논문 2010-47TC-12-13

사내 네트워크 보안을 위한 네트워크 접근제어시스템 설계 및 구현

(Design and Implementation of Network Access Control for Security of Company Network)

백 승 현*, 김 승 광**, 박 홍 배***

(Seung Hyun Paik, Sung-Kwang Kim, and Hong Bae Park)

요 약

급변하는 IT 환경에서 웜 및 바이러스 등 매우 다양한 보안 위협요소들이 증가하고 있다. 특히 기업의 사내 네트워크에서는 이러한 위협을 원천적으로 차단할 수 있는 방안이 필요하다. 이러한 면에서 현재 네트워크 접근제어(NAC: Network Access Control)는 차세대 네트워크 보안기법으로 주목받고 있다. 본 논문에서는 허가되지 않거나 웜이나 바이러스 등 악성코드에 감염된 PC나 모바일 단말 등이 사내 네트워크에 접속하는 것을 원천적으로 차단하기 위해, 네트워크 접근제어시스템을 설계하고 구현방안을 제안하고자 한다.

Abstract

IT environment is rapidly changed, thus security threats such as worms and viruses have increased. Especially company's internal network requires to be inherently protected against these threats. In this respect, NAC(Network Access Control) has attracted attention as new network security techniques. The NAC implements the endpoint access decision based on the collected endpoint security status information and platform measurement information. In this paper, we describe the design and implementation of unauthorized NAC which protect against such as a worm, virus, malware-infected PC, and mobile device to connect to company's internal networks.

Keywords : 네트워크 접근제어시스템, 네트워크필터, 정보보호, 공개키(PKI), 인증서버

I. 서 론

최근 넷북, 스마트폰 등의 다양한 모바일 단말의 등장과 이용증가 그리고 내부 네트워크의 접속방법의 다양화 등으로 인해서 외부에서 유선을 통한 접근을 제어하는 것만으로는 내부 네트워크의 안정성을 보장하기 어렵다[1]. 또한 내부 네트워크 내에서의 새롭게 생기는 보안위협에 대해서도 대처하기가 어렵다. 따라서 네트워크 접근제어강화와 비인가자 및 보안에 취약한 단말에 대한 네트워크 접속을 원천 차단할 수 있어야 한다. 그리고 사내에서의 보안에 필요한 정보를 수집하기 위한 IP 사용 추적/통제, IP 사용 정보저장 및 이력관리를 통한 모니터링 및 통제가 필요하다. 사내 임직원 및 협력업체들이 사용자 인증절차 없이 사내 네트워크에 접속할 수 있기 때문에 이를 통제하여 사내 네

* 학생회원, 경북대학교 전자전기컴퓨터학부
(Eelectrical Engineering and Computer Science, Kyungpook National University)
** 정회원(교신저자), (주)위즈앤테크, 기술이사
(Technical director, Wizntec)
*** 정회원, 경북대학교 전자공학
(Eelectronics Engineering, Kyungpook National University)
※ 본 연구는 산업자원부 산학연협력 기업부설연구소 설치지원사업(000366620210)의 지원을 받아 수행되었음.
접수일자: 2010년7월27일, 수정완료일: 2010년12월10일

트워크 및 기업정보자산을 보호할 수 있어야 한다. 그리고 인증된 사용자의 경우에도 외부에서 모바일 단말기가 바이러스에 오염되어 사내 네트워크에서 바이러스를 전파하는 경우가 많이 발생하므로 이를 방지할 수 있어야 한다. 따라서 사용자 접속제어로 네트워크 보안시스템이 구축되고 네트워크 위협경로 차단정책 통합관리가 필요하다.

기존의 웜, 바이러스 등의 침입을 막기 위한 네트워크 보안방식은 내·외부 네트워크 경계에서 방화벽과 침입탐지시스템(IDS), 침입방지시스템(IPS)과 같은 솔루션을 설치하는 것이었다. 하지만 발전하는 유·무선 네트워크 기술과 단말기의 다양화, 기업 비즈니스 환경의 확대 등으로 기존의 방식으로 네트워크 보안을 유지하는 것에 한계가 생겼다. 보안에 취약한 노트북, 모바일단말기 또는, 집이나 출장지 등의 원격지 컴퓨터를 이용한 기업 내부 네트워크의 접근으로 인해 어디에서 감염이 시작되어 확산되었는지 확인하는 것조차 파악이 어렵다. 사용자단에서의 보안관리가 취약해 공격에 이용당하는 상황이 빈번히 발생하고 있다. 최근 두드러지고 있는 공격 유형이 보안에 취약한 사용자단을 이용해 서버 시스템이나 네트워크를 공격하는 방식이다.

이러한 문제점을 해결하기 위해 본 논문에서는 네트워크 접근제어(NAC: Network Access Control)를 도입하여 사용자가 내부 네트워크에 접근하기 전에 보안정책을 만족하는지 여부를 검사해 네트워크 접속을 통제하고자 한다. 이는 사용자단(endpoint)의 보안기술을 기존 네트워크 보안체계와 결합해 기업 전체 네트워크에 통합보안체계를 구현하는 것이다.

Ⅱ. 네트워크 접근제어

네트워크 접근제어는 네트워크에 접근하는 접속단말의 보안성을 강제화할 수 있는 보안 인프라이다. 보안정책을 준수하고 있는지 검사함으로써 허가되지 않거나 웜·바이러스 등 악성코드에 감염된 PC나 노트북, 모바일 단말기 등이 회사 네트워크에 접속되는 것을 원천적으로 차단해 시스템 전체를 보호한다. 즉, 네트워크 접근제어는 접속하는 단말기의 무결성을 보안정책에 따라 확인하여 통제하고 접속되어 있는 단말의 보안 또한 지속 감시 제어할 수 있도록 자동화 시켜주는 보안 통제시스템이다[2~4]. 이는 기존 보안방법과 전혀 다른 방법으로 보안을 유지시킨다. 기존에는 게이트웨이단의 방어를

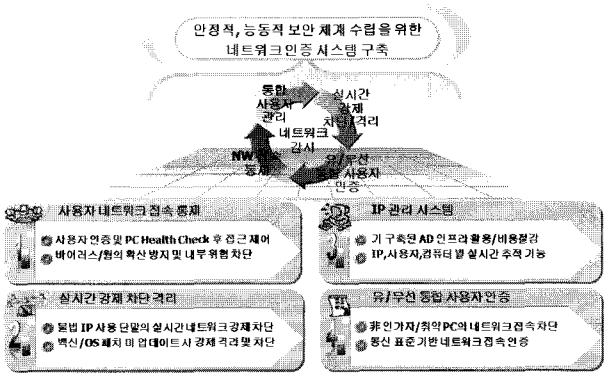


그림 1. 네트워크 접근제어 모델
Fig. 1. NAC Model.

수행하였지만, 네트워크 접근제어는 접속하려는 모든 단말기를 검사하고, 보안정책을 만족하는지 감시하여 네트워크를 보호한다[5].

네트워크 접근제어의 처리과정은 그림 1에 있다. 이 모델은 접속 단말기의 보안상태평가, 보안문제대응, 네트워크 접근허가, 보안정책 준수여부감시 및 대응에 대한 순환절차를 정의한다. 네트워크 접근제어 처리과정은 보안에 취약한 단말의 네트워크 접근 권한 획득을 막고, 이미 접속된 단말도 보안정책에 위반될 경우 네트워크 접근을 통제한다. 또한 IP관리 시스템을 통해 IP, 사용자, 단말 별 실시간 추적이 가능하도록 한다[6].

네트워크 필터링장치를 이용한 인증서기반 네트워크 접근제어는 네트워크 필터링 수단을 하드웨어적으로 구현하여 운영서버에 접속하기 전에 IP 필터링을 통한 접근제어가 이루어지도록 함으로써, 인증서버의 인증모듈을 통해 PKI(Public Key Infrastructure)인증서와 PC 헬스체크정보를 확인하여 1차적으로 인증절차를 거친 클라이언트에 대해 실시간으로 IP 및 포트기반으로 임의 IP 사용자 여부를 확인하여 운영서버접근을 허용 또는 차단할 수 있도록 한다. 이와 같은 방식을 통해 네트

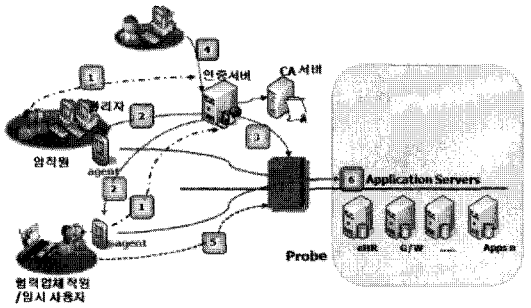


그림 2. 인증서 기반의 접근제어시스템
Fig. 2. NAC based on PKI.

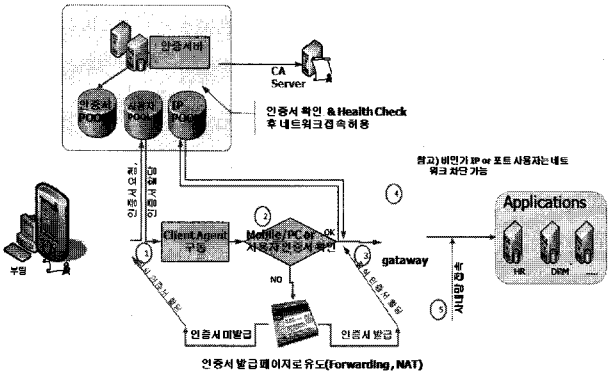


그림 3. 사용자 인증과정
Fig. 3. Process of Client Authentication.

워크 보안을 강화시키도록 네트워크 접근제어를 구성한다. 그림 2에서 전체 시스템 모델을 볼 수 있으며, 그림 3에서 사용자 인증과정을 나타낸다. 접근제어를 하는 하드웨어부를 프로브(Probe)라 한다.

그림 2에서 각 흐름을 살펴보면 다음과 같다.

1. 임직원 인증서 자동신청 발급
2. 인증서 수동발급/에이전트 설치
3. 인증/헬스체크 후 IP 승인, 제거
4. IP 관리 및 IP사용자 추적, 인증서 발급승인
5. 불법IP 사용자 접근차단
6. 에이전트(Agent) 설치 및 인증 후 사내망 접속

Ⅲ. 네트워크 접근제어시스템 설계 및 구현

1. 네트워크 접근제어시스템 구조 및 처리과정

인증서 기반의 사내 접근제어 보안시스템은 크게 사용자의 인증시스템과 프로브에 탑재되어 네트워크에 접근하는 사용자의 IP 및 포트에 대한 접근제어를 수행하

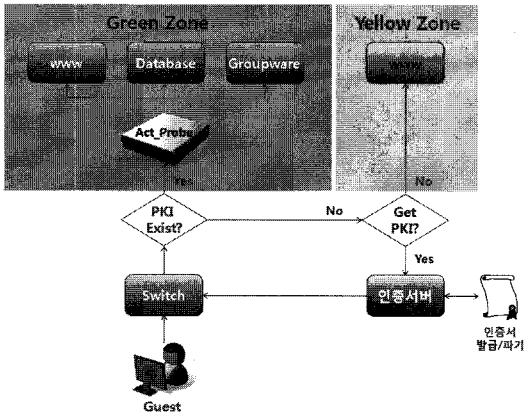


그림 4. PKI 인증서기반 접근제어과정
Fig. 4. Process of Access Control using PKI.

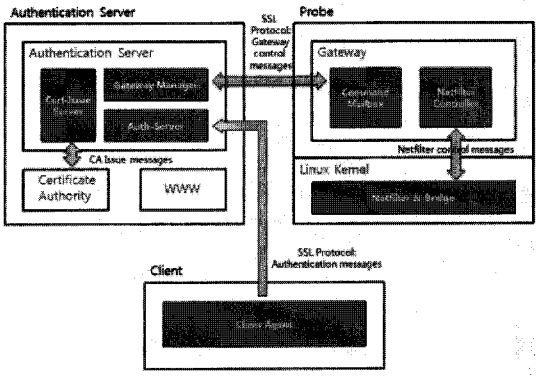


그림 5. 프로브 인증시스템 구조
Fig. 5. Construct of Probe Authentication System.

는 게이트웨이 시스템으로 구성된다.

그림 4에서 인증서 발급과 프로브사용에 대한 과정을 보여준다. 그리고 그림 5에서 프로브 인증시스템의 구조를 보여준다. 프로브 인증시스템은 크게 인증서버, 프로브, 클라이언트 에이전트로 구성되어 있다. 인증서버는 인증서 발급 및 파기, 사용자 인증 등의 작업을 수행하며, 클라이언트 에이전트는 인증서버에 사용자의 정보를 전달하는 역할을 한다. 프로브는 인증서버에서 제공하는 인증정보를 기반으로 실질적인 네트워크 차단 및 허용 작업을 수행한다.

인증시스템은 크게 세 가지로 구성되어 있다.

1) CA(Certificate Authority): CA는 인증서 발급 및 파기를 담당하며, 데이터베이스를 이용하여 인증서를 관리한다.
2) 인증서버: 인증서버는 발급된 인증서와 PC 헬스체크정보를 가지고 사용자를 인증하여 인증된 사용자에 대해 Probe의 게이트웨이를 통해 네트워크 접근을 허용/차단명령을 내린다. 인증서버는 사용자가 인증서를 가지지 않은 경우 사용자이름(User_name)과 암호문(Passphrase)를 가지고 인증한 후, 인증서를 클라이언트가 다운로드할 수 있도록 한다.
3) 클라이언트 에이전트: 클라이언트 에이전트는 서버에 사용자가 가진 인증서와 PC의 헬스체크정보를 보여주는 역할을 한다.

인증서버와 인증발급에 대한 시스템 전체는 OpenSSL기반으로 개발한다. OpenSSL은 SSLeay를 기반으로 한 공개용 암호화 라이브러리이다. OpenSLL의 대표적인 기능으로 Certificate Server는 인터넷에서 메일

이나 프로그램(applet, script)등의 송신자를 인증해주는 서버이다.

게이트웨이 시스템은 네트워크의 IP 및 포트 접근제어 하드웨어인 프로브에 탑재되어 네트워크에 대한 접근제어를 수행한다. 운영체제는 임베디드 리눅스를 기반으로 하여 리눅스에서 지원하는 Netfilter인 IP_tables을 기반한다. 운영서버와 서로 통신하면서 네트워크의 접근에 허용하거나 차단 명령과 사용자의 IP와 포트를 수신하여 실시간으로 적용한다.

클라이언트가 프로브 인증시스템에 의해 관리되는 네트워크에 접근을 시도하면 프로브의 Netfilter&Bridge 모듈에 의해서 연결이 차단된다. Netfilter&Bridge 모듈은 관리되는 목록에 등록된 클라이언트에 대해서만 접근을 허용하기 때문이다. Netfilter&Bridge의 관리 목록에 등록되기 위해서는 먼저 관리자로부터 받은, 접근권한이 부여된 계정(ID, Password)과 인증서가 있어야 한다. 관리자는 Certificate Authority를 이용하여 인증서를 발급/파기하는데, 제공되는 관리자 페이지(Web base)를 이용하여 등록하거나 콘솔로 접속하여 Certificate Authority가 제공하는 스크립트를 실행할 수 있다. 클라이언트가 계정과 인증서를 발급받았다면 클라이언트 에이전트를 이용하여 인증서버에게 사용자 인증을 요청할 수 있다. 인증 요청 시 클라이언트 에이전트는 인증서와 함께 사용자 계정 정보, PC헬스 정보, 사용자 네트워크 정보, 사용자 시간 등을 인증서버에 전달하게 된다. 전달되는 정보는 OpenSSL 기반으로 암호화되어 보호된다. 인증서버는 수신한 사용자 정보 및 인증서의 무결성과 유효성을 검사하고 인증여부를 클라이언트 에이전트에게 알려준다. 인증서버는 인증이 성공한 클라이언트에 대한 접근을 허용하기 위해 Command Mailbox(프로브의 Gateway)모듈에 인증된 사용자의 정보(IP, Port 등)를 전달한다. 전달되는 정보는 OpenSSL 기반으로 암호화되어 보호된다. Command Mailbox는 전달받은 사용자정보의 유효성을 검사한 후 Netfilter Controller를 이용하여 Netfilter&Bridge의 관리목록에 해당 사용자의 정보(IP, Port 등)를 등록한다.

위의 인증작업이 성공한 클라이언트가 프로브 인증시스템에 의해 관리되는 네트워크에 접근을 시도하면 프로브의 Netfilter&Bridge 모듈에 의해서 연결이 허용된다. 인증 흐름도는 그림 6과 같으며, 그림 7, 8, 9에서 각 사용자 유형별 인증과정을 보여준다.

그림 7에서 처음 인증서를 발급받는 사용자의 인증과정을 보여준다. 네트워크 필터링 접속 요청에서 인증

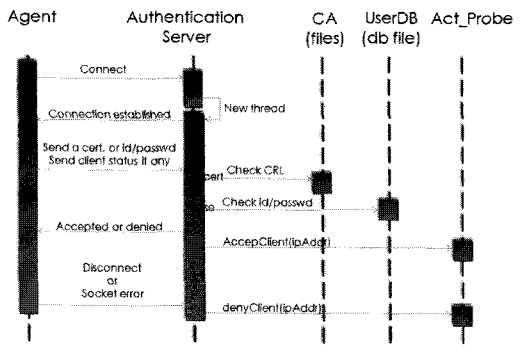


그림 6. 인증 흐름도
Fig. 6. Authentication Sequence.

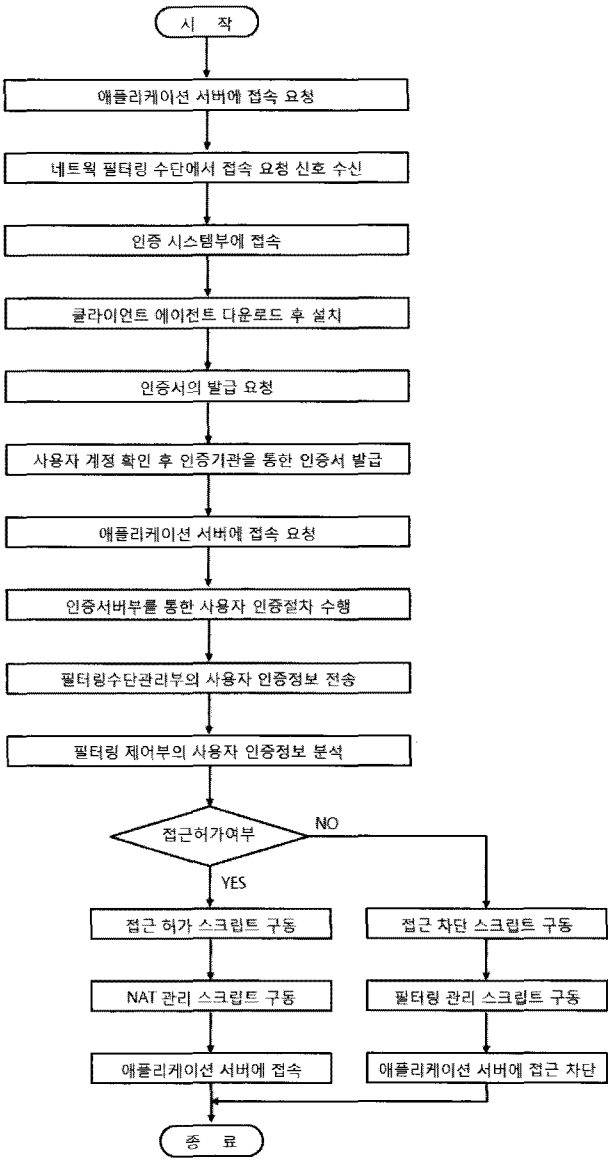


그림 7. 처음 인증서를 발급받는 사용자의 인증과정
Fig. 7. Authentication Process of New User.

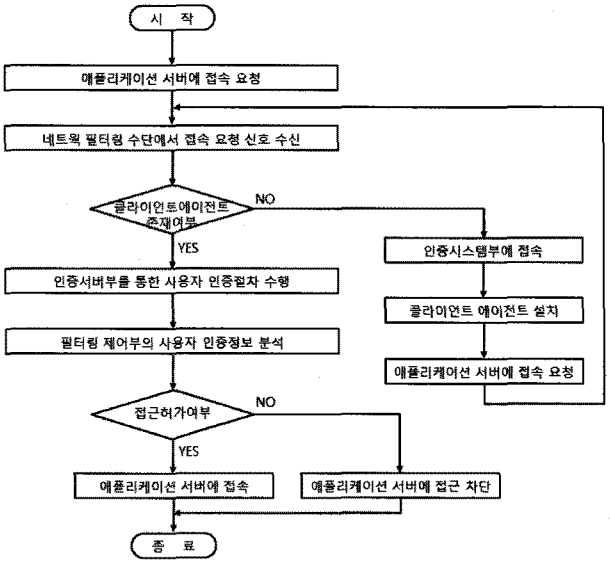


그림 8. 클라이언트부에 인증서가 있는 사용자의 인증과정

Fig. 8. Authentication Process of Existing User with Authentication certificate.

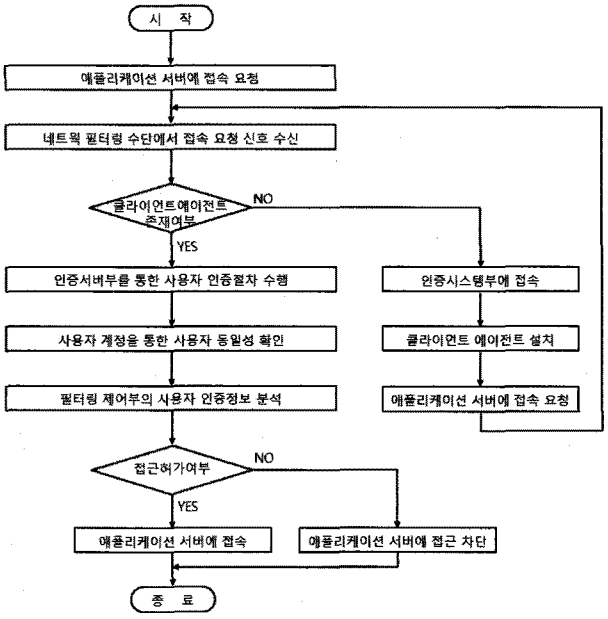


그림 9. 클라이언트가 변경된 기존 사용자의 인증과정

Fig. 9. Authentication Process of Existing User without Authentication certificate.

시스템부로 접속하여 클라이언트 에이전트를 다운로드 설치가 이루어지고, 인증서 발급요청을 하게 된다. 이를 통해 사용자 계정을 확인하고 인증서 발급이 이루어지는 절차를 거친다.

인증서가 있는 경우, 그림 8에서와 같이 인증서버에서 인증절차가 이루어지고, 필터링 제어부에서 인증정보를 분석하게 되어 접근여부가 결정된다.

클라이언트가 변경된 기존 사용자가 발생하는 경우, 그림 9에서 보여주듯이 클라이언트 에이전트 존재유무를 확인하여 없을 경우 클라이언트 에이전트가 설치된 후에 인증절차 등의 접근제어를 실시하게 된다.

2. 네트워크 제어시스템 구현

앞 절에서 설명한 시스템의 실행과정은 다음과 같다. 먼저 프로브를 통해 IP 및 포트에 대한 필터링을 수행하여 기본적으로 인증서버에 대한 IP 주소와 80 포트 접근을 허용하고 그 외 운영서버에 대한 접근을 차단한다. 그리고 클라이언트가 인증서버에게 사용자 인증을 요청하면 인증서버는 클라이언트 에이전트에서 받은 인증서, 사용자 계정 정보, PC헬스 정보, 사용자 네트워크 정보, 사용자 시간 등을 이용하여 인증절차를 거쳐 프로브에 접근허가 메시지를 보낸다. 그리고 그림 10에서 보는 바와 같이 PC 헬스정보체크 결과를 볼 수 있다.

그림 11에서 게이트웨이 시스템으로 네트워크의 IP 및 포트 접근제어가 이루어지는 프로브에 구성된 Netfilter&Bridge 관리목록을 볼 수 있다. 프로브의 Netfilter&Bridge 모듈에 의해서 접속하려는 사용자의

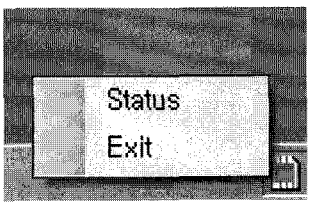
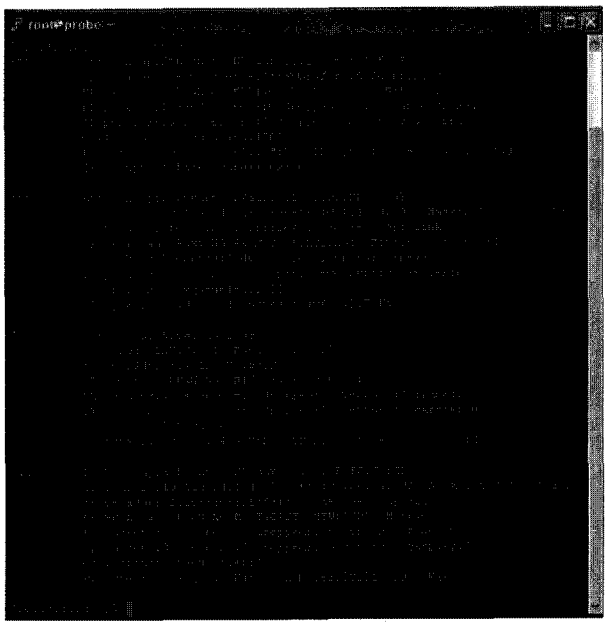


그림 10. 헬스체크 결과 화면

Fig. 10. Result of PC Health Check.



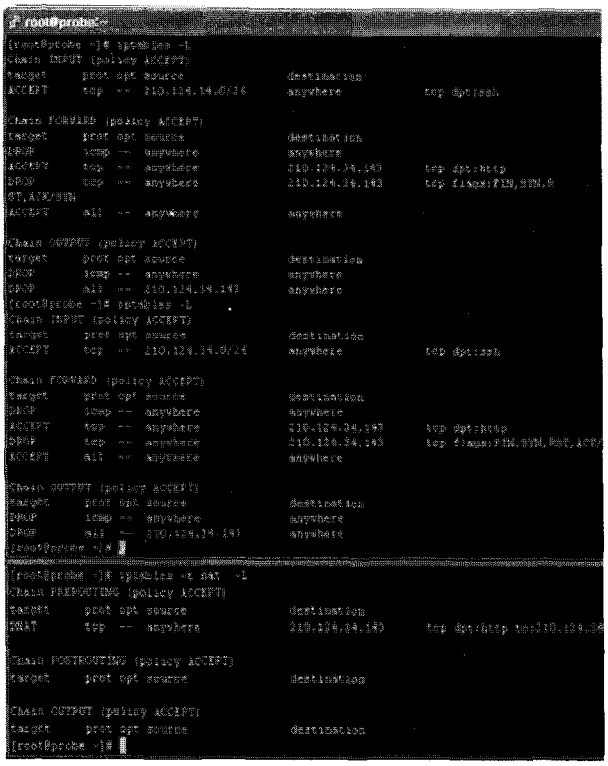


그림 11. 게이트웨이에 의해 프로브의 구성된 Netfilter & Bridge 관리목록

Fig. 11. Netfilter&Bridge Table.

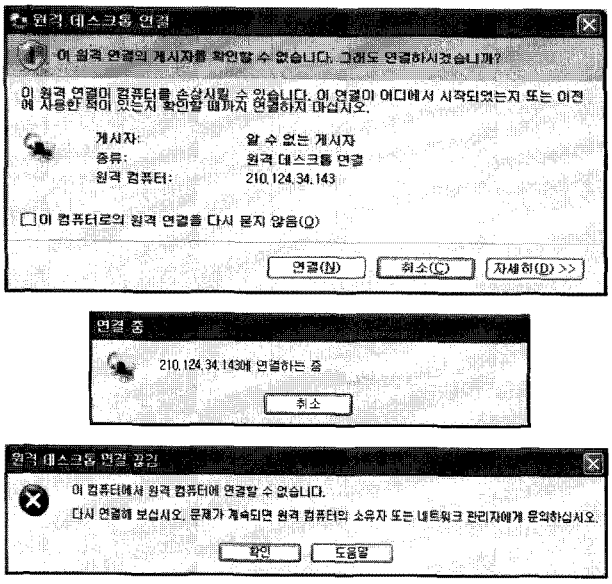


그림 12. 인증받지 못한 사용자 접근차단

Fig. 12. Access Blocking of User without Certificate.

정보를 확인하게 되고, 이를 통해 그림 12에서 보이는 바와 같이 접속을 시도하는 사용자의 정보를 확인하여 인증 받지 못한 사용자의 접속을 차단하고 접속에 실패하였음을 메시지로 알려준다. 그리고 이 사용자는 그림 7에서 보여줬던 과정을 거치면 Netfilter&Bridge 관리

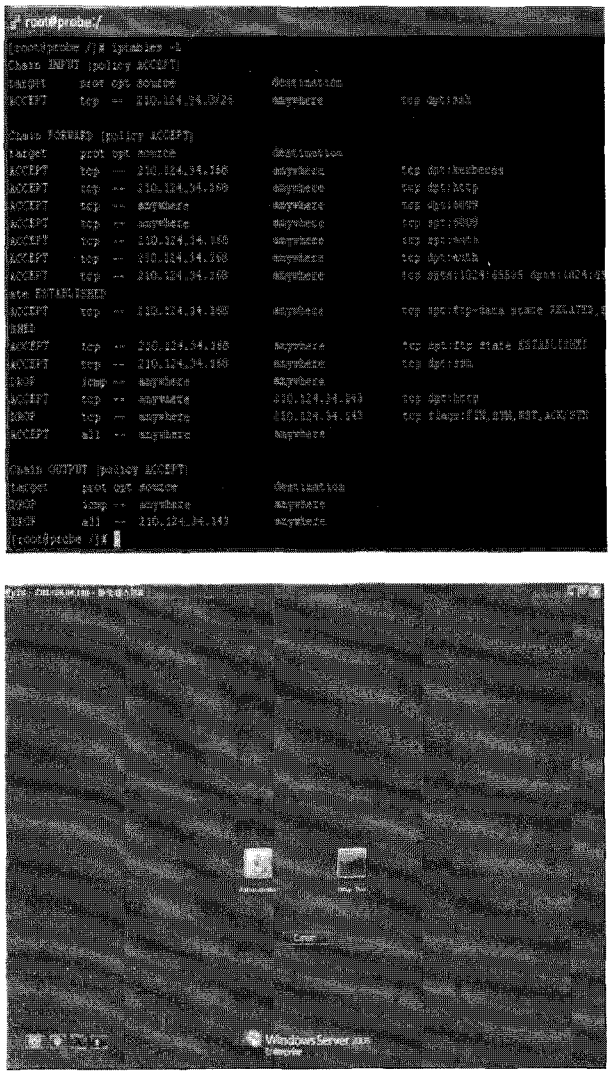


그림 13. IP 접근 허용된 게이트웨이와 접속성공화면

Fig. 13. Allowed Gateway and Success of Access.

목록에 등록이 되고, 인증서버의 인증절차를 거쳐 접속할 수 있게 된다.

인증된 사용자가 네트워크에 접근을 시도하면 프로브의 Netfilter&Bridge 모듈에 의해서 인증서버 접근이 허용되어, 인증절차를 거친 후 사내 네트워크 접근이 허가되면, 그림 13과 같이 접근이 허용된 게이트웨이를 확인할 수 있고 사용자는 접근에 성공한 화면을 볼 수 있다. 이와 같은 접근 제어는 인증서버에 의한 실시간 접근 차단과 허용을 적용한다.

IV. 결 론

본 논문에서는 기업에서 적용할 수 있는 인증서기반 네트워크 접근제어시스템을 제안하였다. 인증서기반 네

트워크 접근제어는 접근하는 단말의 보안성을 강제화 할 수 있었으며, 내부 사용자들을 효과적으로 제어할 수 있고 네트워크 관리와 보안을 자동적으로 실행할 수 있는 시스템을 구현하였다. 네트워크 접근제어시스템의 PKI 인증, PC 헬스체크를 통한 강력한 접근제어를 통해, 보다 안정적인 환경에서 기업업무를 수행할 수 있도록 하였다.

참 고 문 헌

[1] 이원진, 김기원, 부기동, 우종정, "u-Campus의 네트워크 신뢰성 보장을 위한 NAC 도입에 대한 연구", *한국정보기술학회*, 제7권 제4호, 252쪽-258쪽, 2009년 8월

[2] Mirage Network, "*Getting the Knak NAC: Understanding Network Access Control*", A Mirage Networks Industry Report, 2006.

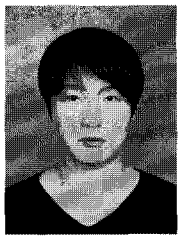
[3] Interop Labs, "*Getting started with Network Access Control*", 2006.

[4] Interop Lab, "*Network ACCess Control Resources*", 2006.

[5] 임재성, "*Network Access Control Overview*", UNET White Paper, 2006.

[6] Gartner, "*Gartner's Network Access Control Model*", 2005.

저 자 소 개



백 승 현(학생회원)
2006년 경북대학교 전자전기컴퓨터학부 학사 졸업
2008년 경북대학교 자전기컴퓨터학부 석사 졸업
2009년~현재 경북대학교 전자공학부 박사과정
<주관심분야 : 이동통신, 센서네트워크, 임베디드 시스템>

김 승 광(정회원)-교신저자
1990년 계명대학교 통계학과 학사졸업
1992년 계명대학교 컴퓨터공학과석사졸업
1992년~2002년 계명대학교 동산의료원 전산운영팀 계장
2002년~2005년 영진전문대학 컴퓨터정보계열 전임강사
2006년~현재 (주)위즈앤테크 기술이사
<주관심분야: 임베디드 시스템, RFID/USN 솔루션, 전문가 시스템>

박 홍 배(정회원)
1977년 경북대학교 전자공학과 학사 졸업
1979년 경북대학교 전자공학과 석사 졸업
1988년 University of New Mexico 전자공학과 박사 졸업
2004년~2006년 모바일단말상용화센터 센터장
1988년~현재 경북대학교 공과대학 교수
<주관심분야 : 임베디드시스템, 견실제어>