情 報 保 護 學 會 誌
第18卷 第3號, 2008. 6

Network 基盤의 保安政策 管理모델 體系에 관한 研究 : 迅速性, 保安强化 側面의 管理모델

황 기 영*, 주 성 원**

요 약

기업의 Network 보안은 회사의 관문 방화벽에만 의존하고 있어 보안정책의 집중으로 효율성이 저하되고 이를 우회할 경우 심각한 위험에 노출될 수 있다. 본 연구는 신속성, 보안강화 측면에서 Network 보안 관리 모델을 제시하여 기업의 보안 수준을 강화하는 것을 목적으로 하고 있다. 따라서 기업 비즈니스 환경 변화를 배경으로 관련 연구 결과 및 Trend에서 제시하는 이론(802.1x 사용자 인증, Virtual Backbone 등)을 조사하고 이를 바탕으로 보안 강화 측면에서의 기업의 Network 구조와 보안정책 관리모델을 제시하여 이를 실제 기업 Network에 적용하여 얻어진 효과를 검증한다.

Ⅰ. 서 론

우리 나라는 세계 최고 수준의 인터넷 인프라가 구축되어 있고, 방송통신 융합, 유비쿼터스 등 Network의 범위와 사용성이 꾸준히 증가하고 있다. 따라서 그에 대한 역기능도 점점 증가하고 지능화 및 고도화가 되고 있는 실정이다. 대부분의 역기능은 개인정보보호 침해나 사이버 테러 및 범죄와 관련된 보안 분야에서 찾아볼 수 있다.[1] 최근의 보안위협은 단순한 재미 및 호기심 위주에서 벗어나 금전적 이득을 얻기 위한 직접적인 수단으로서의 성격을 띠고 있다. 특히, 특정 웹사이트에 금품을 요구하고 이에 불응 시 웹사이트 서비스를 마비시키는 분산서비스거부공격(DDoS) 등을 가한다든지 하는 사례가 다 수 발생하고 있다. 또한, 보안 취약점이 발견되고 이에 대한 대응책이 발표되기도 전에 해당 취약점을 악용하여 이루어지는 제로데이(Zero Day) 공격도 증가하고 있는 추세다. 제로데이 공격의 예로 2005년 11월에 WMF(Windows Meta File) 취약점이 처음 보고된 이후, 2006년 1월에서야 패치가 발표되었다. 최근 기업들은 내부보안 강화에 적극적으로 나서면서 Network 접근제어 솔루션을 비롯하여 데이터베이스 접근관리, 전자우편과 파일전송 보안, 문서 암호화, 출력물 보안, 개인정보 유출 및 방지 솔루션, 이동식 장치 보안 등에 관심이 높아졌다.

보안 위협의 특성이 고도화, 다양화, 스피드화 되고 유무선 등의 인프라 확산과 방통 융합 등 컨텐츠가 통합되면서 정보 자산에 대한 위험도는 그 어느 때보다 높다고 할 수 있다. 이에 반해 기업들의 대응 방안은 상대적으로 경직되어 있는 것이 현실이다. 대부분의 Network 보안을 기업 관문 방화벽에서 담당하고 있어 상황에 따라 급변하는 시장에서 살아 남아야 하는 기업의 입장에서 기업환경 변화에 능동적으로 대처할 수 있는 보안구조와 정책 등이 절실한 상태이다.

이에 본 연구는 비즈니스 환경 변화에 신속히 대응할 수 있는 Network 보안관리 체계 방안을 제시하여, 문제 발견에서 실시간 구성변경, 즉각적인 보안정책 적용 등 기업의 보안수준을 강화하는 것을 목적으로 한다. 따라서, 이를 제시하기 위한 Network를 논리적으로 구분하는 논리적 그룹화 및 사용자 단(End point) Security의 기법인 802.1x 사용자 인증 개념을 이용하여 기업에서의 Network 구조 보안모델을 제시하고 적용 사례를 들어 효과를 분석하고자 한다.

Ⅱ. 기업 비즈니스의 환경 변화

현재까지 기업 Network에서 중요한 것은 비즈니스를

* 삼성SDS 정보보안센터 (kiyoung.hwang@samsung.com)
** 삼성네트웍스 품질보안팀 (sw71.joo@samsung.com)

제대로 운영할 수 있도록 Network 제품(Devices 및 솔루션)의 가용성 및 성능에 초점을 맞추고 있었다. 하지만 이제는 이러한 환경 구축은 기본이고 Network가 Network로 끝나는 것이 아니라 비즈니스를 지원하는 가장 기본적인 단위로서 환경변화에 대처할 수 있는 신속성이 대두되고 있다. 뿐만 아니라 최근의 기업의 정보보호는 외부로부터의 침입보다는 내부자의 정보유출이 더 크게 위협하고 있어 내부 Network 및 사용자 영역에서의 관리가 점점 더 중요해지고 있는 실정이다.

Network 인프라의 조건으로 신속성이 요구되는 이유는 빈번한 조직변경 발생, Mobile 환경 요구, Collaboration 비즈니스 발생, 회사 내부 보안 취약성 상존, 신속한 해킹 및 바이러스 차단 요구, 회사 관문 방화벽 운영 복잡성 증가 등이 있을 수 있다. 이외에도 기업 구조가 변화하면서 다양한 보안 이슈가 발생할 수 있다. 다양한 협업 사용자들이 증가하면 내부 Network에 대한 통제 경우의 수가 증가한다. 따라서 관리해야 할 포인트가 늘어나면서 결국, 보안 취약성도 증가할 수 있는 것이다. 결국 취약성이 증가하면 다양한 경로로 유해 트래픽이 유입되어 전체 Network에 영향을 줄 수 있다. 피해뿐만 아니라 원인을 제거하는데도 상당한 리소스가 할당되어야 한다. 또한, 관문 방화벽 위주의 보안 정책은 다양한 환경 변화에 대해 관리해야 하는 Rule을 수시로 추가 또는 변경해야 한다.

그러나 대부분의 회사는 기존의 보안정책을 유지하거나 강화하는데 경직된 물리적 및 지리적인 Network 구조, 방화벽에 보안 정책이 집중된 구조, 표준에 의한 관리 보다는 담당자에 의존한 정책 관리 등 한계점을 갖고 있다. 이를 해결하기 위해서는 기업의 IT 환경변화를 보장할 수 있는 구조, 사용자 권한별 Network 접근제어가 가능한 보안체계, 보안정책의 통합관리 및 신속한 적용체계 등의 요구가 충족되어야 한다.

Ⅲ. 관련 연구

Network 보안관리 방법인 ACL, VLAN, 802.1x 사용자 인증, NAC, HP의 ANA 등을 살펴보고 장.단점을 알아본다.

3.1 ACL(Access Control List)

ACL은 시스템 자원에 특정 사용자의 특정 Protocol만을 허용 또는 차단하여 시스템을 불필요한 트래픽으로부터 보호하는 기능으로, Network 관리자가 정의한 기준에 따라 Switch, Router 등 Network 시스템이 특정 패킷을 차단하거나 통과 하도록 하는 방법이다.

ACL을 적용하는 방법에는 Standard Access List와 Extended Access List가 있다. 정책 적용 시 Standard Access List는 Source Network, Wild Card Mask만을 고려하여 통제하며, Extended Access List는 Source와 Destination Address, Protocol, Service Port를 고려하여 적용 여부를 결정한다.[2]

ACL 정책 선언 방법은 일반적으로 다음의 순서와 같다. 좁은 범위와 빈번한 트래픽을 발생하는 정책을 먼저 선언, 선언문의 마지막에는 전체 차단 "deny any"가 포함되므로 모든 트래픽을 차단, 모든 트래픽을 차단하고자 않는다면 "permit any"를 마지막에 정의, 여러 줄에 선언을 하였을 경우 임의의 행과 행 사이를 수정할 수 없음, 해당 리스트 번호에 추가하는 것은 모두 마지막에 추가됨, 동일한 Access List Number를 선언할 때는 차례로 전부 선언해야함 등의 절차에 따라 적용한다.[3]

3.2 VLAN(Virtual LAN)

VLAN이란 물리적으로 동일한 Switch Network를 논리적으로 분할 한 것을 말한다. 여기서 동일하다는 의미는 한 Switch 포트에서 만들어진 브로드캐스트 프레임이 도달하는 모든 Network 이라고 볼 수 있다. VLAN을 설정하지 않았거나, Router에 의해서 분리되지 않은 Switch Network에서는 한 포트에서 발생한 브로드캐스트가 동일 Switch뿐만 아니라 다른 Switch로도 전송된다. 최근 업무에 Network 의존도가 높아지고, 트래픽이 많아지며, 보안에 대한 요구가 늘어남에 따라 대부분의 Switch Network에서 VLAN을 사용한다.[4]

서로 다른 VLAN에 접속된 장비들은 Router를 통해서만 통신이 가능하다. 이 때 Router를 통과하는 트래픽에 대해 Router에서 다양한 보안정책을 적용함으로써 VLAN으로 분리된 Network의 보안성을 강화할 수 있다. 즉, VLAN은 Network 자원의 접근을 제한함으로써 보안을 향상시키고, 브로드캐스트 도메인의 크기를 줄여서 브로드캐스트 트래픽 양을 줄이는 효과가 발생하고 결과적으로는 전체 Network 성능을 보다 향상 시킬 수 있다.[5]

VLAN을 구성하는 방법은 여러 가지가 있다. Switch

의 포트 기준, 디바이스들의 MAC 주소 기준, 사용자가 정의한 IP 주소, Protocol, 응용프로그램별로 VLAN을 구성할 수 있다.

3.3 802.1x 사용자 인증

802.1x 표준은 기존의 PPP(Point to Point Protocol) 인증 Protocol를 응용하여 개발된 포트 기반의 접근제어 Protocol을 말한다. 802.1x의 주요 구성요소에서는 Supplicant(접속요구단말), Authenticator(인증자), Authentication Server(인증 서버)가 있다. Supplicant는 망에 접근하려는 PC 등 단말사용자로 무선인 경우에는 무선 단말이 해당된다. Authenticator는 Bridge, Switch, AP (Access Point) 등 망 접근을 제어하는 시스템 인증 교환은 Supplicant 및 인증 서버 사이에서 이루어지고, 인증자는 가교 역할을 하는 Authentication Server는 RADIUS 서버 등 인증 서버가 담당하게 된다. Authenticator는 Authentication Server의 클라이언트이며, 일단은 비 제어 포트(Uncontrolled port)에 접속한 후에 인증이 성공하면 제어 포트(Controlled Port)를 이용하여 데이터를 전송할 수 있게 된다.[6]

인증은 Switch, Bridge, AP에서 포트 단위로 인증을 수행하여 포트 단위로 개별적인 사용 제한, 대역 할당 등 제어가 가능하다. 단말은 인증 이전에는 제어되지 않은 포트를 이용하며, 인증 이후에는 제어된 포트를 이용하게 된다. 단말 인증 보다는 사용자 인증 위주이며 키 분배 등 키 관리 기능은 고려되지 않았다.[7]

주요 구성 Protocol은 기존에 존재하던 다양한 인증 Protocol들을 활용하도록 권고하며, 인증 방식에는 One Time Password, Transport Layer Security, Token Card가 사용된다. 인증용 Protocol에는 EAP (Extensible Authentication Protocol), PAP (Password Authentication), CHAP (Challenge Handshake Authentication Protocol) 등이 있으며 기본으로 EAP (Extensible Authentication Protocol) 사용을 권고한다. 한편, EAP Protocol은 어떤 인증 Protocol과도 결합이 가능하여 이는 인증 및 키 관리를 위한 일종의 뼈대를 형성하나 특정 인증 Protocol은 아님을 의미한다.[8]

3.4. NAC(Natwork Access Control)

최근에 Network 보안시장에 새로운 화두가 되고 있는 NAC는 사용자 PC가 내부 Network에 접근하기 전에 보안정책을 준수 했는지 여부를 검사해 Network 접속을 통제하는 기술이다. 핵심은 사용자 단의 보안기술을 기존 Network 보안체계와 결합해 기업 전체 Network에 통합보안체계를 구현하는 것이다. 따라서 NAC 기술은 궁극적으로 확산되는 보안위협 경로를 미리 차단해 사전 방어적인 Network 보안체계를 구현하는 것을 목적으로 한다.

사용자 단의 보안기술과 통합해 기업의 보안정책을 관리하는 이 모든 프로세스를 자동화해 시스템화 하는 것이 NAC Framework Architecture이며, 이를 구현하는 것이 NAC 솔루션이다. 사용자 접속을 허가, 통제하기 위해서는 먼저 사용자 PC가 인가된 장치인지, 사용자 PC에 기업의 보안정책이 제대로 구현되어 있는지 확인해야 한다. 예를 들어 PC에 보안 패치나 안티바이러스가 최신 버전으로 설치되어 있는지 Network 접속 이전에 점검해야 하기 때문에 사용자 단의 보안체계를 통합 관리하고 보안정책을 일괄 적용할 수 있는 조건을 제공하게 된다.

NAC 솔루션은 일련의 인증과정을 거치며, 이를 살펴 보면, 먼저 Network에 접속하는 PC사용자가 신원이 확실한 사용자인지 확인(인증)하고, 사용자 PC의 보안 상태(OS 패치, 백신 패치, 필수 S/W 설치)가 적절한지를 점검한다. 그리고는 이 두 결과에 따라 내부 Network에 접속하도록 허용하거나 거부 또는 격리한다. 보안정책이 제대로 준수되어 있지 않거나 바이러스에 감염되어 거부 또는 격리된 PC는 필요한 정책 적용, Software 설치 및 치료 과정을 거쳐 다시 점검하는 과정이 이루어진다. 최종적으로 접속이 허락되면 사용자 그룹별로 적절한 ACL이 할당되어 사내 Network에 접속되어 있는 동안 지속적으로 관리 및 모니터링이 되어진다. NAC는 기존에 Switch에 802.1x 사용자 인증 기능이 구현된 Switch 기반의 NAC, 그리고 Switch에 사용자 인증이 없어 별도의 Controller를 사용해야 하는 Controller 기반의 NAC 두 가지 종류가 있다.

3.5 HP ANA(Adaptive Network Architecture)

현재의 Network 환경 설정은 Network에 대한 이벤트가 발생하면 관리자나 운영자가 일일이 수작업으로 환경 설정을 수정해야 하는 수동형 Network이다. 관리자가 수동으로 환경 설정을 하다 보니 작업시간의 지연

과 인재에 의한 장애, 변경 인력관리 어려움, 미 인지된 사고를 당하게 된다. 또한 보안관점에서 각 계층별 보안 등급이 상이해야 하는 경우 기존 Network 구성을 바꿔야만 하는 경우도 생기게 된다. 이러한 취약 요소들을 보완하는 새로운 Network 개념이 바로 ANA이다.[9]

ANA의 구현 단계는 Architecture 설계를 위한 기업 비즈니스 및 IT인프라 분석 단계, 비즈니스 요구에 맞게 Compartment 정의 등의 Architecture Design 단계, ANA Deploy를 위해 ANA 물리적 인프라의 분석 및 기술적 설계 단계, 전 단계에서 수집하고 정의한 Policy 및 Rule을 통해 설계 ANA를 구현하는 단계, ANA Architecture가 구현된 네트워크 운영관리 단계 등 크게 5단계로 나눈다.

ANA 도입에 따른 장점으로는 내부 및 외부 사용자 또는 Application을 물리적 위치가 아닌 Access 수준에 따라 그룹화할 수 있으므로 감사와 추적을 빠르고 쉽게 실행할 수 있는 보안성이 향상된다. 또한 중앙집중식으로 관리하므로 비즈니스와 보안을 이유로 Network를 재구성하는 경우 시간이 적게 소모되어 유연성이 강화된다. 반면에 단점으로 개별적인 보안 Application들의 연계가 필요하고, 비 표준화 장치를 미 지원하며, HP 고유의 유닉스 시스템이나 리눅스 시스템에 기반 한다는 점에서 OS 그 자체가 고가일 뿐 아니라 상용 제품이기 때문에 유지비용도 고가이다.

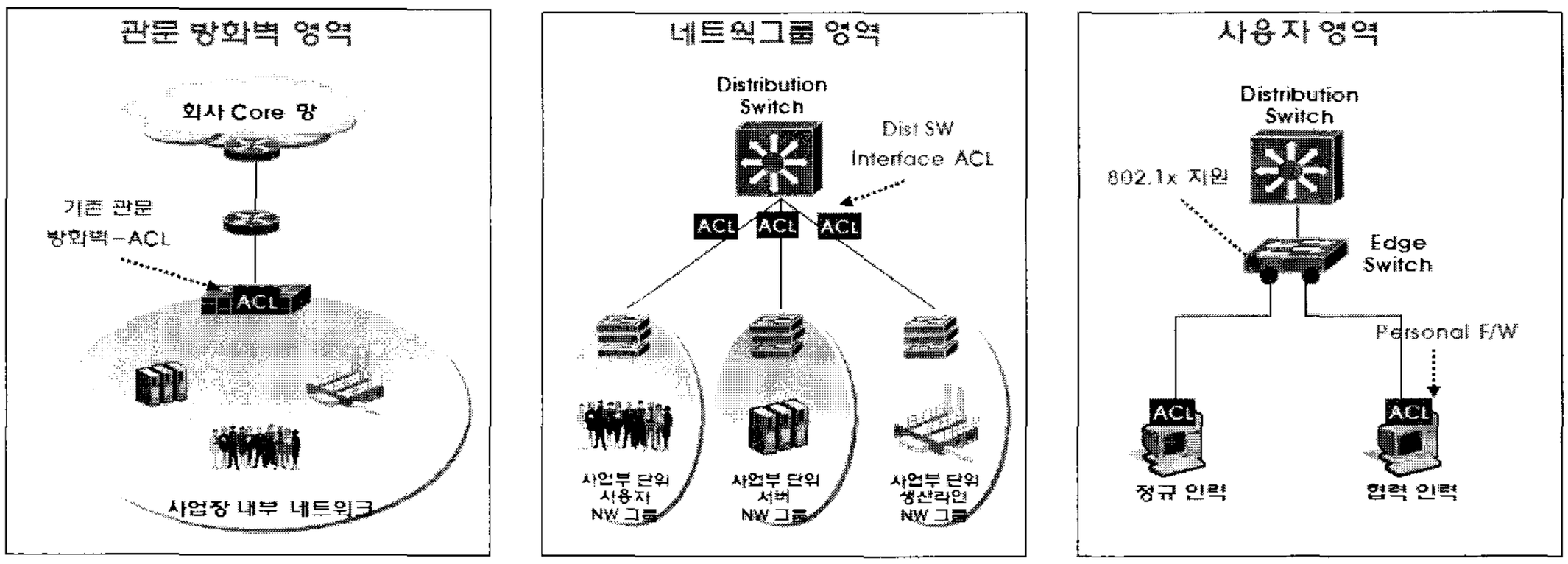
Ⅳ. Network 보안관리 모델

기업 비즈니스 환경변화에 신속히 적응할 수 있는 Network 구조와 보안 강화 측면에서 다 계층 Network 보안 구조와 정책을 제시한다. 다 계층 보안 구조는 기존에 관문 방화벽에서 담당했던 단일 보안 영역을 관문 방화벽 영역, Network 그룹 영역, 사용자 영역으로 분산하여 보안 위협을 분산하고자 하는 체계이다. 이 것은 기존의 기업 Network가 관문 방화벽에만 보안이 집중되어 있는 것에 반해 여러 계층에서의 보안 제어를 통해 외부 침입을 어렵게 하는 한편, 내부 침해 및 보안 피해를 특정 범위로 제한할 수 있어 한층 보안이 강화된 구조라 할 수 있다.

일반적으로 기업 Network 구조를 3가지로 구분할 수 있을 것이다. 관문 방화벽부터 각 사업장 Distribution Switch까지의 영역을 관문 방화벽 영역, 각 사업장 Distribution Switch에서 사용자 Edge Switch까지의 영역을 Network 그룹 영역, Edge Switch에서 사용자까지의 영역을 사용자 영역으로 구분한다.

다 계층 보안 구조의 핵심은 전체 기업 Network를 하나의 가상 백본을 중심으로 연결된 다양한 논리적 그룹을 구성하는데 있다. 본 연구에서는 Network 그룹 영역에 논리적 그룹 적용을 제시한다. 논리적 그룹이란 물리적, 지리적 위치에 상관없이 수행 기능 및 업무 성격별로 구분된 그룹을 말한다. 서울 사무소에 있는 사용자가 부산 사무소에 있는 사용자와 동일한 역할과 직무를 수행한다면 이들은 동일한 논리적 그룹으로 묶을 수 있고, 동일한 사설 서브넷(Sub Network)에 있는 것 처럼 구성될 수 있다. 이러한 논리적 구분은 물리적인 경계화는 무관하며 가상 백본(Virtual Backbone)이라는 논리적 백본에 연결된다.

논리적 그룹으로 변경하는 과정을 예를 들어 제시 하고자 한다. 서울과 부산에 IT 백본을 갖고 있고, 광주,



〔그림 1〕 다 계층 보안 구조 영역별 주요 기능

부산, 해외에 지사를 두고 있으며, 각각의 지사에는 Customer, Supplier, Dealer그룹 등이 연결되어 있는 물리적 구성를 가진 기업이 있다. 이를 지역별로 기능별로 논리적인 구성으로 그룹화 하는데, 이 때 기능을 구별하는 요소로는 기업의 비즈니스 유형, 지역, 조직, 내부 및 외부, 독립성, 중요도, 기반 인프라, 관리방법 등이 있을 수 있다. 이 회사를 논리적 구성으로 정리하면 Customer, Supplier, Dealer, Branch Office(서울 본사, 부산 지사), Internet, Intranet, IT System 7개로 구성할 수 있겠다.

다 계층 보안 구조에서 계층별로 보안 정책을 관리하는 방법은, 관문 방화벽 영역에서는 사업장 외부에서 내부로 Inbound 되는 트래픽에 대한 기존 보안 제어를 유지하고, Network 그룹 영역에서는 각 그룹 별로 Distribution Switch Interface에 양방향 트래픽에 대해 ACL(Access Control List)를 설정하여 접속을 제어하며, 사용자 영역에서는 Edge Switch에 802.1x 등의 사용자 인증 구현을 통한 접속 제어와 동시에 사용자 PC에 개인 방화벽 등을 이용한 ACL 설정 및 보안 프로그램 등의 소프트웨어를 통해 유해 트래픽을 원천적으로 차단하는 등의 역할을 담당한다. [그림 1]은 다 계층의 구조와 역할을 개략적으로 설명한 것이다.

4.1 방화벽 및 Network 그룹 영역 보안 정책

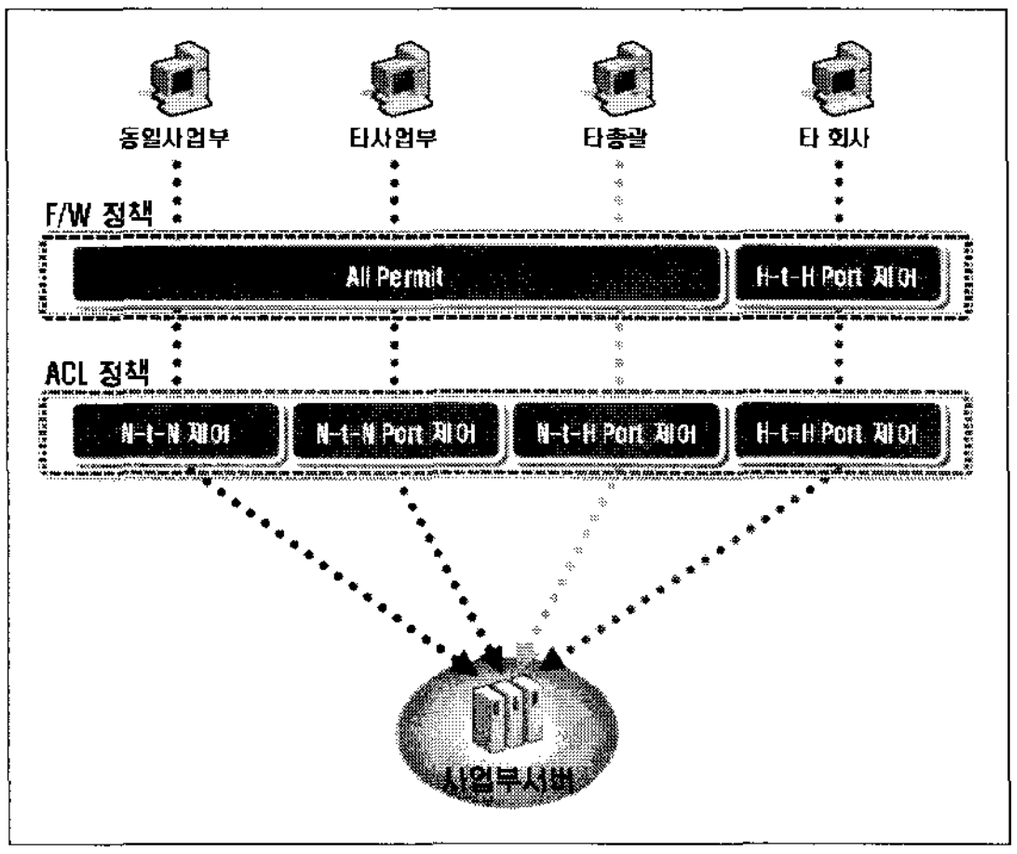
다 계층 보안 구조에서 제안하는 방화벽의 물리적인 구조는 기존 구조와 크게 다르지는 않지만 Rule의 구성은 기존에 Host-to-Host 기반에서 Network-to-Network 기반으로, 다수의 Rule에서 소수의 Rule 구조로 변경한다. 거시적인 관점에서의 Rule은 관문 방화벽에서 담당하고, 기능 그룹별로 내부 시스템 및 외부 인터넷 접속에 대한 제한을 Network 그룹 영역에서 수행한다. 기존 Network 구조의 경우 모든 사용자로 부터 시스템으로의 접근통제는 Host 기반 방화벽 Rule을 통해서만 적용하였지만, 다 계층 보안 구조에서는 방화벽과 Network 그룹 영역의 Switch의 ACL을 동시에 활용하여 방화벽의 부담을 줄일 수 있다.

보안 정책은 방화벽 영역에서 방화벽에 등록된 정책 대부분의 Rule이 Network 그룹의 ACL로 설정되어 있어 사업장이나 사업부 고유의 정책 또는 사업장 내부의 여러 사업부에 공통되는 정책만을 적용할 수 있게 된다. 또한, 외부에서 내부 Network로 유입되는 유해 트래픽 제어를 주요 목적으로 Rule를 설정한다. Network 그룹 영역은 Network를 논리적 그룹으로 분류하고 Distribution Switch에 그룹별로 IP 기반의 VLAN을 할당한다. VLAN이 결정되면 각 Distribution Switch에 해당 VLAN별로 ACL을 일괄적으로 적용한다.

A회사를 사례를 들어 방화벽과 Network 그룹 영역의 보안 정책 적용을 설명하겠다. A회사의 조직 구조는 총괄, 사업부, 부서로 구성되어 있다. 서버에 접속하는 사용자는 동일 사업부에서 접속하는 경우, 타 사업부에서 접속하는 경우, 타 총괄에서 접속하는 경우, 그리고 타 회사에서 접속하는 경우로 구분할 수 있다. 이 때 사용자들은 Trust 그룹, Distrust 그룹으로 나눌 수 있는데 Trust 그룹은 동일 사업부, 타 사업부와 같이 동일 총괄 내 모든 사업부의 사용자로 구분하고, Distrust 그룹은 타 총괄 및 타 회사 사용자로 구분한다. 즉, 동일 총괄 내 사용자는 Trust 그룹으로, 이외의 사용자는 Distrust 그룹으로 나누는 것이다. 이 때 보안 정책은 방화벽의 경우 Trust 그룹은 모두 허용(Permit) 해주고 Distrust 그룹은 타 총괄의 경우 모두 허용을, 타 회사의 경우

〔표 1〕 방화벽 및 Network 영역의 보안 정책

영역		적용 정책
방화벽 그룹 영역	Trust	All Permit
	Distrust	(타 총괄) All permit (타 회사) Host-to-Host 제어
Network 그룹 영역	Trust	Network-to-Network 제어
	Distrust	(타 총괄) Network-to-Host 제어 (타 회사) Host-to-Host 제어



〔그림 2〕 다 계층 보안 구조 영역별 주요 기능

Host-to-Host 제어를 하게 된다. 또한, Network 그룹 영역의 Trust 그룹은 Network-to-Network 제어를, Distrust 그룹은 타 총괄의 경우 Network-to-Host, 타 회사의 경우 Host- to-Host 제어를 적용한다. 지금까지 설명을 [표 1]로 정리하였고 [그림 2]는 이를 그림으로 표현한 것이다.

4.2 사용자 영역 보안 정책

사용자 영역에서 이동성을 강화하고 비 인가 사용자에 대한 접근을 통제하기 위해 802.1x 기반의 사용자 인증과, 인증을 득한 사용자에게 동적으로 IP를 할당하는 DHCP 적용 방식에 대해 설명하겠다.

현재의 IP 주소 부여 방식은 사업장 및 부서 등 위치에 따른 체계로서 네트워크 접근 통제가 불가능 하므로 비즈니스 및 위치 중심의 IP 주소 체계로 변경하게 된다. IP를 할당하기 위해서는 사전에 IP 주소 체계를 수립해야 하는데 대역별로 일반 사용자, 출장자, 협업 사용자, Guest 사용자로 좀 더 세분화가 가능하다. 예를 들면 A부서의 IP 주소 부여 체계는 [표 2]와 같이, 일반 사용자의 경우 C Class의 1부터 213까지를 부여하고 출장자, 협업 사용자, Guest 사용자는 그 이후인 232부터 254까지를 부여 하였다.

사용자 인증 과정은 생산라인의 개발 장비, 프린터나 팩스와 같은 사무용 장비, 기타 특정한 목적을 위해 사용자 인증이 필요하지 않은 경우 고정 IP를 부여하고, 이외의 사용자에게는 단계별 과정을 거쳐 IP Address를 할당하게 된다. 단계별 과정은 사용자는 Network에 접속하여 인증 요청, Network는 인증서버에 인증을 요청, 인가 사용자 여부 판단 및 최신 패치나 백신 소프트웨어 설치 확인, 인가된 사용자가 Network 장비에 IP 요청, Network 장비는 DHCP 서버에 IP 요청, 해당 DHCP 서버는 중계 Router의 그룹 정보를 확인하여 그룹화로 미리 설정된 IP 대역의 IP 를 할당하는 과정을 거친다.

〔표 2〕 IP 주소 부여 체계

구분	IP Address	사용 개 수
일반사용자(동일 사업부)	X.1.1.0 ~ 231	232개
출장자(타 사업부)	X.1.1.232 ~ 239	8개
협업 사용자	X.1.1.240 ~ 247	8개
Guest 사용자	X.1.1.248 ~ 255	8개

사용자 인증과정에서 사용자 인증정보는 논리적인 그룹인 사용자 그룹과 DHCP Relay Router의 그룹 정보를 비교하여 결정하게 된다. 예를 들면, 인가된 사용자의 해당부서 사용자라면 해당부서 일반 사용자용 IP를 할당해 주고, 인가된 사용자의 협업 사용자라면 소수 협업 사용자용 IP를 할당하게 된다. 특히, 사용자 인증의 특징으로 사용자 인증과 무결성 체크가 완료된 후 해당 사용자 중 접근제어가 좀 더 세분화될 필요가 있는 사용자에 한해 사용자 ACL을 할당하게 된다.

사용자 영역에서는 Edge 단에서 내부로의 보안을 주요 목적으로 정책을 설정할 수 있다. 일반 사용자의 경우 인터넷, 사업장 공통 서버 팜(Sever Farm), 회사 서버 팜, 사업부 서버 팜 접근을 허용하고, 출장자의 경우 인터넷, 사업장 등의 서버 팜을 접근할 수 있도록 보안 정책을 설정하지만, 협업 사용자 및 방문자의 경우 내부 사용자가 아니기 때문에 별도의 사용자 ACL을 추가로 PC에 설정해 주도록 한다.

V. 구현 사례 및 효과

지금까지 제시한 다 계층 보안 구조와 보안 정책을 기업 Network에 적용하여 얻어진 개선 효과를 검증하고 이를 설명한다.

5.1 구현 사례

5.1.1 구현 환경 및 장비

효과를 검증하기 위해 <가 사업장>의 Network 구성 현황을 소개하겠다. <가 사업장>의 백본은 이중화되어 있고, '가동'과 '나동'으로 이루어져 있으며 서버 팜에는 다수의 개발 서버가 존재한다. 자세한 네트워크 및 장비 현황은 [표 3]과 같다.

A회사 Network 체계에서의 이슈사항은, 사업장 내에서 A회사와 협업 사용자 Network이 구분 없이 사용되고 있으며, 대규모 조직 변경이 연 1 ~ 2회 발생하고 있어 방화벽 Rule 변경 작업 업무가 과중하게 발생하고 있고, 출장자 등 사용자 이동으로 사용자 IP 변경 관련 작업이 수시로 발생하고 있다. 또한, 신규 Application 도입 및 변경 시 매 번 방화벽에 Rule 생성이 발생하고 있다. 이를 개선하기 위한 방안으로 본 연구에서 제시한 사용자를 논리적으로 그룹화하고, 사용자 인증을 적용하였다.

〔표 3〕 〈가 사업장〉 Network 및 장비 현황

구분	세부 내용	수량
방화벽	관문 방화벽	2대
Switch	Core, Distribution, Edge Switch	80대
서버	사업부 서버	118대
PC	임직원, 협업 사용자	5,180대

〔표 4〕 그룹화 요소 정의

그룹화 요소	정의
일반 사용자	사업부 내부 사용자
협업 사용자	협업 업체(협력사, 관계사, 자회사), 협업 사용자(외부개발자, 파견근무자)
서버	사업부 서버군
인프라	IT 서비스를 제공해주는 시스템 및 장비군

〔표 5〕 장비 도입 현황

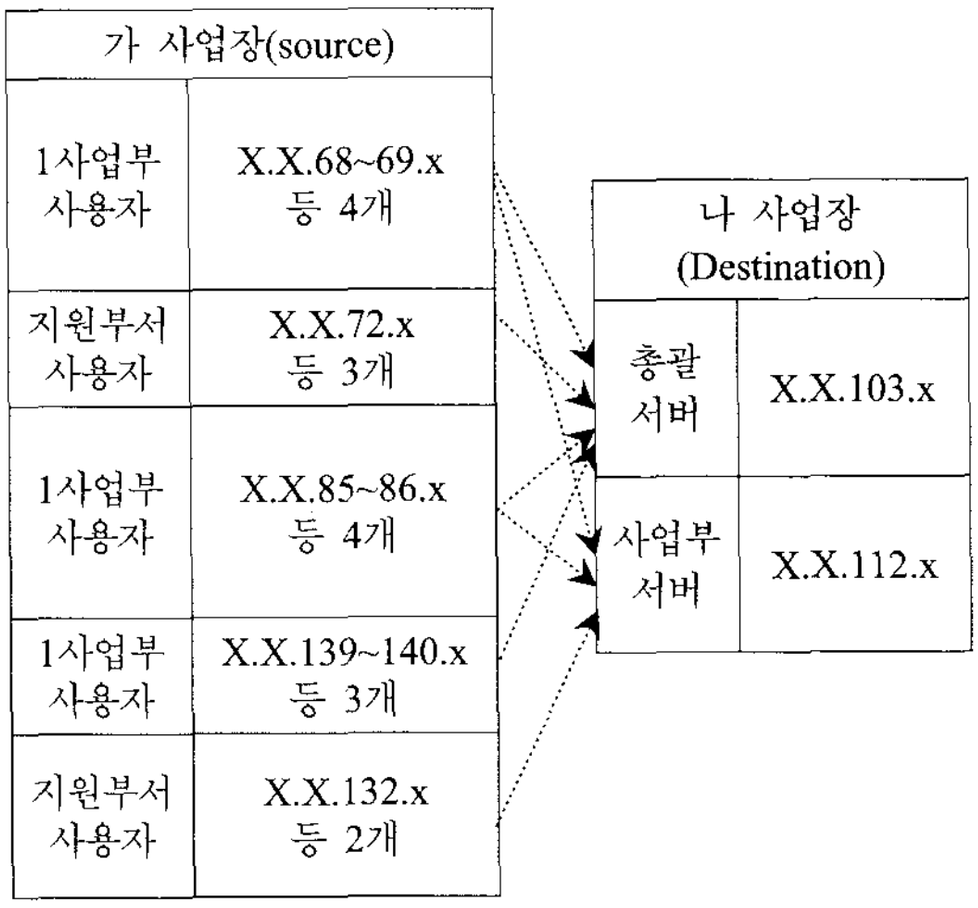
구분	세부 내용	수량
분산 Switch	Extream6808 & 관리모듈	13대
	16포트 기가 모듈	73대
서버 팜 Switch	Catalyst6509/Sup720/FWSM	2대
	48포트 10/100/1000T	2대
PC S/W	NAC Agent(Any click)	5,180대

논리적 그룹은 [표 4]와같이 내부 사용자, 협업 사용자, 서버, 인프라 등의 큰 그룹으로 정의할 수 있었고 각각의 그룹은 필요에 따라 더 세분화된 그룹으로 구분할 수 있다.

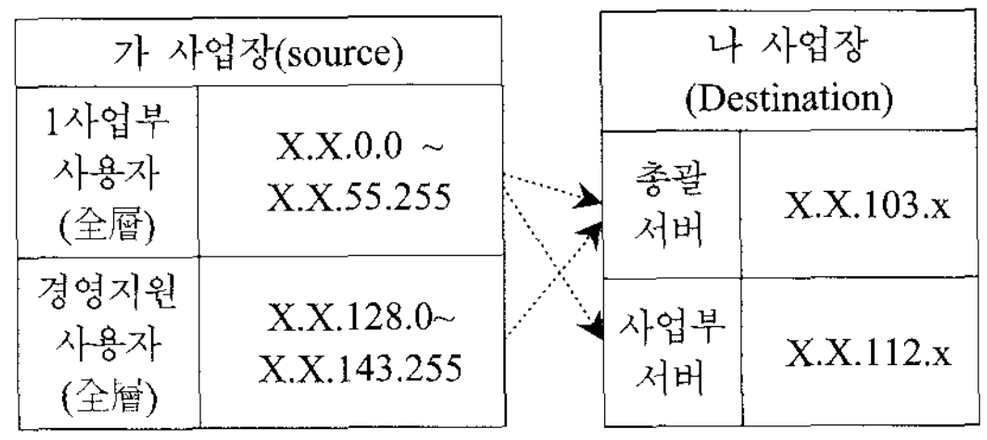
다 계층 보안 구조가 적용되기 전에는 Network가 업무 중심이 아닌 사업장 위치 중심으로 IP 주소가 부여되고 있어 하나의 Network에도 여러 업무 및 사용자 그룹이 혼재되어 있었지만, 개선 후에는 업무 특성을 갖는 논리적 그룹으로 분류되어 적용하였다. [표 5]는 이를 구현하기 위한 장비의 도입 현황을 정리한 것이다.

5.1.2 방화벽 ACL

[그림 3]과 같이 <가 사업장>의 1사업부 사용자 그룹은 <나 사업장>의 총괄 서버와 1사업부 서버를 사용하고 있다. 이 경우 <가 사업장>을 논리적으로 그룹화하기 이전의 사용자 IP 주소 체계를 보면 1사업부 사용자는 X.X.68~69.x 등 11개, 그리고 지원부서 사용자는 X.X.72.x 등 5개의 C Class 단위로 운영되고 있어 타 사업부 사용자들과 혼재되어 일일이 관문 방화벽에 등



〔그림 3〕 Host 기반 방화벽 정책(개선 前)



〔그림 4〕 Network 기반 방화벽 정책(개선 後)

록을 하여야 했다. 그러나 <가 사업장> 논리적 그룹화를 통해 1사업부 사용자는 X.X.0.0~55.255로, 지원부서 사용자는 X.X.128.0~143.255로 Network-to-Network 정책을 적용하여 [그림 4]와 같이 방화벽 Rule 설정의 간소화가 가능하였다

5.1.3 Network 그룹 ACL

Network 그룹 영역에서의 보안 정책은 동일 그룹에 대해 지리적, 물리적 상황에 상관없이 일괄적인 ACL을 적용하고, 상호 그룹간 Network 트래픽을 차등 제어함으로서 사업장 내 보안 공격을 차단하고 확산을 방지하는데 있다. 각 사업부의 서버 그룹에는 사업부 일반 사용자 그룹만이 Network-to-Network으로 접속할 수 있고, 타 사업부의 서버 그룹으로의 접속은 업무에 연동되는 일부 포트만 Network-to-Network 또는 Network-to-Host로 접속할 수 있으며, 타 회사 Network 그룹은 Host-to-Host 접속만 허용한다.

5.1.4 사용자 인증

사용자 PC가 네트워크에 연결되면 인증과정이 진행된다. 사용자 인증정보가 논리적 사용자 그룹과 DHCP Relay 그룹정보를 비교하여 일반 사용자, 출장자, 협업 사용자, Guest의 4개 논리적 그룹에 따라 해당 IP를 DHCP서버로부터 할당받게 된다.

개인 PC에 설치된 Agent인 ACL 모듈 및 Switch HUB에서 Dynamic VLAN Tagging(동적인 VLAN 구현)을 이용한 Network 접근 권한 관리, 위치 기반에 의한 접근 권한 관리, 사용자별 사용 기간 및 시간대별 접근 권한 관리, 사용자별 IP 주소 강제 할당에 의한 네트워크 접근 권한 관리를 한다.

협업 사용자의 경우 필요한 IT 리소스에만 접속할 수 있도록 하고, 방문 사용자의 경우 A회사의 모든 리소스에는 접근할 수 없고 오직 인터넷만 사용하도록 Host 접근 제어를 사용자 인증 후 설정을 한다.

5.2 적용 효과

5.2.1 Network 구조 개선

논리적 그룹화 이전의 Network 환경에서는 조직 변경 시 해당 조직의 IP 변경과 그로 인한 방화벽 Rule 변경 작업이 발생하고, 이에 따라 변경 조직의 IP 파악이 어려울 수 있으며, 변경 IP에 대한 방화벽 Rule 변경 작업이 자동이 아닌 수동으로 개별 신청해야 하기 때문에 방화벽 Rule 담당자의 업무가 과중되는 어려움이 발생했다. 또한, 변경에 대한 영향 및 작업 범위의 예측이 어렵기 때문에 변경에 대한 의사 결정을 신속히 할 수 없는 어려움도 있다.

이에 반해 본 연구에서 제안된 방식은 사용자 인증 과정에서 자신의 업무 특성에 맞는 사용자 그룹별로 자동으로 IP가 할당되므로 IP 변경으로 인한 상기의 과정들에 소요되는 시간이 거의 할당되지 않는다. 또한, 조직 변경같은 대규모 변경이 아닌 사용자의 이동 및 출장 같은 환경에서도 IP 변경 및 관리에 따른 사용자 및 IP 관리 담당자의 업무가 위와 같은 사용자 인증 방식으로 인해 담당인력이 적용 전에 8M/M에서 0.5M/M호 7.5M/M(94%)의 절감 생산성 향상을 가져 왔다.

5.2.2 Network 보안 강화

기존 관문 방화벽 중심의 보안 정책으로는 A회사 내부 및 외부 접근제어를 통한 외부에서 내부로의 악의적인 침입 및 유해트래픽은 차단이 가능하나 관문 방화벽 아래 Distribution Switch, Edge Switch, 사용자 영역에서 발생한 바이러스 확산이나 비인가 접속은 차단이 쉽지 않았다. 더욱이, 협력사, 관계사 등의 외부 인력들과 구분 없는 Network를 사용함으로써 자사 보안정책 통제가 어려운 문제점 등이 있었다. 따라서, 하나의 PC 또는 서버에서 보안 문제 발생 시 사업장 내부로 확산되는 데 오래 걸리지 않았다. 또한, 한 사업장에서 문제가 밝혀지면 A회사 보안 정책 관리자는 다른 사업장에서 동일한 문제가 발생할 수 있다는 사실과 그 문제가 확산되지 않도록 특정 ACL을 설정 할 것을 유선 전화나 메일을 통해 각각의 사업장 담당자에게 통보해야 한다. 이는 보안 사고 탐지에서 조치까지의 시간을 지연시키는 결과를 낳았다. 결국, 긴 시간과 많은 인력 동원은 또 다른 비용으로 기업 비즈니스에 악 영향을 줄 수 있다.

자사 일반 사용자와 협업 사용자, 방문자 등의 인력을 구분하여 각각의 그룹에 ACL을 설정하였다. 따라서 자사 인력이 아닌 관계사의 사용자 PC에 대해서는 Network에 접속 시점부터 사용자 인증 및 무결성 체크를 통하여 별도의 ACL을 설정하여 접속 권한을 제한하여 사고가 발생할 수 있는 근거를 원천적으로 차단할 수 있었다. 그리고, 이러한 Network 구조는 각 영역에 보안 정책을 분산시키면서 관문에 집중되어 있는 보안 집중도는 전사로 고르게 부담하는 Security Balancing 효과도 얻을 수 있었다. 따라서 각 그룹 Switch 및 방화벽의 보안 정책 수의 합이 관문 방화벽에 설정된 보안 정책의 수보다 큰 폭으로 감소하였다.

이를 A회사 전체에 적용할 경우 현재 26,000 여개의 Rule이 2,600 여개로 감소가 예상된다.

5.2.3 Network 운영 및 관리 효율성

ID와 Password를 활용한 사용자 인증을 통한 자동 IP 할당을 적용하기 전에는 출장 등으로 업무 이동이 발생하면 새로운 IP 신청과 할당 업무에 상당한 시간을 소비 했어야 했다. 사용자 추적성을 확보하기 위하여 대부분의 Network에서 고정 IP를 사용했기 때문이다. 또한 IP 변경은 사용자가 사용하는 Application에 따라 보안 장비의 보안 정책에 변경을 가져오는 경우가 많았다.

특정 Application을 사용하는 A회사 임직원의 이동으로 관리자의 보안 정책 등록업무 일 평균 처리 건수

는 보안등록 대상 장비 문의 약 5건, 결재 지연으로 인한 업무 지연 건당 약 2일 이었다. 본 연구에서 제안하는 사용자 인증에 따른 자동 IP 할당은 이러한 업무 자체가 필요 없으며, 미리 할당된 IP를 부여 받기 때문에 부가적인 보안 정책 등록이 전혀 발행하지 않는다.

Ⅵ. 결 론

본 연구에서는 관문 방화벽에 의존하는 경직된 보안 구조를 가진 기업 Network에 신속성과 보안 강화라는 두 마리 토끼를 잡기 위해 다 계층 보안 구조를 제안했다.

구현 방법으로 방화벽 영역에서는 방화벽 ACL을, Network 그룹 영역에서는 논리적 그룹화라는 기법을 사용하였고, 사용자 영역의 보안을 위해 사용자 인증, 무결성 체크 및 사용자 ACL을 설정할 수 있는 802.1x 인증 기법과 PC 방화벽을 도입하였다.

방화벽 영역은 기존에 모든 접근 통제 정책이 집중화 하던 것을 신속성과 관리 편의성을 위해 대부분의 Rule을 Network 그룹의 ACL로 변경하여 사업장의 공통 정책만 설정하도록 간소화를 제시하였다. Network 그룹 영역은 업무 성격에 따라 기업 Network를 분류하는 논리적 그룹화를 통하여 기업 Network의 구성 변경 용이성을 제시하였다. 사용자 영역은 802.1x 인증 기법을 사용자 영역에 도입하여 다양한 사용자와 이동이 잦은 대기업 Network 환경 하에서 사용자 단 보안 및 변경의 용이성을 제시하였다.

향후, 개선해야할 과제로는 Network를 논리적 그룹으로 분리하여 각각의 그룹에 일괄적으로 ACL을 적용하고 자동으로 관리할 수 있는 중앙의 ACL 적용 Tool의 개발이 필요하다.

참고문헌

[1] 신용섭, 정보통신부 정보보호 과장, “정보화 역기능 방지 대책”, 나라경제 1월호, pp.93-96, 2000

[2] Todd Lammle, Donald Porter, “CISCO CERTIFIED NETWORK ASSOCIATE”

[3] Cisco Press, “Cisco LAN Switching Fundamentals”, 2004.7.

[4] 박문기, “Ethernet Switching Network 설계 및 구현: 고성능 고가용성”, 2008.1

[5] Chris Lewis, “Cisco Switched Internetworks : VLANs, ATM & Voice/Data Integration”.

[6] AUERBACH, “802.1x Security Solution for Wired and Wireless Networks”, 2008.4

[7] Wiley, "Implementing 802.1x Security Solutions for Wired and Wireless Networks", 2008.4

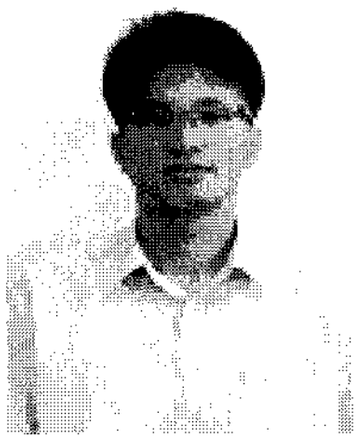
[8] Colin Weaver, "Using 802.1x Port Authentication To Control Who Can Connect To Your Network", ITdojo, Inc, 2005.1

[9] 김대식, “802.1x 미지원 네트워크를 위한 보안정책 관리도구”, 전남대학교 대학원 정보보호 협동과정, pp.8-9, 2007.2

〈著者紹介〉

황 기 영 (Ki Young Hwang)
정회원

1987년 2월 : 광운대학교 전자계산학과 졸업
2006년 2월~현재 : 고려대학교 정보경영공학전문대학원 석사과정
2003년 5월~현재 : 삼성SDS 정보보안센터 센터장
<관심분야>정보보호정책, 인터넷 침해사고대응, 네트워크보안



주 성 원 (Sung Won Joo)

1995년 2월 : 연세대학교 전자공학과 졸업
2000년 8월 : KAIST 전기및전자공학과 석사
2000년 3월~2005년 6월 : (주)시큐어넥서스 개발팀
2005년 7월~현재 : 삼성네트웍스 품질보안팀 책임
<관심분야> 정보보호, ITIL, Wireless-LAN, NAC