는 방식의 네트워크 보안 접근이다. 주요 장비로는 Radware Application Switch III, Array Networks 의 Array 시리즈, Top Layer 의 Attack Mitigator IPS, Packereer 의 PacketShaper 와 PacketSeeker 등이 있다.

그러나 트래픽 제어 장비에서의 네트워크 보안 서비스는 deep packet inspection 과 같이 패킷의 payload 까지 살펴보고 침입 여부를 판단하여 3~4 계층 네트워크 보안 장비보다는 정확성이 높으나, VPN, 취약성 분석 등과 같은 서비스가 제공되지 못하는 한계성과 100Mbps 급 이하의 성능을 제공한다는 것이 단점으로 지적되고 있다.

3. 제안하는 차세대 네트워크 보안 구조

본 논문에서 앞서 살펴본 네트워크 보안 장비들의 동향을 통해 차세대 네트워크에 적합한 "차세대 네트워크 보안 구조" 를 제안한다. 제안하는 구조는 Access Network 와 Customer Network 을 위한 Security platform 과 Security Management System(SMS)로 구성되며, 제안하는 시스템의 보안 기능과 관리 기능을 중심으로 설명한다.

3.1 Security Platform for Access Network

Access Network 은 일반적으로 서비스 제공자가 관리하는 네트워크로 다양한 고객망과 연결된다. 따라서 고속의 트래픽을 처리할 수 있는 라우팅 기술과 함께 신속한 사이버 공격 및 위협 대처를 위한 정책 기반의 보안 관리가 반드시 요구된다.

그림 1 에서와 같이 보안 블록(Security Block)에는 보안 관리 시스템(SMS)과의 안전한 통신을 위한 SSL/TLS, SSH 가 제공되고, 전송되는 데이터의 안전성을 확보하기 위해 암호화 및 인증을 제공해주는 VPN 과, 이상 증후 트래픽을 차단하면서도 성능과 속도 측면을 고려한 Clustered Firewall 또는 패킷 필터링과 proxy 기능을 통합하여 가지고 있는 Stateful Firewall, 항 바이러스 기능, 그리고 Content filtering 을 제공한다.

관리 블록(Management Block)에서는 SMS 로부터 전달 받은 보안 및 관리에 대한 정책을 집행할 수 있는 Policy Enforcement Engine 과 새로운 관리 및 보안을 위한 정책들을 자동적으로 수용하기 위한 Update Engine 이 존재한다.

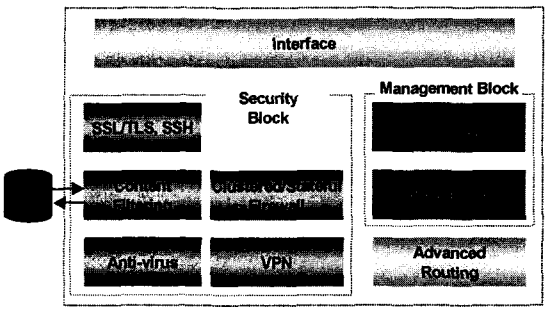

그림 1. Security Platform for Access Network 의 기능 블록

3.2 Security Platform for Customer Networks

Customer Network 은 Access Network 와는 달리 고속의 트

래픽 전송보다는 강력하고 안전한 보안 제공에 초점을 두고 있다. 따라서 보안 블록에서는 보안 관리 시스템(SMS)과의 안전한 통신을 위한 SSL/ TLS, SSH 가 제공되고, 전송되는 데이터의 안전성 확보를 위해 암호화 및 인증을 제공해주는 VPN 과, 이상 증후 트래픽을 차단하기 위한 Proxy Firewall, 데이터베이스와 접근 제어 리스트를 관리하는 Access Control, 그리고 MD5 Routing Authentication 을 제공한다.

또한, 관리 블록에서는 SMS 에서 생성된 보안 및 관리에 관한 정책을 집행하기 위한 Policy Enforcement Engine 이 존재한다.

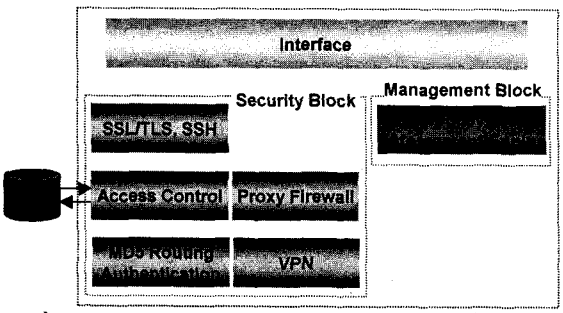

그림 2. Security Platform for Customer Networks 의 기능 블록

3.3 Security Management System(SMS)

Security Management System 은 서비스 제공자 망에 중앙 집중적으로 존재하여 Security Platform 에서 수행할 보안 정책을 생성, 결정, 관리하고 기존의 NMS(Network Management System) 시스템의 기본 기능을 포함하고 있다.

SMS 의 보안 블록에서는 Security Platform 과의 안전한 통신을 위해 SSL/TLS, SSH 를 지원하고, Role-based Access Control 을 통해 체계적으로 분류된 사용자의 권한에 따른 파일 및 시스템에 대한 접근 제어를 제공한다.

관리 블록에서는 기본 NMS 의 기능인 장애 관리, 구성 관리, 서비스에 대한 비용 청구를 위한 Accounting 뿐만 아니라 데이터베이스로 보안 및 관리용 정책을 생성, 결정 및 관리하고, 새로운 규칙 생성을 확인하기 위한 Rule Checking Engine, 성능 및 트래픽 흐름을 살펴보기 위한 모니터링 기능이 제공된다.

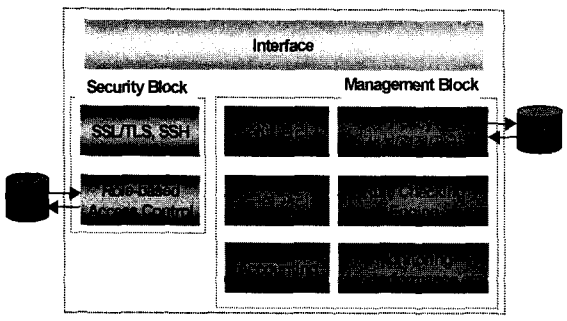

그림 3. Security Management System 의 기능 블록

4. 차세대 네트워크 보안 시나리오

본 논문에서 제안하는 차세대 네트워크 보안 구조를 바탕으로 구성된 네트워크는 그림 4 와 같다. 본 시나리오에서는 Attacker 가 다른 Customer Network 에 존재하는 특정 시스템에게 DoS(Denial of Service) 공격을 예로 제안하는 구조의 특징과 장점을 설명한다.

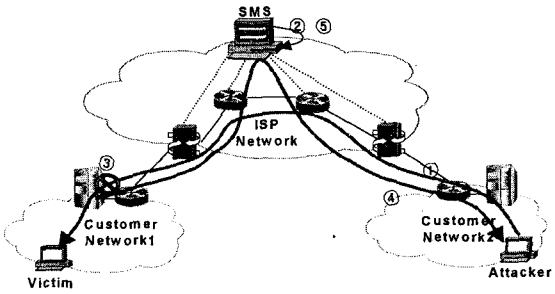

그림 4. 차세대 네트워크 보안 구조 시나리오

① Customer Network2 에 존재하는 Attacker 가 Customer Network1 에 있는 Victim 에게 DoS 공격을 시도한다.

② 이 경우, ISP 네트워크를 통과하는 전체 트래픽의 흐름을 모니터링하고 있던 SMS 가 특정 호스트에게로 향하는 과다 트래픽 발생 증후를 발견한다. SMS 는 이상 징후를 분석하고 기존의 정책 중 이러한 증후와 관련된 것을 찾아 보고, 만약 이와 관련된 정책이 없는 경우 새로 정책을 생성하여 대응 방식을 결정한 후 관리하는 모든 Security Platform 에게 안전하게 전달한다.

③ 모든 Security Platform(Access network, Customer network 포함)은 SMS 로부터 전달 받은 해당 정책을 Policy Enforcement Engine 을 통해 수행하고, 특히 Customer Network1 의 Security Platform 에서는 자신의 네트워크에 대한 공격이므로 우선적으로 보안 블록의 firewall 기능을 통해 유해 트래픽을 차단한다.

④ SMS 가 침입 정보를 분석한 내용을 바탕으로 Attacker 가 속한 네트워크를 역추적하여 유해 트래픽을 Customer Network2 에서 차단하고, SMS 는 다시 Customer Network1 의 blocking 을 해제하여 정상 기능으로 복귀시키라는 명령을 전달한다.

⑤ 그리고 Attacker 에 대한 정보 및 사용한 침입 유형을 분석하여 SMS 의 정책 관련 DB 에 업데이트한 후 지속적으로 관리한다.

위의 시나리오는 DoS 의 경우만 예를 든 것이나, DDoS (Distributed DoS), DRDoS(Distributed Reflected DoS)의 경우도 특정 호스트에게 집중하는 트래픽의 양이 폭주한다는 측면에서 유사한 정책을 통해 침입 탐지 및 대응이 실시간으로 가능하다.

따라서 제안하는 차세대 네트워크 보안 구조를 통해서 네

트워크 전체를 마비시키는 DoS 및 여러 DoS 변형 공격, 웜 바이러스로 인한 트래픽 폭주로부터 네트워크의 붕괴를 방지할 수 있다. 또한, SMS 를 통해서 새로 발견되는 모든 침입 유형에 대해 정책 기반 관리 방식을 사용하여 정책 형태로 각 Security Platform 에 실시간으로 전달 가능하므로, 이를 Policy Enforcement Engine 에 적용시켜 침입에 대한 네트워크 전체의 생존성을 강화시킬 수 있는 장점이 있다.

그리고 Security Platform for Access Network 의 Advanced Routing 을 통해서 네트워크 부하로 손상된 라우터가 존재할 경우, 새로운 경로를 빠르게 발견하여 다른 Security Platform for Access Network 에 전달 및 적용하여 트래픽의 중단을 예방할 수 있다.

5. 결론

본 논문에서는 갈수록 심각해지는 사이버 위협을 예방하고 차세대 네트워크의 발전 방향에 적합한 차세대 네트워크 보안 구조를 제안하였다.

제안하는 차세대 네트워크 보안 구조는 네트워크 자체의 생존성(Survivability)을 향상시킴으로써 네트워크 붕괴를 미연에 방지하는 형태로, 1.25 대란과 같은 대규모 트래픽 발생에서도 네트워크 마비를 예방 가능한 구조이다. 또한 본 구조는 개별 네트워크 보안 시스템들의 기능을 최대한 활용할 수 있도록 네트워크 환경을 조성해주는 장점을 가지고 있다. 안전한 네트워크 보안 구조만이 다변화, 다양화, 복잡화, 지능화되는 사이버 위협으로부터 네트워크의 안전성을 보장해 줄 수 있다.

본 논문에서는 제안하는 차세대 네트워크 보안 구조를 검증하기 위한 네트워크 보안 시나리오를 통해 DoS 뿐만 아니라 DDoS, DRDoS 와 같은 유형의 사이버 공격에서도 실시간으로 침입 탐지 및 대응을 효율적으로 할 수 있음이 검증되었다.

차후 연구로는 보안 위협에 대한 자동 업데이트 기능, 자체 복구 기능 및 편리한 관리 방식에 대해 지속적으로 이루어져야 할 것이다.

참고문헌

[1] David Ginsburg, Marie Hattar, "Implementing IP Services at the Network Edge," p131~167, Addison-Wesley, 2002
[2] http://www.nokia.com
[3] http://www.cisco.com/en/US/products/hw/switches/ps708/index.html
[4] http://www.nortelnetworks.com/products/01/contivity/index.html
[5] http://www.cosinecom.com/products/switches/index.html
[6] http://www.quarrytech.com/products/iq8000.shtml
[7] http://www.nortelnetworks.com/products/01/shasta/index.html