적응형 네트워크 보안시스템의 네트워크 접근제어 설계

김대식*, 박종률*, 노봉남*
*전남대학교 정보보호협동과정

Design of Network Access Control by Adaptive Network Security System

DaeSik Kim*, JongYoull Park*, BongNam Noh*
*Interdisciplinary Program of Information Security, Chonnam National University.

요 약

현재의 네트워크 시스템은 보안시스템 및 신규시스템이 추가됨에 따라 복잡함이 증가하고, 그에 따라 관리하기가 어려워져 관리자나 사용자가 이용하기에 불편함이 따른다. 또한 사용자의 잦은 변동과 단말의 이동성으로 인해 네트워크 관리하는데 있어 관리자가 해야할 일들이 많아졌다. 따라서 앞으로의 네트워크 관리도구는 복잡성을 해결하고, 사용자의 편의성에 중점을 두어야 한다. 이러한 요구사항을 정리하여 본 논문에서는 사용자에게는 보다 쉽게 사용하고, 관리자에게는 최소비용과 관리의 용이성을 위한 보안시스템을 설계하였다. 이 시스템은 신규 사용자의 네트워크 접속후 인증을 받기위한 부분에 있어서 리눅스 시스템과 네트워크 장비를 연동해서 관리자가 정책적용시 자동으로 ACL을 구성해 보안관리를 강화하는데 목적을 두고 설계하였다.

I. 서론

오늘날 IT기술의 급격한 발전과 인터넷을 이용하는 응용분야의 수가 급증함에 따라 네트워크에 대한 기술도 한층 더 발전하고 있다. 이러한 환경변화에 대응하기 위한 여러 가지 기술들이 연구되고 있는데, 그중 하나가 이 NGN(Next Generation 네트워크)이다[1].

그러나, 현재의 NGN은 실제망에 접속하기 위해서는 다년간의 테스트가 필요하며, 실생활에 적용하기 위해서는 많은 비용이 필요하다. 또한 사용자는 속도와 안정성을 필요로 하는 반면 기술이 기대에 부응하지 못해 사용자의 요구를 시기 적절하게 반영하는 것은 현재 어렵다. 따라서, 사용자의 요구에 실시간으로 대응할 수 있으며 새로운 기술 및 서비스를 즉각적으로 적용할 수 있도록 유연성과 능동성을 갖는 새로운 네트워크의 필요성이 대두되고 있다[2].

본 논문에서는 대규모 및 기업환경에서 적응형 네트워크를 구성하는데 있어 리눅스 환경에서 네트워크에 접속하는 사용자에 대해 차단 정책과 라우팅 설정을 통해 접근제어를 설계하는 데 목적을 두었다.

다음 장에서는 이와 관련된 기술들의 연구동향을 알아보며, 3장에서는 적응형 네트워크 접근제어 구현을 위한 설계를 설명한다. 마지막 결론에서는 적응형 네트워크의 발전방향과 필요성을 살펴본 다음 결론을 맺는다.

II. 적응형 네트워크 구조

2.1 적응형 네트워크 필요성

우리가 일반적으로 네트워크 보안이라 하면 네트워크를 통해 흘러가는 정보나 컴퓨터에 보관되어 있는 정보가 사용자의 과실이나 제 3자의 부정행위 등으로 의하여 손상되는 것을 방지하고, 정보와 사용자에 대한 신뢰성을 유지한다는 것을 의미한다[3].

최근의 데이타 및 각종 IT기술은 복잡 다양화 되어 보안공백이 관리자도 모르는 사이에 생겨나고 있다. 이러한 부분을 찾아내어 차단하고, 보완하는 것이 사용자 정보나 데이타를 보호하게 되고, 기업의 자산가치, 넓게는 국가정보의 보호를 하는 것이다. 그러므로 현대사회에 있어 보안은 생존경쟁에 있어 필수적이라고 할 수 있다. 항시 통신망을 이용하여 정보를 교환할 때에는 반드시 DATA를 암호화된 상태로 정보를 주고 받아야 안전할 수 있다.

지금의 네트워크 설정은 환경설정에 대한 이벤트가 발생할 시에 관리자가 일일이 수작업으로 환경설정을 수정해야 하는 수동형 네트워크이다. 수동적으로 환경설정을 하다 보니, 작업시간의 지연과 인재에

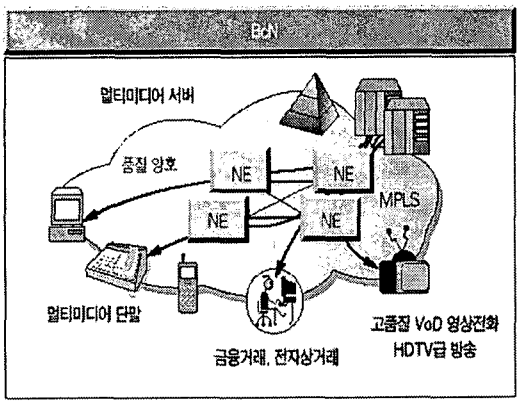
* 본 연구는 정보통신부 대학 IT연구센터 육성, 지원사업의 연구결과로 수행 되었습니다.

의한 장애, 변경이력관리 등이 부재, 미인지된 사고를 당하게 된다. 또한 보안관점에서 각 계층별 보안등급이 상이해야 하는 경우도 생기게 된다. 이러한 취약요소들을 보완하는 새로운 네트워크 개념이 바로 적응형 네트워크(Adaptive Network)인 것이다. 기업의 네트워크 환경이 직면한 비즈니스목적에 유연하게 적용할 수 있는 네트워크 인프라로 기존의 물리적인 내부망/외부망 개념의 획일적이고 경직된 네트워크 구조를 비즈니스 중심으로 그룹화(Compartment)시켜 각 그룹에 특화된 보안정책을 적용함으로써 네트워크 구조변경에 있어서 민첩성은 물론 대규모 및 기업환경의 보안강화도 동시에 할 수 있는 강점을 지니고 있다.

2.2 차세대 네트워크 기술

IT기술의 발전과 더불어 네트워크와 관련된 기술들도 많은 발전을 하였다. 이제는 기존의 관념처럼 케이블만이 네트워크가 아니라 작게는 무선부터 넓게는 BcN 까지 종합적인 개념으로 인식하고 있다.

[그림 1]은 BcN 네트워크의 구성을 나타낸 그림으로 End-User단의 접속장치를 한 눈에 볼 수 있다.



[그림 1] BcN 네트워크 구성

현재 차세대 통신으로 각광받고 있는 BcN 은 전화, 방송, 데이타 통신등 모든 통신 네트워크를 공통망으로 통합해 망 구축비용과 운영비용을 절감하고, 유연하고 개방적인 네트워크 솔루션과 다양한 어플리케이션을 제공하기 위한 통합망이다. 이 BcN 시대가 도래되면 생활에 있어서 많은 변화가 일어날 것으로 기대하고 있다.

이와 더불어 네트워크 인텔리전스 개념도 같이 부상하고 있다. 네트워크 인텔리전스란 기존의 네트워크 계층에서 벗어나, 어플리케이션 계층 측면에서 네트워크에 발생한 특정 작업을 식별하고, 또한 사용자의 개별적인 액세스 행위와 행동유형을 파악해 개인별 또는 그룹별 정책을 적용할 수 있는 능력으로 정의할 수 있다[4]. 이를 위해서는 사용자가 누구이고, 어디에서 어떤 장치를 통하여 사용하고 있고, 어떤 어플리케이션을 사용하며 무엇인지 파악할 수 있어야 한다.

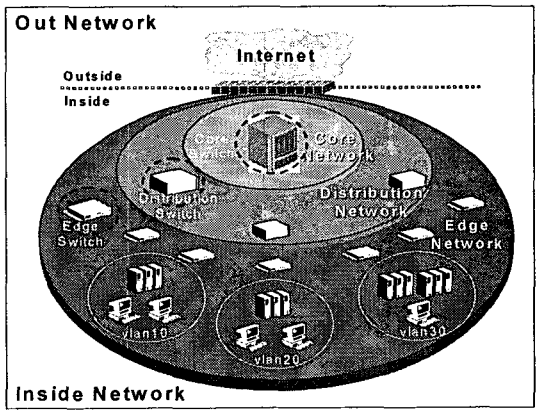
인텔리전트 네트워크 보안은 기업이 직면한 다양한 보안과 가용성의 문제를 정확히 인지하고 네트워크에 연결된 모든 장비가 성능을 최대한 보장할 수 있을 때 구현이 가능하며, 특히 어플리케이션 통합의 과정에서 직면하게 될 다양한 보안 문제를 정확히 이해하고 이를 극복할 수 있도록 기능을 적절히 반영하는 것이 중요하다.

이 네트워크 인텔리전스가 이 논문에서 다루고 있는 적응형 네트워크 개념과 유사하다. 사용자맞춤형 서비스를 제공하여 서비스 품질의 차별화와 정보보안강화를 유도하는 것이다. 하지만 이런 Infra를 통해 서비스를 이용하더라도 QoS부분이 고려되지 않는 다면 속도의 저하 및 생산성 저하로 사용자의 불만과 차세대 네트워크에 대한 믿음이 사라지게 된다. 현재 10Gbps까지 지원이 가능한 코어 보안 솔루션의 발표는 이러한 배경으로 나타난 것이라고 볼 수 있다.

2.3 네트워크 현황

지금부터는 우리가 현재 사용하고 있는 네트워크 Infra 구조와 보안이라는 측면에서 살펴보자.

[그림 2]은 간략하게 도식화하여 네트워크 구조를 나타낸 그림으로 다음과 같이 설명될 수 있다[5].



[그림 2] 네트워크 구성

(1) 물리적인 장비기반의 네트워크 구조로서 지역적이거나 그룹별로 서브넷(VLAN) 구성을 사용한다.

(2) 대규모 기업환경 표준 Infra 모델이 미비하여 신규 비즈니스 발생에 따른 네트워크 구조 변경에 어려움이 있다.

(3) 어떠한 사용자도 인증 절차없이 네트워크 접근이 가능하며, 사용자나 그룹별 네트워크 자원에 대한 사용권한 정책이 미비해 비인가 사용자에 의한 내부 보안위협이 존재한다.

(4) 기업이나 단체의 인수/합병, 기업의 분사등에 경직된 네트워크 구조를 가지고 있어 환경변경에 즉시성이 떨어진다.

(5) 외부 네트워크로 부터의 보안위협에 대한 차단은 집중되는 반면, 내부 네트워크의 보안에는 미비하

다.

(6) 무선이 확산됨에 따라 내부 네트워크의 보안위협에 노출이 심각하다.

(7) 부분별 보안이 아닌 전체적인 보안정책을 유지함으로서 보안관리에 있어 효율성이 떨어진다.

[그림 2]를 통해 네트워크 환경 및 보안이 얼마나 열악하고 취약한지 알 수 있었다. 이러한 취약성들로 인해 많은 Security Application들이 출시 및 연구되고 있다. 하지만 적절한 구성을 하지 못하면 이 또한 무용지물이 되며 시스템의 Cost만 올려놓는 상태로 남을 가능성이 높다. 이러한 부분을 좀 더 효율적이고 민첩하게 변경관리할 수 있도록 해야 한다.

2.4 업계 동향

적응형 네트워크에 대해 각 업계에서도 서둘러 제품을 출시하고 있다. 현재 HP의 ANA Product나 IBM의 ODNS, Sun, CISCO의 NAC, 3Com 등 기타 여러 보안업체가 관련 솔루션을 연구개발하고 있으며 발전시키기 위해 많은 노력을 기울이고 있다. 아래 [표 1]은 주요업체의 현황을 분석한 표이다.

	HP ANA	IBM ODNS	Sun
민첩성	기술적 표준화에 따른프로세스로 비용 효율적	장기적인 프로세스에 의존하며 긴 데이터분석 시간이 필요	컨설팅 파트너와 전문 서비스에 의존하여 비용과다
IT비용통제	고 객 비 용 50%개선	높은 TCO 필요	데이터센터의 TCO만 효과
서비스수준	변화속도에 보조자 역할	최근의 정책은 아직 평가중	Sun전용 N-1 정책기반관리
착수평가	고객이 직접 통제	IBM이 직접 통제	제3자시스템통합업체에 의존
관리능력	수많은 3rd Party 제품 수용	Tivoli 제품내의 ITIL인증	자체 플랫폼에만 적용가능

[표1] 주요 업체의 동향

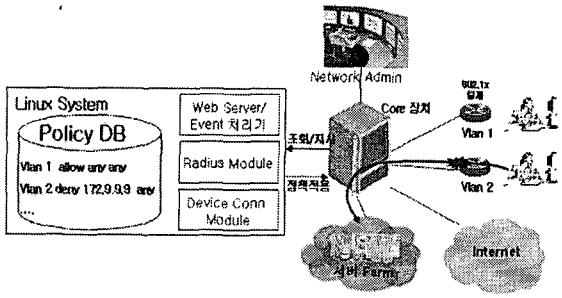
네트워크 전문업체인 CISCO나 3Com도 이에 발맞춰 적응형 네트워크 보안과 시스템 위협까지도 통제할 수 있는 솔루션을 내 놓고 있다. CISCO의 NAC 제품은 엔드포인트 보안인증(802.1x)을 바탕으로 지능적인 접속권한 여부를 결정하는 방식으로 구성이 되어있다. 3Com은 EMS라는 솔루션으로 시장에 뛰어들어 타사들과 경합을 벌이고 있는 실정이다.

III.적응형 네트워크 ACL 설계

2.3절의 네트워크 구성에서 가장 두드러진 특징은 외부보안은 누구나 다 보안에 대한 인식을 하고 있는데, 내부보안에 있어서 보안에 대한 관심은 상당히 취약하다는 점이다.

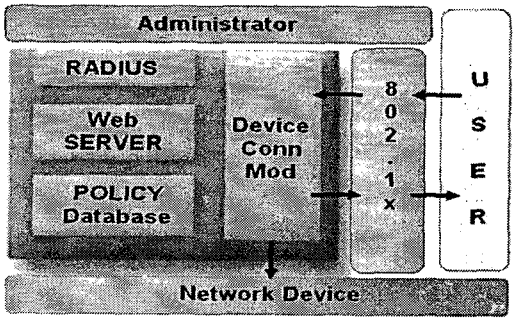
예를들어, 어떤 회사에 A라는 직원과 B라는 직원이 있다. A라는 직원은 인사팀 소속이고, B라는 직원은 일반 생산팀 소속이다. 어느날 B 직원이 해킹도구를 사용해 인사팀만 볼 수 있는 사내시스템에 접속을 하게 되었다. 회사 전체의 인사정보가 들어있는 중요한 시스템을 아무런 제약없이 접속을 한 것이다. 생산팀 직원은 생산라인과 관련된 시스템만 접속하면 되는데, 아무런 설정이 들어있지 않은 이 회사는 모든 직원이 모든 시스템에 접속을 할 수 있게 설정되어 있었던 것이다. 그렇다면 이 취약점을 어떻게 해결할 수 있을까?

다음과 같이 [그림 3]으로 표현할 수 있겠다.



[그림 3] 적응형 네트워크 설계

[그림 3]에서 알 수 있는 것은 네트워크 관리자가 정책적용이 가능한 접근통제시스템을 통해 해당 인가자의 네트워크 장치에 ACL(Access Control List)을 적용시켜 담당 시스템에만 접속할 수 있도록 허용하여 사내의 정보시스템을 보호할 수 있다.



[그림 4] 802.1x를 이용한 적응형 네트워크 구성

[그림 4]는 적응형 네트워크의 접근제어 설계를 802.1x를 이용하여 모델링한 그림이다. 향후 이러한 방법으로 네트워크를 관리한다면, 사용자별, 그룹별, Vlan별, 기타 등등 각각의 권한을 부여함으로써 내부망의 보안을 강화할 수 있다. 또한 각 권한별로 분류하면 트래픽 분석을 통하여 해당 그룹의 데이터 사용량이나 불필요한 트래픽 차단까지 할 수 있어 관리자 및 네트워크 어드민에게는 더 할 나위없이 좋은 시스템이다. 하지만 기본적으로 네트워크 구성이 하나의 Vlan으로 구성이 되어 있어야 한다는 전제하에 구현이 가능하다.

지금까지 시스템적인 관점에서 살펴보았다. 하지만 잘 구성된 시스템이라 하더라도 정책이 잘못 적용되어 있다거나, 관리가 제대로 되지 않는다면 소용이 없다. 능동적인 네트워크 보안을 위해서는 각 조직에 맞는 보안정책(Security Policy)를 수립하고, 각각의 구성원들이 강제적으로 이 보안정책을 따르도록 해

야 한다[6][7]. 또한 주기적으로 보안취약성을 검사하고, 만약 취약성이 발견되면 즉각 조치하거나 기타 다른 방법으로 보호해야 한다. 이렇게 보안을 해야만 정보보안 및 네트워크를 마비시키는 것을 방지할 수 있다.

IV. 결론

IT기술이 점점 더 발전함에 따라 보안이라는 새로운 화두가 탄생하였다. 이동성이 강조되고, 내부보안의 문제가 발생되고, 인터넷을 통한 보안위협을 받고 있는게 현실이다. 향후 BcN등의 핵심서비스 사업이 본격화 되면 적응형 네트워크에 대한 관심은 끝없이 높아질 것이다.

본 논문에서는 현재의 네트워크 보안의 취약점과 내부 사용자의 접근제어를 통한 보안의 취약점 대응, 그리고 앞으로 적응형 네트워크가 필요함에 대해서 살펴보았다.

국내에서 현재 구축되고 있는 광대역 통합망(BcN)과 같은 초고속 통합망 및 기간망 환경에서는 네트워크 자원이 여러 가지의 침입행위에 쉽게 노출될 수 있는 위협이 존재하며, 또한 네트워크 대역폭의 증가로 인하여 웜이나 바이러스의 확산을 가속화 시킬 수 있는 위험성을 내포하고 있다.

특히, PC 및 네트워크에 대해 관련 지식이 부족한 사용자 일수록 보안이라는 항목에 대해서는 무관심하기 때문에 모든 보안정책을 사용자가 쉽게 이해하고, 설정할 수 있도록 자동화되어야 할 필요가 있다. 자동화가 된다면 사용자뿐만 아니라, 관리자의 입장에서도 훨씬 더 업무의 생산성을 높이고 업무의 효율도 높아지게 할 것이다. 또한 적응형 네트워크 보안과 ESM을 연계시킨다면, 2중, 3중 보안시스템을 구성할 수 있을 것이다.

앞에서 서술되었던 취약성을 극복하고 보안을 강화하기 위해서는 아직은 미약하지만, 적응형 네트워크 보안이 활성화가 되어야 하며, 관련 업계나 연구기관에서도 통합망관리를 염두해 두고 발전시킬 필요가 있다고 생각된다.

[참고문헌]

[1] 능동망의 보안기술, 김종원, 김화종, June, 2002.

[2] 네트워크보안연구부, "차세대 인터넷을 위한 능동보안 기술 백서",한국전자통신연구원, 2001.

[3] "정보통신 보호를 위한 전자서명과 접근제어",이종근,최돈승,이경석, 정보통신논문집, 1998.

[4] 네트워크 인텔리전스로 구현하는 사용자 중심 서비스, 박홍근, On the Net, April, 2006.

[5] http://www.hp.com

[6] C.P. Pfleeger, "Security in Computing", 3rd Edition, Prentice-Hall International, 2002.

[7] 능동적인 네트워크 보안시스템 구축 (NCSC-TR050025), 국가사이버안전센터, Dec, 2005.

[8] 네트워크 보안 프로토콜, 윤종호, 교학사, Oct, 2004.

[9] http://www.cisco.com/kr

[10] http://www.3com.co.kr