졸업연구 보고서

SSL과 VPN을 이용한 안전한 원격 업무환경 구축

팀 명 : 풍림화산

90012445 장장곤

90011972 서 희

90111954 명재찬

90012639 조상원

90311463 박주미

2006. 11

중부대학교 정보보호학과

지도교수: 이병천

목 차

요 약·····07

1. 서 론·····08
1.1 사내망에서의 정보보호 요구사항 ·····08
1.2 안전한 외부접속의 필요성 ·····08
1.3 기존의 기술, 비용 ·····08
1.4 본과제의 목표 및 내용·····08
1.4.1 목 표
1.4.2 추진방법

2. 주요 기반기술 ·····09
2.1 Windows 2003 환경의 유용성 ·····09
2.1.1 Windows server 2003의 종류
2.1.2 Windows Server 2003의 기능
2.1.3 Windows 2000 Server와 Windows 2003의 다른 점
2.2 AD (Active Directory) ·····12
2.2.1 AD 개념 및 특징
2.2.2 AD 등장배경 및 필요성
2.2.3 AD 주요기능 및 장단점
2.3 VPN (Virtual Private Network) ····· ·····15
2.3.1 VPN 개념 및 특징
2.3.2 VPN 등장배경 및 필요성
2.3.3 VPN 주요기능 및 장단점
2.4 SSL (Secure Sockets Layer) ·····17
2.4.1 SSL 개념 및 특징
2.4.2 SSL 등장배경 및 필요성
2.4.3 SSL 주요기능 및 장단점
2.5 IPSec (IP Security Protocol) ·····18
2.5.1 IPSec 개념 및 특징
2.5.2 IPSec 등장배경 및 필요성
2.5.3 IPSec 주요기능 및 장단점
2.6 SSL-VPN (Secure Sockets Layer - Virtual Private Network) ·····19
2.6.1 SSL-VPN 개념 및 특징
2.6.2 SSL-VPN 등장배경 및 필요성
2.6.3 SSL-VPN 주요기능 및 장단점

3. 구축 및 운영·····22
3.1 원격 연결 서비스 설계·····22
3.1.1 망구성도
3.2 Main Server (rca) ·····23
3.2.1 DNS (Domain Name System)
3.2.2 DHCP (Dynamic Host Configuration Protocol)
3.2.3 AD (Active Directory)
3.2.4 SSL (Secure Sockets Layer)
3.2.5 VPN (Virtual Private Network)
3.2.6 IIS (Internet Information Service)
3.3 Sub Server (rweb)·····48
3.3.1 Web Site (biz.plhs.com)
3.3.2 E-mail Server (mail.plhs.com)
3.3.3 NNTP (news.plhs.com)

4. 결 론·····67

5. 부 록·····68

참고자료 ·····71

그 림 목 차

<그림 3-1-1> 망구성도·····22

<그림 3-2> Main Server·····23

<그림 3-2-1a> 시스템 등록정보·····24
<그림 3-2-1b> DNS Server

<그림 3-2-2> DHCP(Dynamic Host Configuration Protocol)·····25

<그림 3-2-3a> Active Directory 사용자 및 컴퓨터 ·····26
<그림 3-2-3b> Active Directory Site 및 Service

<그림 3-2-4> 인증기관·····27
<그림 3-2-4-1-가> SSL(Secure Sockets Layer) 관리
<그림 3-2-4-1-나> 풍림화산 - Business Site 등록정보 (1)
<그림 3-2-4-1-다a> 등록정보 - 디렉터리보안
<그림 3-2-4-1-다b> 웹서버 인증서 마법사
<그림 3-2-4-1-라> IIS 인증서 마법사 - 서버인증서
<그림 3-2-4-1-마> IIS 인증서 마법사 - 요청 연기 또는 즉시요청
<그림 3-2-4-1-바> IIS 인증서 마법사 - 이름 및 보안설정
<그림 3-2-4-1-사> IIS 인증서 마법사 - 조직정보
<그림 3-2-4-1-아> IIS 인증서 마법사 - Site 일반이름
<그림 3-2-4-1-자> IIS 인증서 마법사 - 지역정보
<그림 3-2-4-1-차> IIS 인증서 마법사 - 인증기관 선택
<그림 3-2-4-1-카> IIS 인증서 마법사 - 인증서 요청제출
<그림 3-2-4-1-타> IIS 인증서 마법사 - 웹 서버인증서 마법사 완료
<그림 3-2-4-1-파> 인증서 보기
<그림 3-2-4-1-하a> 풍림화산 - Business Site 등록정보 (2)
<그림 3-2-4-1-하b> 등록정보 - 보안 통신

<그림 3-2-5-1-가> 라우팅 및 원격 액세스 ·····36
<그림 3-2-5-1-나> 라우팅 및 원격 액세스 구성 및 사용
<그림 3-2-5-1-다> 라우팅 및 원격 액세스 서버 설치 마법사
<그림 3-2-5-1-라> 설치 마법사 - 구성
<그림 3-2-5-1-마> 설치 마법사 - 연결
<그림 3-2-5-1-바> 설치 마법사 - IP주소할당
<그림 3-2-5-1-아> 설치 마법사 - 다중원격 액세스 서버관리
<그림 3-2-5-1-자> 설치 마법사 - 완료
<그림 3-2-5-1-차> 라우팅 및 원격 액세스 완료 (1)
<그림 3-2-5-1-카> 라우팅 및 원격 액세스 완료 (2)
<그림 3-2-5-2-가> 네트워크 연결
<그림 3-2-5-2-나> 새 연결 마법사
<그림 3-2-5-2-다> 새 연결 마법사 - 네트워크 연결 형식
<그림 3-2-5-2-라> 새 연결 마법사 - 네트워크 연결
<그림 3-2-5-2-마> 새 연결 마법사 - 연결이름
<그림 3-2-5-2-바> 새 연결 마법사 - VPN서버 선택
<그림 3-2-5-2-사> 새 연결 마법사 - 연결 유용성
<그림 3-2-5-2-아> 새 연결 마법사 - 완료
<그림 3-2-5-3-가a> 풍림화산에 연결
<그림 3-2-5-3-가b> 풍림화산에 연결중
<그림 3-2-5-3-가c> 풍림화산에 인증
<그림 3-2-5-3-나> 네트워크 상태

<그림 3-2-6a> Internet 정보서비스(IIS) 관리 ·····47
<그림 3-2-6b> 풍림화산 인터넷 웹사이트
<그림 3-2-6c> 풍림화산 인트라넷 웹사이트

<그림 3-3> Sub Server ·····48
<그림 3-3-1a> 풍림화산 - Business Site (1)
<그림 3-3-1b> 풍림화산 - Business Site (2)
<그림 3-3-1-1> 보안경고
<그림 3-3-1-2> 디지털 인증서 선택

<그림 3-3-1-3> rweb.plhs.com 연결
<그림 3-3-1-4> 풍림화산 인트라넷 업무 웹사이트
<그림 3-3-1-5> 다른 부서 선택
<그림 3-3-1-6> 로그인 에러 화면
<그림 3-3-1-7> 부서 업무페이지
<그림 3-3-1-8> 부서 자료실
<그림 3-3-1-9> 부서 게시판

<그림 3-3-2-1> POP3 Service ·····55
<그림 3-3-2-2> SMTP Server
<그림 3-3-2-2-가-ㄱ> Outlook Express - 계정
<그림 3-3-2-2-가-ㄴ> Internet 계정 - 추가
<그림 3-3-2-2-가-ㄷ> Internet 연결마법사 - 사용자 이름
<그림 3-3-2-2-가-ㄹ> Internet 연결마법사 - Internet 전자메일 주소
<그림 3-3-2-2-가-ㅁ> Internet 연결마법사 - 전자메일 서버이름
<그림 3-3-2-2-가-ㅂ> Internet 연결마법사 - Internet 메인 로그인
<그림 3-3-2-2-가-ㅅ> Internet 연결마법사 - 완료
<그림 3-3-2-2-가-ㅇ> Internet 계정 (후)
<그림 3-3-2-2-가-ㅈ> 이메일 보내기
<그림 3-3-2-2-가-ㅊ> 보낸 편지함

<그림 3-3-3> NNTP Server ·····61
<그림 3-3-3-1-가> Outlook Internet 계정 - 추가
<그림 3-3-3-1-나> Internet 연결마법사 - 사용자 이름
<그림 3-3-3-1-다> Internet 연결마법사 - Internet 뉴스 전자메일주소
<그림 3-3-3-1-라> Internet 연결마법사 - Internet 뉴스 서버이름
<그림 3-3-3-1-마> Internet 연결마법사 - Internet 뉴스 서버로그인
<그림 3-3-3-1-바> Internet 연결마법사 - 완료
<그림 3-3-3-1-사> Outlook Express - 뉴스 그룹 다운로드
<그림 3-3-3-1-아> 뉴스 그룹가입
<그림 3-3-3-2-나> 뉴스 개재하기
<그림 3-3-3-2-다> 뉴스 확인

요 약

Internet을 기반으로 한 통신이 보편화되면서 이제 어떤 기업도 국내에서만 머무를 수 없게 되었다. 시장 개척의 기회가 주어진 많은 기업들은 점차 세계적으로 뻗어나가는 추세이며 이 넓은 기업망을 다스리기 위한 적절한 방책이 필요하게 되었다.

특히 어느 곳이든 업무를 수행할 수 있는 사무 환경과 넓은 지역에 분포해있는 지사들 간의 연결은 필수가 되었고, 업무의 자동화와 데이터의 보안을 위해 독자적인 기업망을 구축하는 것은 일반화된 추세로 바뀌고 있다. 그러나 전용 회선을 임대하는 방식의 기업망은 넓은 시장을 개척하려는 기업에게 큰 부담이다. 이런 때 Internet 망을 이용한 기업의 사설망은 획기적인 대안이면서 많은 기업들이 VPN에서 관심을 갖게 되었다.

국내 VPN 시장은 그동안 이해가 높지 않아 활성화되지 못한 게 사실이다. 그러나 최근 정부나 공공 기관에 VPN 구축이 잇따라 추진되고 많은 기업들이 VPN의 필요성을 절실히 느끼면서 VPN 시장은 이제 큰 폭으로 성장할 것이다.

세계 시장조사업체들은 대부분 VPN 시장의 폭발적인 성장을 전망하고 있다. 시장조사 업체인 프로스트&설리반(Frost & Sullivan)에 따르면 2005년 세계 VPN 시장은 180억 달러 규모로 성장할 것으로 예측하고 있으며, 포레스터 리서치에서도 1999년 7억 5100만 달러에서 2002년 144억 달러의 성장세를 예측한바 있다.

국내의 경우 대부분 기업에서 이미 Internet 인프라가 구축되어 있는 상태이고 보안에 대한 관심이 타국에 비해 월등히 높기 때문에 VPN의 긍정적인 발전 가능성 있다. 그러나 VPN의 수준이 아직은 초창기에 머물러 있어 하드웨어적 보안 장비에 많은 부분 기반을 두고 있다. 이러한 이유로, VPN은 전용 회선을 임대하는 형식의 사설망에 비해 초기 비용 감소의 이익은 기대 할 수 있다.

SSL은 텍스트 기반으로 통신이 이루어지는 Internet 환경에서 보완의 중요성이 대두되면서 보안의 기능을 강화하고자 계발된 기술이다. SSL의 경우 송수신지 양쪽에 SSL이 설치되 있어야 사용이 가능하며 전송중간에 데이터를 해킹 하더라도 암호화 되어있기 때문에 정보노출의 위험이 덜하다.

이처럼 VPN과 SSL은 현재가장 발전가능성이 있는 기술로서 이번 저희 졸업작품에는 VPN과 SSL을 이용하여 간단한 사내망을 구축하여 사내망의 원격접속, 및 계정 생성, 이메일 계정 제공, 뉴스 제공 등의 기능을 활용할 계획이다.

1. 서　　론

1.1 사내망에서의 정보보호 요구사항

현대사회에서의 정보란 무한한 가치를 포함하고 있다. 이런 정보의 보호의 중요성은 아무리 강조해도 지나치지 않다. 하지만 지금 흔히 사용되고 있는 Internet은 개방적인 부분이 많아 정보유출의 위험이 있다. 사내망은 이에 비해 회사 자체적인 서버를 이용함으로서 보안을 강화시킬 수 있다.

1.2 안전한 외부접속의 필요성

정보화 사회로 들어서면서 정보화의 역기능이 발생되고 있다. 작게는 개인 사생활의 침해, 자유로운 통신의 비밀이 보장되지 않아 기본인권의 침해의 원인제공 정보의 불법 침해를 유발시켜 컴퓨터 범죄의 유발 등이 있다 또는 기업과 기업간의 정보유출로 인한 핵심 기술의 유출의 문제가 발생되고 있다. 이로 인해 정보의 보호, 보안의 필요성이 대두되고 있다.

1.3 기존의 기술, 비용

기존에 사용되고 있는 기술로는 IPSec이 가장 많이 사용되고 있다. 하지만 현재 IPSec의 기본 보안 기능의 취약점이 많이 노출되어 있어 이를 보안하기 위해 SSL-VPN이 부각되고 있다. SSL-VPN의 경우에는 적은 비용으로 공개망을 마치 사설망을 이용하듯 사용하며 보안의 강화를 위해 SSL을 도입 한 것으로 적은 비용으로 큰 효과를 기대 할 수 있다. 하지만 현재에는 SSL-VPN을 완전히 활용하여 장비나 소프트웨어의 교체를 하기보다는 SSL-VPN의 장점을 도입해 상호 보완적으로 사용되어 가고 있다.

1.4 본과제의 목표 및 내용

1.4.1 목　표

기업 인트라넷을 원격지에서 VPN을 이용하여 접속하고 업무사이트에 접속하는데 있어 좀 더 안전한 접속을 위한 방법을 모색하여 보안을 강화하고 평가분석을 하는데 있다.

1.4.2 추진 방법

윈도우 2003 Server Enterprise Edition의 다양한 기능을 이용하여 인트라넷을 구축, 인증기관과 VPN서버를 구축하고 인트라넷 내에 구축되어있는 업무사이트를 인증기관을 이용하여 SSL보안을 하여 관리/운영하고 원격지 PC로 VPN을 이용하여 인트라넷에 접속하여 인증서를 이용하여 업무사이트에 접속하고 업무를 보는 것을 직접 해보고 평가분석을 한다.

2. 주요 기반기술

2.1 Windows 2003 환경의 유용성

이번에 졸업 작품에 사용한 운영체제는 Microsoft Windows 2003 Server 2003 Enterprise Edition이다. 이 운영체제를 이용한 이유는 아래와 같다.

2.1.1 Windows Server 2003 종류

① Windows Server 2003 Standard Edition

㉮ 비즈니스 솔루션을 쉽고 빠르게 제공해 주는 네트워크 운영체제이다.

㉯ 소규모 업체와 부서에서 사용 시 최적이다

㉰ 파일 및 프린터 공유 지원한다.

㉱ 안전한 Internet 연결 제공을 한다.

㉲ 중앙 집중화된 데스크톱 응용 프로그램 배포가 가능하다.

㉳ 지원 사항 : Internet 인증 서비스, 네트워크 브리지, Internet 연결공유, 4-way SMP, 4GB의 RAM.

② Windows Server 2003 Enterprise Edition

㉮ 모든 규모의 비즈니스에서 다양한 용도로 사용되도록 개발되었다.

㉯ 높은 안정성, 성능, 뛰어난 비즈니스 가치 제공하는 응용 프로그램, 웹 서비스, 인프라를 위한 플랫폼이다.

㉰ 최대 8개의 프로세서를 지원하는 완전한 기능의 서버 운영체제이다.

㉱ 8노드 클러스터링 및 32GB 메모리 지원 등의 엔터프라이즈급 기능을 제공한다.

㉲ 64비트 컴퓨팅 플랫폼에서 사용 가능하다.

㉳ 네트워킹, 메시징, 인벤토리 및 고객 서비스 시스템, 데이터베이스, 전자 상거래 웹 사이트, 파일 및 인쇄 서버 등의 응용 프로그램을 실행하는 서버용 운영 체제로 적합하다.

㉴ 지원 사항: 8way SMP, 8노드 클러스터링, 32비트 에디션에서 64GB RAM, 64비트 에디션에서는 128GB의 RAM 지원한다.

③ Windows Server 2003 Datacenter Edition

㉮ 높은 수준의 확장성, 가용성, 안정성을 요구하는 중요 응용프로그램 개발용이다.

㉯ 최대 32way SMP와 64GB RAM을 지원한다.

㉰ 8노드 클러스터링과 로드 균형 조정 서비스를 표준 기능으로 제공한다.

㉱ 32개 프로세서와 128GB의 RAM을 지원하는 64비트 컴퓨팅 플랫폼에 사용한다.

㉲ 프로그램은 Microsoft 및 OEM(original equipment manufacturer)과 같이 공인된 Datacenter 서비스 제공업체를 통해 통합된 하드웨어, 소프트웨어 및 서비스를 제공한다.

㉳ 지원 사항: 32way SMP,8노드 클러스터링, 32비트 에디션에서는 64GB RAM, 64비트 에디션에서는 128GB RAM을 지원한다.

㉴ 기 능

㉠ 물리적 메모리 공간 확장.

㉡ Intel Hyper-Threading 지원.

㉢ NUMA(Non-Uniform Memory Access) 지원.

㉣ 클러스터 서비스.

㉤ 64비트 지원.

㉥ 다중 프로세서 지원.

㉦ TCP/IP(Transmission Control Protocol / Internet Protocol)를 사용하는 Windows Socket 응용 프로그램에서 응용 프로그램을 수정하지 않고도 SAN의 성능을 향상시킨다.

㉧ 터미널 서비스 세션 디렉터리 터미널 서비스 세션 디렉터리는 사용자가 터미널 서비스를 실행 중인 서버 그룹에서 연결이 끊어진 세션에 쉽게 다시 연결할 수 있도록 하는 로드 균형 조정 기능이 있다.

㉨ 관리자가 응용 프로그램별로 CPU와 메모리 사용량을 할당할 수 있는 Windows Server 2003, Enterprise Edition 및 Windows Server 2003, Datacenter Edition에 포함된 기능(Windows System Resource Manager)

④ Windows Server 2003 Web Edition

㉮ 웹 서버와 호스팅 관련.

㉯ 웹 응용 프로그램, 웹 페이지 및 XML 웹 서비스를 구축.

㉰ IIS 6.0 웹 서버로 사용되도록 설계되었다.

㉱ NET Framework의 핵심 부분인 XML 웹 서비스와 ASP.NET 기술을 사용한 응용 프로그램을 신속하게 개발하고 배포할 수 있는 플랫폼을 제공한다.

㉲ 배포 관리가 쉽다.

㉳ 단일용도 웹 서버로 특별히 사용하기 위해 설계된 Windows Server 2003, Web Edition은 차세대 Windows Server 운영 체제의 차세대 웹 인프라 기능을 제공한다.

2.1.2 Windows Server 2003의 기능

① Active Directory: 이 서비스는 네트워크 환경을 구성하는 ID와 관계를 관리한다.

② 응용 프로그램 서비스: 총 소유 비용(TCO)를 절감하면서 더 나은 성능을 얻는다.

③ 클러스터링 기술: 가용성, 확장성 및 관리 효율성을 크게 향상한다.

④ 파일 및 인쇄 서비스: 파일 및 인쇄 기능이 향상되어 조직의 총 TCO를 절감한다.

⑤ Internet 정보 서비스 6.0: Microsoft는 Internet 정보 서비스(IIS) 6.0과 함께 Windows 서버 운영 체제의 IIS 아키텍처를 완벽하게 수정. 기업 고객, Internet 서비스 공급자(ISP), 소프트웨어 공급업체(ISV)의 요구 충족.

⑥ 관리 서비스: 배포, 구성 및 사용이 훨씬 간편해져 중앙 집중적이고 사용자 지정이 가능한 관리 서비스를 제공하여 TCO를 절감한다.

⑦ 네트워크 및 통신: 향상된 네트워킹 기능과 새로운 기능은 네트워크 인프라의 다양성, 관리 효율성 및 신뢰성을 확장한다.

⑧ 보안: 업무 수행을 위한 안전한 플랫폼, 기존의 IT자산을 최대한 활용한 이점을 파트너, 고객 및 공급업체로 확장한다.

⑨ 저장소 관리: 디스크 및 볼륨의 유지 관리, 데이터 백업과 복원 및 SAN(Storage Area Network) 연결 작업을 더 쉽고 안전하게 할 수 있다.

⑩ 터미널 서버: 안정적이고 확장과 관리가 강화된 서버 기반 컴퓨팅 플랫폼을 조직에 제공한다.

⑪ Windows Media 서비스: 기업의 인트라넷과 Internet을 통해 디지털 미디어 콘텐트를 배포하는 데 사용되는 Windows Media 기술의 서버 구성 요소. Windows Media 서비스는 스트리밍 오디오, 비디오를 배포하는 데 가장 안정적이고 확장, 관리가 가능한 경제적인 솔루션 제공한다.

⑫ 엔터프라이즈 UDDI 서비스: XML Web services, 기타 프로그래밍이 가능한 리소스의 개발, 공유 및 재사용을 간단하게 할 수 있다.

2.1.3 Windows 2000 Server와 Windows 2003의 다른 점

① Active Directory 기능

㉮ 윈도우 2000 서버의 Active Directory 서비스를 사용하면 복잡한 네트워크 디렉터리를 간단하게 관리, 대규모 네트워크에 있는 리소스도 쉽게 찾을 수 있다.

㉯ 디렉터리 서비스 확장 가능, Internet 표준 기술 기반이다.

㉰ 윈도우 서버 2003은 포리스트, 상호간 트러스트, 도메인 이름 변경기능, 스키마의 특성과 클래스를 비활성화 시켜 정의를 변경할 수 있는 기능을 포함한다.

② 그룹정책 관리 콘솔

㉮ 윈도우 2000 서버는 관리자는 그룹 정책을 사용하여 사용자와 컴퓨터에게 허용되는 작업과 설정을 정의 할 수 있다. 그룹정책을 사용하면 액티브 디렉터리의 특정 사이트, 도메인, 조직 구성단위 전체에 걸쳐 적용되는 정책을 설정한다.

㉯ 윈도우 2003 서버는 그룹정책 관리 콘솔(GPMC)을 통해 그룹 정책을 더욱 쉽게 사용, 액티브 디렉터리의 강력한 관리 기능을 최대한 활용한다.

③ 정책 결과 집합

㉮ RSoP는 관리자가 로깅 모드와 계획 모드의 두 모드에서 현재의 정책 집합을 결정하고 분석할 수 있는 일련의 MMC(Microsoft Management Console) 스냅인으로 제공되는 인프라이다.

㉯ 로깅 모드에서 관리자는 특정 대상에 적용되는 정책에 액세스 할 수 있다.

㉰ 계획 모드에서 관리자는 대상에 정책이 어떻게 적용되는지를 알 수 있으며 그룹 정책에 변경내용을 배포하기 전에 결과를 검사 할 수 있다.

④ 볼륨 새도 복사본 복원

㉮ 볼륨 섀도 복사 서비스의 기능을 사용하여 관리자는 서비스를 중단하지 않고도 중요 데이터 볼륨의 적절한 복사본을 구성 할 수 있다.

㉯ 사용자는 서버 세어 자동으로 관리되는 저장된 버전의 문서를 검색한다.

⑤ Internet 정보 서비스 6.0

㉮ 프로그램의 안전성을 상당히 향상시켜 주는 새로운 내결함성 프로세스 모델로 아키텍처가 완전히 다시 구성된다.

㉯ 윈도우 서버 2003에서 MS ASP.NET은 기본적으로 새로운 IIS 프로세스 모델 사용한다.

⑥ 통합 .NET Framework

㉮ 윈도우 서버 2003 운영체제에 완전히 통합된 .NET Framework를 사용하여 관리자는 배관처럼 복잡한 코드를 작성하는 대신 실질적 비즈니스 가치를 제공하는데 집중 할 수 있다.

⑦ 명령줄 관리

㉮ 그래픽 사용자 인터페이스를 사용하지 않고도 대부분의 관리 작업을 수행한다.

㉯ 윈도우 서버 2003 제품군의 강력한 명령줄 기능과 스크립트 결합으로 더 높은 총 소유비용과 관련돼 다른 운영 체제의 성능을 뛰어 넘는다.

⑧ Clustering (eight-node support)

㉮ 윈도우 서버 2003 엔터프라이즈 에디션, 윈도우 서버 2003 데이터센터 에디션 에서만 사용할 수 있는 서비스는 데이터베이스, 메시징 시스템, 파일 및 인쇄 서비스 등의 중대한 응용 프로그램에 뛰어난 가용성과 확장성을 제공한다.

㉯ 엔터프라이즈 에디션, 데이터센터 에디션 둘 다 최대 8개의 노드로 구성되는 서버 클러스터를 지원한다.

⑨ 안전한 무선 LAN (802.1X)

㉮ 자동키 관리, 사용자 인증 및 LAN 액세스 이전 인증 등의 향상된 무선 LAN 보안 및 성능을 제공한다.

⑩ 응급 관리 서비스

㉮ 헤더 없는 서버 기능을 사용해 IT관리자는 모니터, VGA디스플레이 어댑터, 키보드, 마우스가 없이도 컴퓨터를 설치 관리한다.

2.2 AD(Active Directory)

2.2.1 AD 개념 및 특징

① AD 개념

Active Directory는 분산된 디렉터리이다. 정보가 한 서버에 있는 것이 아니라 네트워크상의 여러 서버에 분산되어 있기 때문에 필드 사용자들이 빠른 속도로 액세스 할 수 있고 또한 서로 복제 되어 이중화를 하기 때문에 결함허용이 지원된다.

② AD 특징

㉮ 몇 개의 object를 가진 소규모의 회사에서 몇 백 만개의 object를 가지는 대규모 회사까지 지원할 수 있도록 설계되어 있어서 확장성이 뛰어나다. 그리고 Active Directory에서 만들어 지는 모든 object를 정의하는 스키마(schema)가 있어서 여기에 각 object의 특징이나 속성(attribute)이 들어있어서 이에 기준해서 새로운 object class나 class attributes를 만들 수 있다.

㉯ Internet 표준 이름 풀이와 질의에 사용되는 프로토콜을 지원하기 때문에 Internet과 바로 통합 운영할 수 있다.

㉰ 관리자는 어디에서든 한 곳에서 로그 온하여 네트워크 전체를 관리할 수 있도록 되었다.

㉱ 각 서버가 다중 멀티 복제를 하기 때문에 결함 허용(fault tolerant)이 지원된다.

㉲ 지역적으로 떨어져 있는 경우엔 보안 관리 책임을 해당 지역의 책임자에게 위임 할 수 있다.

㉳ 다른 운영체제의 디렉터리 서비스와 서로 연동할 수 있도록 X.500이나 LDAP 2,3을 지원한다.

2.2.2 AD 등장 배경 및 필요성

① AD 등장배경

지난 수년간 컴퓨터 환경에서 “Directory"란 말은 많은 주목을 받아 왔다. 컴퓨팅 환경이 점차 커지고 복잡해짐에 따라, 네트워크/시스템 관리자는 네트워크 자원을 효율적으로 관리하는데 많은 어려움을 겪게 되었다.

② AD 필요성

일반 사용자는 자신이 원하는 네트워크 자원을 쉽게 찾지 못하는 결과를 낳게 되었다. 이러한 난제를 해결하기 위해서는 정보를 체계화하고 재정립 시키면서 관리를 쉽게 할 필요성이 대두되었고 이를 해결하기 위해 “Directory"란 개념이 나타나게 되었다.

2.2.3 AD 주요 기능 및 장단점

① AD 주요 기능

㉮ authentication & authorization

위 단어를 우리말로 하자면 각각 인증서 확인(또는 허가)이다. 여기서 인증이라 함은 어딘가에 들어가기 위해 인증을 받는 것을 말한다. 즉 우리가 우리의 컴퓨터를 키고 로그인하는 과정이 바로 인증이다. 또는 회원전용 사이트에 회원 아이디와 비밀번호를 입력하고 로그인하는 과

정이 바로 인증을 받는 과정이 된다.

확인(허가)이란 우리가 우리의 컴퓨터에 로그인한 후에 특정 폴더나 파일을 열려고 할 때 그 폴더나 파일에 대한 열기(읽기)권한이 있는지 확인하고 허가를 주는 과정을 authorization이라 할 수 있다. 즉 회원전용 사이트에 로그인은 했지만 그 사이트에 특정 서버는 유료서비스라면 비록 회원으로써 인증은 받았지만 유료서비스를 신청하지 않았다면 그 서비스는 받을 수 없을 것이다. 이러한 특정한 곳에 접속(인증)은 한 후에 그 안에서 어떤 액세스하는 과정에 대한 권한여부를 확인하는 과정이 authorization 이다.

㉯ 중앙 집중 관리(Centralized Management = single login)

액티브 디렉터리를 설치(정확한 표현은 승격이 될 것이다.)하면 네트워크상의 모든 컴퓨터 및 사용자 계정 등을 AD에서 모두 관리 할 수 있다. 즉 관리자는 네트워크에 있는 모든 컴퓨터들의 아이디 비밀번호 등을 일일이 적어두거나 외우지 않아도 AD상에서 일괄적으로 관리가 가능한 것이다

㉰ 클라이언트 & 서버 - 만남의 증가

Windows 2000서버를 설치하여 사용하는 사용자가 AD에게 인증을 요청하거나 다른 사용자의 정보를 요청하게 되면 그 순간 그 사용자의 Windows 2000 서버는 클라이언트가 되며 그 요청에 대한 정보를 제공하는 AD는 서버로서의 서비스를 제공하게 되는 것이다.

㉱ 관리 제어 위임(Delegating Administrative Control)

규모가 큰 네트워크일 경우 관리자 혼자서 큰 네트워크를 관리하기는 역부족일 것이다. 이럴 경우 특정 계정에게 적절한 권한을 주는 관리 제어 위임을 할 수 있다.

㉲ 확장성 및 거대성

AD는 DNS의 이름 영역을 사용함으로써 뛰어난 확장성을 보여준다. 또한 한 개의 도메인에 1600만개의 객체를 저장할 수 있는 등 규모가 대단히 방대하다.

㉳ single login

네트워크상의 컴퓨터가 몇 대이건 상관없이 AD로만 로그인하면 나머지 모든 컴퓨터에도 로그인 한 것과 같이 자유롭게 이용할 수 있다.

② AD 장점

㉮ 정보 보안

AD 환경의 도입으로 얻을 수 있는 첫 번째 장점은 보안의 강화라는 점이겠습니다. 점점 더 네트워크의 환경이 비대해짐에 따라서 문제시 되는 보안 문제인데 이를 중앙에서 통합 관리할 수 있음은 물론이며 위임정책을 통해서 그룹별로 정의할 수 있기도 하다. 관리자의 수고를 덜어주면서도 효과적인 관리가 가능 한 점이 바로 이러한 위임 정책 등을 통해서 가능하다고 할 수 있다. AD 에서는 각각의 객체에 따라서 액세스 권한을 달리 할 수 있으며, 그룹 보안 정책을 통해서 보안에 대한 정책을 세울 수 있다.

㉯ 정책 기반 관리

Active Directory 디렉터리 서비스에는 데이터 저장소와 논리 계층 구조가 포함된다. 논리 구조로서의 Active Directory는 정책 운용을 위한 계층적 컨텍스트를 제공하며 디렉터리로서는 특정 컨텍스트에 지정된 정책(그룹 정책 개체)을 저장한다. 그룹 정책 개체는 아래 사항을 결정할 수 있는 설정을 포함한, 해당 컨텍스트에 대한 다양한 업무 규칙 집합이다. 디렉터리 개체 및 도메인 리소스에 대한 액세스 사용자가 사용할 수 있는 응용 프로그램 등의 도메인 리소스 이러한 도메인 리소스의 사용을 제어하는 구성 방법 예를 들어, 그룹 정책 개체는 로그인한 사용자의 컴퓨터에 표시되는 응용 프로그램의 종류, 사용자가 서버에서 시작하는 경우에 Microsoft SQL Server에 연결할 수 있는 사용자 수, 다른 부서나 그룹으로 이동할 때 사용자

가 액세스할 수 있는 문서나 서비스를 결정할 수 있다. 그룹 정책 개체를 사용하면 수많은 사용자와 컴퓨터를 관리하는 대신 약간의 정책만 관리하면 된다. AD는 전체 조직이든 조직 내의 특정 부서이든 상관없이 원하는 컨텍스트에 그룹 정책 설정을 적용할 수 있도록 해준다.

㉰ 확장성

관리자가 스키마에 새 개체 클래스를 추가할 수 있고 기존 개체 클래스에 새 특성을 추가할 수있다.

㉱ 조정성

AD는 하나 이상의 도메인을 가지며 각 도메인은 하나 이상의 도메인 컨트롤러를 가진다. 따라서 네트워크 요구 사항에 맞게 디렉터리 규모를 조정할 수 있다. 여러 도메인을 결합하여 도메인 트리를 만들 수 있으며 여러 도메인 트리를 결합하여 포리스트를 만들 수 있다. 디렉터리는 해당 디렉터리에 있는 모든 도메인 컨트롤러에 스키마 및 구성 정보를 배포한다. 이 정보는 도메인의 첫째 도메인 컨트롤러에 저장되며 도메인의 모든 추가 도메인 컨트롤러에 복제된다. 디렉터리를 단일 도메인으로 구성한 경우 도메인 컨트롤러를 추가하면 추가 도메인으로 인한 관리 오버헤드 없이 디렉터리 규모를 확장할 수 있다.

㉲ 정보 복제

복제는 디렉터리에 정보 가용성, 내결함성, 로드 조정 및 성능의 이점을 제한다. AD는 멀티마스터 복제를 사용하기 때문에 단일 주도메인 컨트롤러는 물론 다른 모든 도메인 컨트롤러에서도 디렉터리를 업데이트할 수 있다. 멀티마스터 모델은 단일 도메인 컨트롤러가 작동을 멈추더라도 다중 도메인 컨트롤러를 통해 복제가 계속되기 때문에 내결함성이 높다는 이점이 있다. 멀티마스터 복제 때문에 사용자들은 인식하지 못하겠지만 실제로는 디렉터리의 단일 복사본이 업데이트되는 것이다. 도메인 컨트롤러에서 디렉터리 정보를 만들거나 수정하면 새 정보 또는 변경된 정보가 도메인에 있는 다른 모든 도메인 컨트롤러로 전송되기 때문에 디렉터리 정보가 최신 상태를 유지할 수 있다. 도메인 컨트롤러는 최신 디렉터리 정보를 필요로 하지만 새 디렉터리 정보 또는 변경된 디렉터리 정보가 있을 때만 업데이트가 이뤄지도록 제한해야 효율성을 높일 수 있다. 도메인 컨트롤러 간에 디렉터리 정보를 무차별적으로 교환하면 네트워크 성능이 급속히 떨어질 수 있다. AD는 변경된 디렉터리 정보만 복제하도록 개발되었다. 멀티마스터 복제를 사용하면 여러 도메인 컨트롤러에서 동일한 디렉터리 변경 작업이 이뤄질 가능성이 항상 있다. AD 또한 충돌하는 디렉터리 변경 내용을 추적하고 조정하여 거의 모든 경우에 자동으로 충돌을 해결하도록 개발되었다. 한 도메인에 여러 도메인 컨트롤러를 배치하면 내결함성 및 로드 조정 이점을 얻을 수 있다. 특정 도메인 컨트롤러의 속도가 떨어지거나 중지되거나 고장 나는 경우 그 도메인의 다른 도메인 컨트롤러에 똑같은 디렉터리 데이터가 있기 때문에 필요한 디렉터리 액세스를 제공할 수 있다.

㉳ DNS와 통합

Active Directory는 DNS을 한다. DNS는 mycomputer.microsoft.com과 같은 읽기 쉬운 호스트 이름을 숫자로 구성된 IP 주소로 변환하는 Internet 표준 서비스이다. DNS는 TCP/IP 네트워크의 컴퓨터에서 실행되는 프로세스를 식별하고 이 프로세스에 연결할 수 있게 한다. DNS에서 사용하는 도메인 이름은 DNS의 계층적 명명 구조에 기반하고 있다. 이는 역전된 트리 구조로, 단일 루트 도메인 아래 부모와 자식 도메인(분기 및 리프)이 포함될 수 있다. 예를 들어, child.parent.microsoft.com과 같은 Windows 2000 도메인 이름에서 "child" 도메인은 "parent" 도메인의 자식 도메인이다. 또한 "parent" 도메인은 루트 도메인인 microsoft.com의 자식 도메인이다. DNS 도메인의 각 컴퓨터는 DNS 도메인 전체 이름으로 고유하게 식별된다. child.parent.microsoft.com 도메인에 있는 컴퓨터의 도메인 전체 이름은 computername.child.parent.microsoft.com이 된다.

㉮ 다른 디렉터리 서비스와의 상호 운용성

AD는 LDAP(Lightweight Directory Access Protocol) 버전 3 및 NSPI(Name Service Provider Interface)와 같은 표준 디렉터리 액세스 프로토콜에 기반하고 있기 때문에 이러한 프로토콜을 사용하는 다른 디렉터리 서비스와 상호 운용할 수 있다. LDAP는 AD에서 정보를 검색하고 쿼리를 만드는 데 사용되는 디렉터리 액세스 프로토콜이다. LDAP는 산업 표준의 디렉터리 서비스 프로토콜이기 때문에 LDAP를 사용하여 프로그램을 개발하면 LDAP를 지원하는 다른 디렉터리 서비스와 AD 정보를 공유할 수 있다. Exchange 디렉터리와의 호환성을 위해 AD는 Microsoft Exchange 4.0 및 5.x 클라이언트에서 사용하는 NSPI 프로토콜을 사용한다.

㉯ 융통성 있는 쿼리

AD 의 글로벌 카탈로그를 이용하여 사용자 및 관리자는 시작 메뉴의 검색 명령, 네트워크 환경 또는 AD 사용자 및 컴퓨터를 사용하여 개체 속성을 통해 네트워크상의 개체를 신속하게 찾을 수 있다. 예를 들어, 이름, 성, 전자 메일 이름, 사무실 위치 또는 사용자 계정의 기타 속성을 사용하여 사용자를 찾을 수 있다. 글로벌 카탈로그의 사용으로 정보 찾기 작업이 한결 수월해졌다.

③ AD 단점

AD 의 도입 시에는 조직의 요구를 충분히 파악한 뒤 실행되어야만 한다. 일반적으로 AD 를 구성함으로써 단점이 될 만한 내용들은 주로 소규모 네트워크상에서 AD를 사용 할 때의 경이다. 소규모 네트워크상에서는 굳이 AD를 통해서가 아니라도 쉽게 사용자 및 각 자원을 구성원들이 쉽게 찾을 수 있으며 충분히 잘 활용할 수 있다. 일반적으로 AD를 도입하게 되면 네트워크상의 부하는 기존의 NetBIOS만을 사용하던 네트워크에 비해서는 당연히 더욱 많은 패킷이 흐르기 때문에 손실이 발생할 수 있다. 때때로는 WINS서버가 구성된 환경에서도 충분히 효과적이었던 소규모 네트워크에서는 AD를 도입함으로써 오히려 더욱 느려진 네트워크로 사용자들이 불만을 토로 할 수 있을 수도 있다. 분명한 점은 AD를 도입함으로써 기존의 네트워크상의 서버들은 업그레이드를 하거나 새로이 구입을 해야만 한다.

2.3 VPN(Virtual Private Network)

2.3.1 VPN 개념 및 특징

① VPN 개념

VPN(Virtual Private Network)이란 Public Switched Network 상에서 (예 : Internet) 물리적인 Network의 구성과 무관하게 논리적으로 폐쇄된 UserGroup을 구성하여 다양한 기능의 서비스를 제공하는 Network의 한 형태이다. VPN 상에 소속된 User는 VPN을 Physical Private Network으로 인식한다.

② VPN 특징

VPN 상에 소속된 User는 VPN을 Physical, Private Network으로 인식한다.

㉮ Private Network이 갖고 있는 장점은 Network을 직접적으로 통제함으로서 Network의 운영에 유연성과 독립성을 제공한다는 점이다. 또한 Network 장비에 대해 독점적으로 사용함으로서 인증되지 않은 접근에 대해 높은 수준의 보안을 구현 한다는 데에 있다. 그러나 사설 네트워크에 의존하는 기업들은 독자적인 지역적, 국가적, 범국가적 네트워크를 필요로 하며, 이를 위해서는 막대한 비용의 초기 투자가 필요하다는 문제점이 있다. 따라서 Private Network을 도입할 것인가의 여부를 결정하는 요소로 많은 기업들은 운영의 유연성과 보안성을 중요 기준으로 삼기도 하며 이와는 반대로 설비 투자비용과 운영비용이 부담되는 회사들은 통신 서비스

를 아웃소싱하기도 한다.

㉯ Public Network을 활용한 통신의 경우 Private Network과 비교하여 많은 이점을 제공한다.

㉠ 투자비용이 Terminal 장비로 한정되며 교환 장비, 전송장비, 회선 설비 등에 대한 투자가 불필요하다.

㉡ 높은 수준의 가용성, 신뢰성을 제공하며, 지역적 한계를 극복할 수 있고, 인증된 접근에 대해 보안성을 제공한다. 그러나 대부분의 회사들은 Public Network을 활용하면서도 Private Network의 장점인 운영의 유연성과 독립성을 원하고 있다. VPN 서비스는 Public Network 상에서 이러한 요구를 수용하는 Customer -oriented 솔루션을 제공한다.

2.3.2 VPN 등장 배경 및 필요성

① VPN 등장 배경

정보 기술의 급속한 진전으로 멀티미디어 환경, Internet 환경이 확산되면서 사용자의 대역폭 요구량이 급격히 증가하고 있다. 이러한 환경에서 일반 기업에서는 통신비용 및 운영 관리 비용이 증가되고 있는 추세로 인해 이를 보안하기 위하여 개발되었다..

② VPN 필요성

VPN은 PSDN과 같은 통신망을 이용하여 Private Network의 특성과 이점을 유지하면서 비용을 획기적으로 절감할 수 있는 대안으로 제시된 기술이다. 또한 이러한 기술이 현실적으로 가능한 것은 PSDN, ISDN, ATM과 같은 통신 인프라의 기반이 강화되고 있기 때문이다.

2.3.3 VPN 주요 기능 및 장단점

① VPN 주요 기능

VPN은 공중망을 사설망처럼 사용하거나 서비스를 받을 수 있고 주로 말단과 말단 사이에 통신하는 패킷을 압축 및 암호화하고, 이 패킷을 터널링 기술을 통해 전송함으로써 해커등 악의적인 의도를 가진 누군가가 패킷을 가로채기 어렵게 하거나 설사 가로채었다 하더라도 해석할 수 없도록 하는 진보된 방식의 보안 서비스이다.

② VPN 장점

㉮ 기존 Internet은 TCP/IP를 많이 사용하였다. 하지만 이 기술은 보안이 약하다는 단점을 갖고 있다. 이러한 단점을 보안한 것이 VPN으로서 TCP/IP를 이용하여 전송 시 암호화 하여 정보를 전송한다. 그러나 VPN은 TCP/IP에 한 번 더 암화를 해서 2중 암호화 후 정보를 전송하여 보안을 강화시켰다.

㉯ ISP (Internet Service Provider)들이 제공하는 Internet 망을 이용하여 구축하여 기존 사설망 구축에 드는 장비, 회선 비용 획기적으로 절감

㉰ 해당 ISP가 있는 곳이면 어디서든 접속 가능하고 관리 비용이 감소하였다.

㉱ 구축방법의 다양화로 IPSec (IP Security Protocol), MPLS (Multi Protocol Label Switching) 등이 있다.

③ VPN 단점

㉮ TCP/IP에 1번의 암호화를 추가 시켰기 때문에 TCP/IP에 비하여 속도가 떨어지는 단점을 갖고 있다.

㉯ 표준의 부재로 명확한 표준이 없어 ISP마다 다른 기술을 채택하고 있어 상이한 ISP 간의 연동에 문제발생 된다.

2.4 SSL (Secure Sockets Layer)

2.4.1 SSL 개념 및 특징

① SSL 개념

넷스케이프사가 개발한 Internet 상거래시 개인 정보 보안 유지 프로토콜로 TCP/IP계층과 어플리케이션 계층(HTTP, TELNET, FTP 등) 사이에 위치하여(5계층) 데이터를 송수신하는 두 컴퓨터 사이 즉, 종단 간 서비스를 제공한다. SSL 프로토콜은 Netscape에 의해 개발되어 현재 Internet Explore, Netscape, AQL 및 Opera 와 같은 대중적 웹브라우저에 지원된다. SSL은 전자거래의 위험성인 정보 도용(Sniffing), 불법사이트(Spoofing) 등을 막기 위해 SSL 인증서를 설치함으로써 위험성을 해결할 수 있다.SSL은 전자서명기술을 기반으로 한 암호화 프로토콜이며 이 기술이 적용된 전자문서는 별도의 암호화 과정을 거쳐 상대방에게 전달되므로 정보송신자의 수신자 외에는 별도의 암호화 과정을 거쳐 상대방에게 전달되므로 정보송신자와 수신자 외에는 그 내용을 해독할 수 없다. 따라서 전자 문서가 전송되는 도중에 해커가 Sniffing을 시도한다 해도 정보가 암호화 되어 있어 내용을 파악할 수 없다. (단 SSL 보안접속은 데이터의 이동 경로상에서 데이터의 유출만을 막아준다. 일단 상대 호스트에 안전하게 데이터가 전송된 후에도 호스트 관리자에 의한 신용정보 노출이나 해킹에 의한 자료 유출은 막을 수 없다.) SSL이 가동되기 위해서는 인증기관에서 발행된 SSL인증서가 웹서버에 설치되어 있어야 하고 그리고 나서야 SSL은 브라우저와 웹서버 상호간에 전송되는 Data를 암호화 하는데 사용할 수 있다. 브라우저는 http를 https로 바꾸거나 조그마한 자물쇠모양을 표시함으로서 SSL보안 세션을 나타낸다.

② SSL 특징

애플리케이션 내부에서 함수 형태로는 이용이 가능한 반면에 컴포넌트 환경을 지원해 주기 위한 API 호환 기능을 충분히 가지고 있지는 않으며, 한번 설정된 SSL 연결에 대해서는 모든 데이터들을 암호화해야만 한다.

2.4.2 SSL 등장 배경 및 필요성

① SSL 등장 배경

최근 네트워크상의 정보량이 기하급수적으로 증대되면서, 개방형 시스템에 대한 보안 문제의 중요성이 대두되고 있다. 이에 따라 보안과 암호 API에 대한 전문 지식을 모두 갖춘 개발자의 수요가 증가하고, 분산 환경 하에서 애플리케이션에 표준화된 암호화 API 도입이 필요하게 되었다. 현재, 정보에 대한 보안 프로토콜로 SSL이 가장 일반적으로 이용되고 있다.

② SSL 필요성

Internet상의 모든 정보는 TEXT를 기반으로 전송된다. 우리가 흔히 Internet 쇼핑, 증권, 기업간의 전자상거래 등 중요한 정보를 입력할 때 거래당사자의 신원 및 거래내용의 위, 변조여부 확인이 불가능 하다는 치명적인 문제점을 안고 있을 뿐 아니라 신용카드번호, 신상정보 등 중요한 개인정보가 전송되는 중간 단계에서 제 3자에게 유출될 위험이 존재한다. 이러한 문제를 보안하기 위하여 SSL의 중요성이 대두되고 있다.

2.4.3 SSL 주요 기능 및 장단점

① SSL 주요 기능

웹서버에 SSL(Secure Sockets Layer) 인증서를 설치할 경우 이 기술이 적용된 전자문서는 별도의 암호화 과정을 거쳐 상대방에게 전달되므로 정보 송신자(웹브라우저에 정보를 입력하는 사용자)와 정보 수신자(해당 사이트의 웹서버 관리자) 외에는 그 내용을 해독할 수 없다. 따라서 전

자문서가 전송되는 도중에 해커가 Sniffing을 시도한다고 해도 정보가 암호화되어있기 때문에 그 내용을 절대로 파악할 수 없다.

㉮ 신원 확인

SSL 서버인증서는 회사에 대한 방문 조사 후 발급되기 때문에 고객들은 서버인증서를 확인하여 귀사의 웹 사이트가 실제로 존재하고, 귀사의 소유임을 확인할 수 있다.

㉯ 메시지의 비밀보장

SSL로 웹서버와 고객과 교환된 정보(신용카드 번호 등)을 하나의 Session키로 암호화한다. 이Session키를 안전하게 고객에게 전달하기 위해서는 귀사의 공개키로 암호화하여 보낸다. 하나의 Session키는 한번만 사용된다. 그리고 각 Session에 한 고객에게 하나의 키가 사용된다. 따라서 권한이 없는 사용자는 이를 중간에 가로채어 볼 수 없다.

㉰ 메시지의 무결성

메시지가 전송 될 때, 메시지의 내용에 따라 수신자와 발신자의 컴퓨터에서 암호화 방식을 생성, 한글자라도 전송 중 수정되어지면 수신 받은 컴퓨터에서 다른 암호방식을 생성하여 수신자에게 경고를 보낸다. 메시지의 무결성으로 두 당사자가 서로에게 보내주는 메시지가 그대로 전달되었음을 알 수 있다.

② SSL 장점

㉮ 정보유출 방지

학교, PC방과 같은 공공장소에서 컴퓨터를 사용 시 SSL이 미설치된 경우 Sniffing Tool을 사용하여 개인정보의 유출될 수 있는 위험을 방지

㉯ 데이터 변조방지

각종 통신 환경을 이용하여 컴퓨터 내의 정보 또는 데이터의 전송 결과를 임의로 변조하는 범죄의 일종으로서 제 3자의 악의적인 개입으로 인한 데이터 변조를 방지

③ SSL 단점

모든 데이터들을 암호화 하는데서 가져오는 높은 시스템 부하로 인해 오버헤드가 발생하는 단점을 가진다.

2.5 IPSec (Internet Protocol Security)

2.5.1 IPSec 개념 및 특징

① IPSec 개념

IPSec은 Internet Protocol Security 의 약어로서 network 통신 중 network layer에서의 보안을 위한 표준이다. IPSec은 Internet 상에서 VPN(Virtual Private Network)을 구현하는데 사용될 수 있도록 IETF (Internet Engineering Task Force)에서 개발된 protocol set이다.

② IPSec 특징

IPSec은 네트워크상의 IP layer에서의 보안에 중점을 두었으며, 사설 및 공중망을 사용하는 TCP/IP 통신을 보다 안전하게 유지하기 위한 end-to-end encryption과 authentication을 제공한다. 따라서 PGP와 같은 application에 대해서는 고려하지 않는다. 다음은 IPSec을 구성하는 RFC이다.

2.5.2 IPSec 등장 배경 및 필요성

① IPSec 등장 배경

안전에 취약한 Internet에서 안전한 통신을 실현하는 통신 규약. Internet상에 전용 회선과 같이

이용 가능한 가상적인 전용 회선을 구축하여 데이터를 도청당하는 등의 행위를 방지하기 위하여 만들어졌다.

② IPSec 필요성

IPSec은 사용자 측 단말기에 탑재할 수 있으며, Internet을 거쳐 특정 클라이언트와 서버만이 IPSec으로 데이터를 주고받을 수 있다. 암호화나 인증 방식은 규정되어 있지 않으나 이들 방식을 통지하기 위한 틀을 제공하고 있는데, 이 틀을 보안 연관(SA)이라고 한다. SA 정보는 SA 데이터베이스에 보존해 두고 있으며 몇 개의 SA가 등록되어 있다. IPSec 이용 상 주의 사항으로는 NAT 기능을 구비한 침입 차단 장치 등과의 공존 방법이 있다. 원칙적으로는 대향하는 2개의 NAT 장치 간에 IPSec 게이트웨이를 설치해야 한다.

2.5.3 IPSec 주요 기능 및 장단점

① IPSec 주요 기능

안전에 취약한 Internet에서 안전한 통신을 실현하는 통신 규약. Internet상에 전용 회선과 같이 이용 가능한 가상적인 전용 회선을 구축하여 데이터를 도청당하는 등의 행위를 방지하기 위한 통신 규약이다.

② IPSec 장점

㉮ Transparency IPSec은 network layer에서 동작하므로, 사용 application과는 무관하게 동작한다. HTTP에서만 동작하는 SSL과는 다르게, IPSec은 FTP, HTTP, SMTP등 모든 TCP/IP 프로그램에 대한 연결에 대하여 security를 보장한다. 또한 SSL, S/MIME등과 같은 상위 layer의 보안 프로토콜과 연계하여 사용가능하다.

㉯ Network Topology 의존성이 없다. TCP/IP 프로토콜을 사용하므로 Ethernet, TokenRing, PPP등 모든 network topology에 사용할 수 있다.

㉰ 표준화 L2F등으로 구현될 수 있는 PPTP같은 tunneling protocol과는 다르게, L2FIPSec은 표준화된tunneling, authentication, encryption 방법을 사용한다.

㉱ Multiprotocol IPSec은 tunneling mode를 사용할 경우 여러 프로토콜과도 동작할 수 있다. IPX, Appletalk의 경우 오랫동안 ip tunneling을 사용할 수 있으므로 IPSec 또한 적용 가능하다.

㉲ 개별 사용자 컴퓨터의 변경 없이도 보안에 관한 준비가 처리될 수 있다는 것이다.

③ IPSec 단점

IPSec은 해킹기술로 인해 보안이 많이 취약해져있다. 현재는 SSL-VPN을 부분적으로 이용하여 보안을 강화시키기도 한다.

2.6 SSL-VPN

2.6.1 SSL-VPN 개념 및 특징

① SSL-VPN 개념

SSL(Secure Sockets Layer)은 웹 서버와 웹 브라우저간의 안전한 통신을 위해 넷스케이프에서 제창한 프로토콜로 Internet 익스플로러, 넷스케이프 네비게이터와 같은 웹 브라우저에 기본적으로 탑재돼 있는 보안 표준 프로토콜이다.

② SSL-VPN 특징

SSL은 오늘날 온라인 상거래, 웹서비스, 그리고 안전한 애플리케이션 계층 액세스를 포함하는 많은 다른 네트워크 기능을 위해 보안을 제공하는 Internet 보안 프로토콜의 선두주자다. 현재 SSL의 2.0, 3.0, 3.1(TLS 1.0)이 사용되고 있으며, 아래와 같은 중요한 보안 기능들을 사용해

Internet 등 공개된 네트워크상에서 민감한 데이터의 전송을 가능하게 한다.

㉮ 상호인증

클라이언트와 서버간의 상호 인증(RSA, DSS, X.509)·기밀성 : 대칭키 암호화 알고리즘을 통한 데이터의 암호화(DES, 3DES, RC4등)

㉯ 데이터 무결성

MAC기법을 이용해 데이터 변조 여부 확인(md5,SHA-1)

2.6.2 SSL-VPN 등장 배경 및 필요성

① SSL-VPN 등장 배경

지난 몇 년 동안의 기술적인 동향은 안전한 네트워크 액세스를 위해서 저가의 광대역 서비스를 통한 Internet과 암호화 기술을 사용하는 것이었다. 특히 기업 및 기관들이 업무적인 생산성을 개선하고 비용 절감 차원에서 전용선과 모뎀 설비를 광대역으로 대체하기 시작했다. Internet 연결성의 편리성으로 인해 언제 어디서든 네트워크 접속이 용이해지면서 통신의 비밀을 보장하기 위해 암호화를 사용하는 동안, 기업은 재택근무자, 원격 근무자 또는 이동 근무자들을 위해 내부 컴퓨팅 자원을 효율적으로 액세스하게 해줘 전반적인 네트워크 및 컴퓨팅 환경에 대한 비용의 절감을 실현할 수 있었다.

② SSL-VPN 필요성

현재 SSL-VPN은 웹, 웹 애플리케이션, 메시징 클라이언트, 이메일, 파일 공유, 클라이언트/서버 애플리케이션 등 기업의 핵심적인 모든 업무 형태를 모두 지원함으로 업무 적용의 한계가 완전히 극복된 상태며, 자체적으로 DMZ 서비스를 지원해 인트라넷의 사설 IP 네트워크 구성 시에도 정상적인 서비스 구현이 가능하다. 또한, 다양한 암호화 기법(DES, 3DES, RC4)과 데이터 무결성 기법(MD5, SHA-1)을 모두 지원한다.

2.6.3 SSL-VPN 주요 기능 및 장단점

① SSL-VPN 주요 기능

SSL-VPN은 사용자와 SSL-VPN 장비 사이의 안전한 데이터의 교환을 위해 애플리케이션 계층에서 SSL을 이용한 암호화 서비스를 제공함으로써 기존 VPN의 문제점인 네트워크와 방화벽을 통과할 경우 발생하는 포트 블럭(Port Block)과 같은 문제점을 해결한다. 또한 SSL-VPN은 클라이언트리스 VPN이라고 부르기도 하는데 그 이유는 오늘날 대부분의 표준화된 웹 브라우저는 HTTP와 HTTPS(SSL)를 기본적으로 모두 지원하므로 IPSec 리모트 VPN과는 대조적으로 사용자 측면에 VPN 클라이언트의 설치, 구현, 그리고 지원과 함께 결부된 모든 문제들을 해결할 수 있다. SSL은 웹 브라우저와 웹 서버간의 안전한 통신을 위해 넷스케이프에서 개발됐고, 애플리케이션에서 암호화가 이뤄지기 때문에 하위 레이어의 다양한 프로토콜 및 응용 프로그램의 지원에 제한을 받게 된다. 그래서 SSL-VPN업체들은 초창기 웹 및 웹 기반의 애플리케이션만을 지원했으며, 고객 및 시장의 확장성을 위해 대부분의 SSL-VPN 업체들은 기업의 다양한 애플리케이션을 지원하기 위한 기술 투자에 많은 시간을 투자해야 했다. SSL-VPN을 이용한 서비스의 지원 발전 단계는 다음과 같이 3단계로 발전해왔다.

㉮ 초기 단계

웹, 웹 기반의 애플리케이션, 파일 공유 지원

㉯ 확장 단계

클라이언트 / 서버 애플리케이션 지원

㉰ 성숙 단계

UDP 트래픽, 네트워크 레이어 트래픽 지원

② SSL-VPN 장점

SSL-VPN은 기존의 IPSec이 제공하지 못했던 이동성이나 확장성 등에서 뛰어나다. 값비싼 장비나 소프트웨어를 따로 설치할 필요 없이 기업 내 통신망과 Internet이 연결되기만 한다면 지역적인 제한 없이 편리하게 업무를 수행할 수 있기 때문이다.

㉮ SSL (HTTPS)는 표준 웹 브라우저에 기본적으로 포함된다.

㉯ 광범위한 애플리케이션의 지원.

㉰ VPN은 NAT와 proxy 장비 사이에서 투명하게 동작한다.

㉱ SSL-VPN은 사용자와 서버 사이에서 방화벽에 의해 서비스의 영향을 받지 않는다.

㉲ 단 시간 내에 보안망 구축이 가능하다.

㉳ 그룹 단위의 세분화된 서비스 정책 구현.

㉴ 다양한 사용자 인증서비스 제공.

③ SSL-VPN 단점

아직 도입 초기의 검증되지 않은 기술이라는 점 때문에 빠른 확산이 이뤄지지 않고 있다.

㉮ SSL-VPN은 일반적으로 Site-to-Site VPN 형태로 사용하지 않고 IPSec/IKE VPN를 사용한다.

㉯ SSL-VPN은 SSL-VPN장비로 트래픽을 통과시키기 위해 방화벽에서 HTTPS (TCP 443) port를 오픈해야 한다.

㉰ SSL-VPN은 리모트 사용자 PC의 보안성을 검증하기 위해 타 업체의 기술이나 통합 보안 설비를 요구한다.

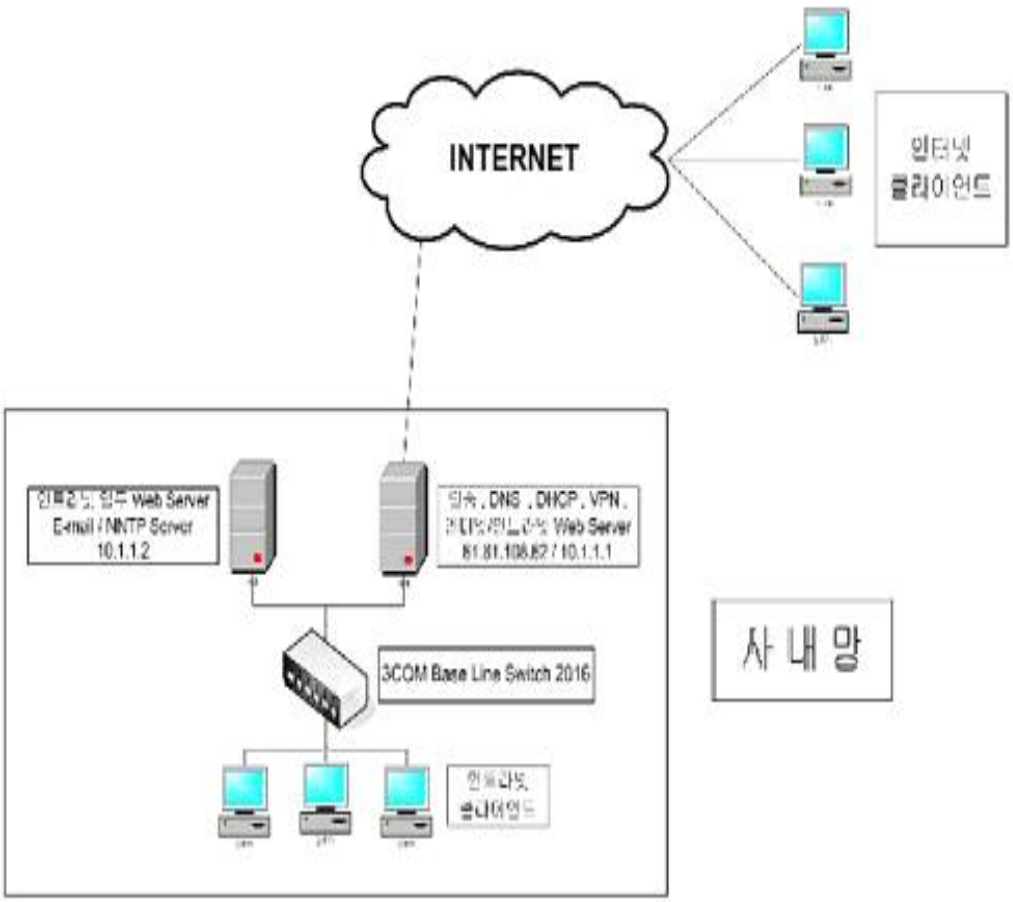
3. 구축 및 운영

3.1 원격 연결 서비스 설계

3.1.1 망 구성도

이번 졸업 작품은 도메인을 plhs.com를 사용하고 10.1.1.X의 IP주소를 사용한다. Main Server (rca.plhs.com = 10.1.1.1)는 인트라넷을 구축하기 위해서 DNS Server, DHCP Server, Active Directory, 인증기관이 구축되고 웹사이트로 Internet 웹사이트 (61.81.108.62)와 인트라넷 웹사이트 (www.plhs.com)을 구축한다. 그리고 랜카드를 두 개를 사용하여서 하나는 Internet(61.81.108.62)과 하나는 인트라넷(10.1.1.1)과 연결을 하여 VPN Server로서 원격지에서도 VPN에 연결하여 인트라넷을 이용할 수 있게 중개 역할도 수행한다. Sub Server (rweb.plhs.com = 10.1.1.2)는 인트라넷 업무 사이트를 구축하고 또한 인트라넷에서 사용할 수 있게 E-mail Server (mail.plhs.com)와 NNTP Server (news.plhs.com)를 구축한다.

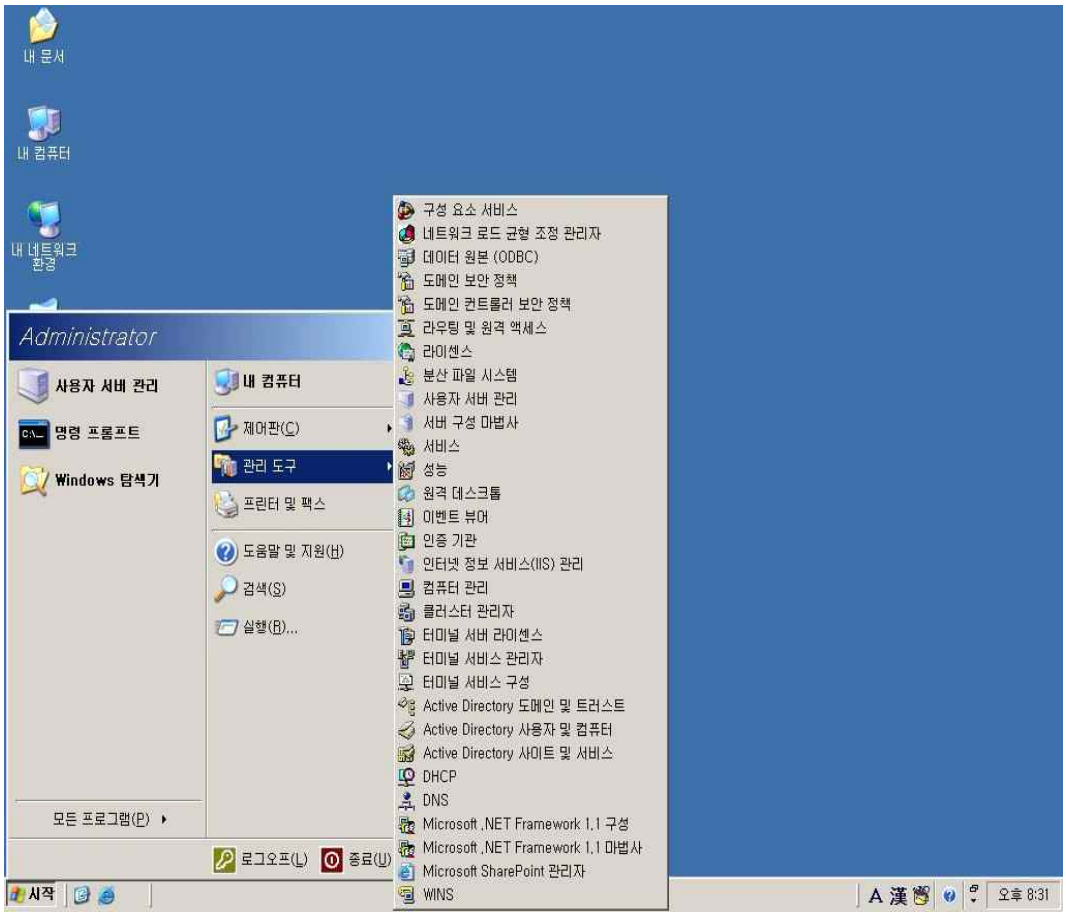
위 내용의 구성도는 아래 [그림 3-1-1]과 같다.



[그림 3-1-1]

3.2 Main Server (rca.plhs.com)

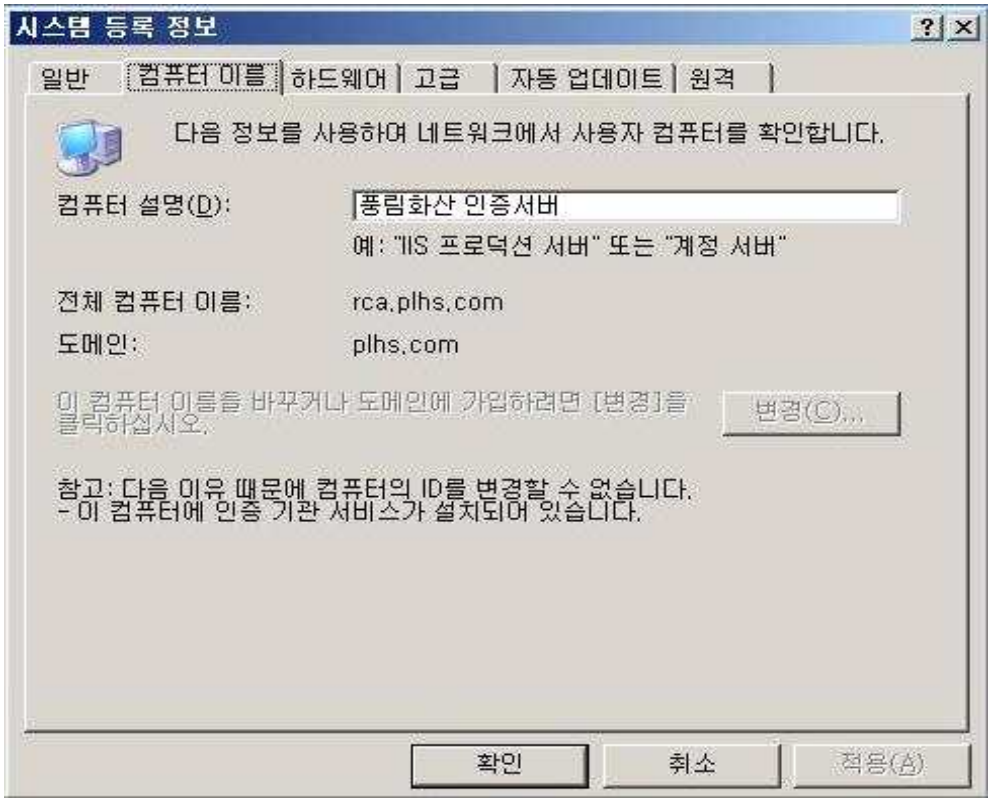
아래 [그림 3-2]은 Main Server (rca.plhs.com)에 DNS, DHCP, 인증기관, IIS, VPN, Active Directory 가 구성된 것 을 보여준다.



[그림 3-2]

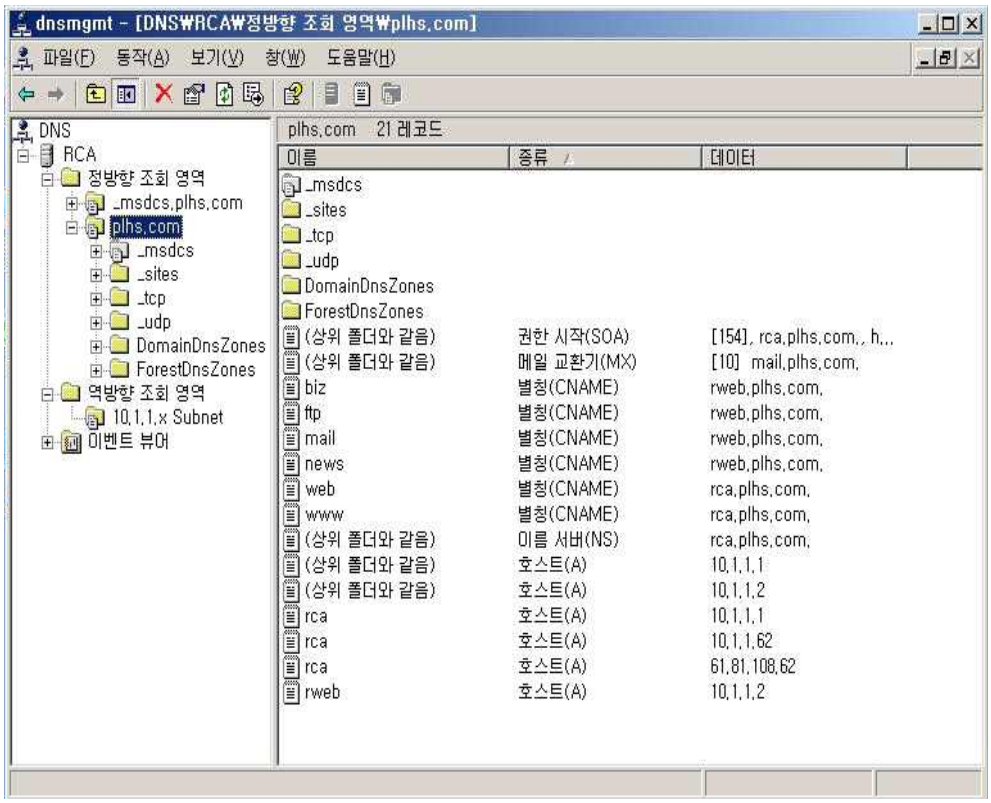
3.2.1 DNS (Domain Name System)

Active Directory 기반의 도메인을 생성하기 이전에 도메인 컨트롤러를 찾기 위한 DNS 구성이 먼저 되어야 한다. Windows 2000, Windows XP, Windows Server 2003 계열의 운영체제들은 자신의 호스트를 이름을 DNS 서버에 동적 업데이트하기 위해 주 DNS 접미사를 사용하고, FQDN 으로 지정하지 않은 이름에 대한 DNS 이름 풀이를 처리하기 위해 주 DNS 접미사를 사용한다. 예를 들어, Windows Server 2003의 명령 프롬프트에서 Ping rca와 같이 명령을 하게 되면 Windows Server2003은 RCA 이라는 컴퓨터 이름을 호스트 이름으로 간주하고 DNS 질의를 하게 된다. DNS 질의를 하기 위해 Ping rca + 주DNS 접미사, 즉, Ping rca.plhs.com과 같이 만들어서 질의하게 된다. 기본적으로 도메인 컨트롤러는 DNS 도메인 이름을 자신의 주 DNS 접미사로 사용하게 되며, 멤버 컴퓨터들은 자신이 소속된 도메인의 DNS 도메인 이름을 자신의 주 DNS 접미사로 사용하게 된다. 이런 설정은 자동으로 이루어진다. 아래[그림 3-2-1a]은 rca 의 주 DNS 접미사를 설정한 그림이다.



[그림 3-2-1a]

DNS Server에 별칭과 호스트가 설정되어 있는 것을 아래 [그림 3-2-1b]에서 확인 할 수 있다.



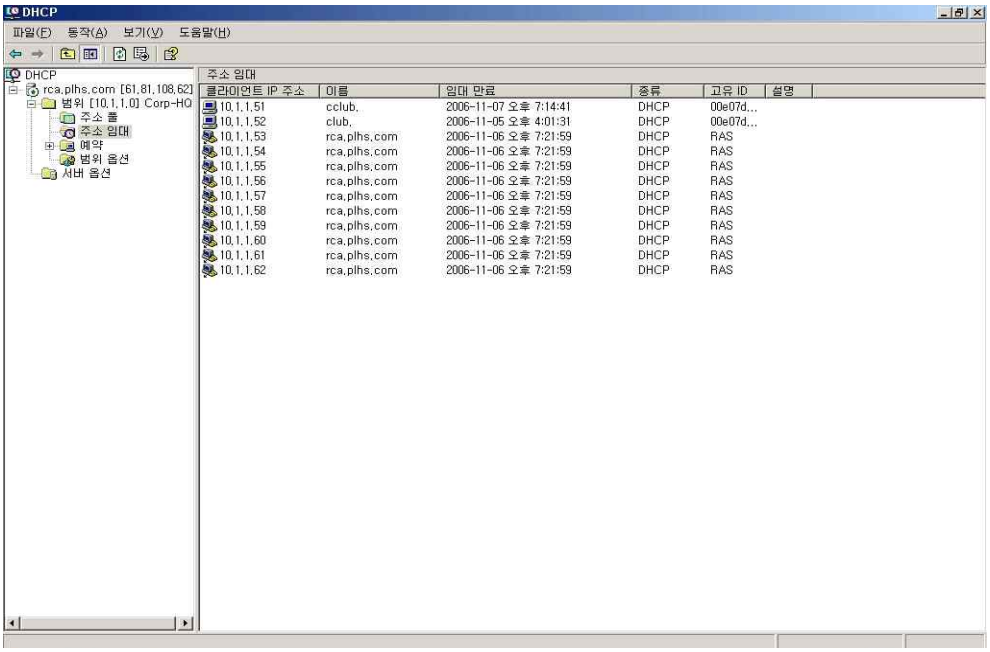
[그림 3-2-1b]

3.2.2 DHCP (Dynamic Host Configuration Protocol)

여러 대의 클라이언트 컴퓨터에 IP 주소와 옵션을 자동으로 할당하기 위해서 사용되는 프로토콜이 DHCP이다. DHCP를 사용하면 Internet 프로토콜을 설정하기 위해 소모되는 시간을 획기적으로 줄일 수 있다. 또한, 수동으로 설정할 때 발생할 수 있는 IP 주소 충돌 발생이 줄어들고, IP 주소가 바뀌어도 쉽게 다시 적용할 수 있다.

Windows Server 2003 DHCP 서버는 임대 기간을 8일로 설정한다. DHCP 클라이언트는 임대 기간의 50%가 경과되었을 때 임대를 갱신해야 한다. 임대를 갱신하기 위해서 클라이언트는 DHCP Request 메시지를 원래 IP를 공급받았던 서버에게 보낸다. 서버는 DHCPAck를 클라이언트에게 보낸다. 이 때, 클라이언트는 사용 중인 IP 주소가 있으므로, IP와 MAC 레벨에서 모두 유니캐스트 한다.

만약, 임대 갱신 프로세스에 임대를 갱신하지 못했다면, 임대 기간의 87.5%가 경과되었을 때 DHCPRequest 메시지를 브로드캐스트한다. 클라이언트가 DHCPAck 메시지를 받는다면, 클라이언트는 IP 주소를 계속 사용하고, 그렇지 않다면, 클라이언트는 초기 임대 프로세스를 다시 진행할 것이다. 아래 [그림 3-2-2]는 DHCP Server에서 주소를 할당한 그림이다.

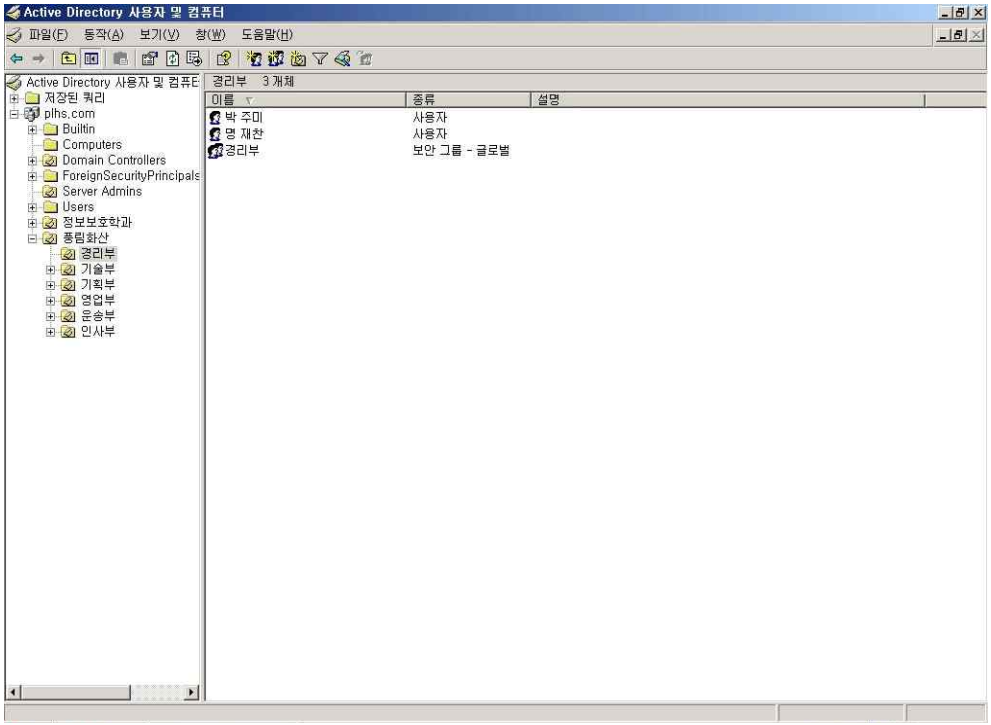


[그림 3-2-2]

10.1.1.1~10.1.1.20 , 10.1.1.21~10.1.1.50 , 10.1.1.251~10.1.1.254는 서버들이 사용할 IP 주소가 DHCP 클라이언트에게 할당되지 않도록 서버들이 사용할 주소 영역을 제외 영역으로 설정을 하였다. (10.1.1.53~10.1.1.62 는 VPN Server 에 할당한 IP 주소이다.)

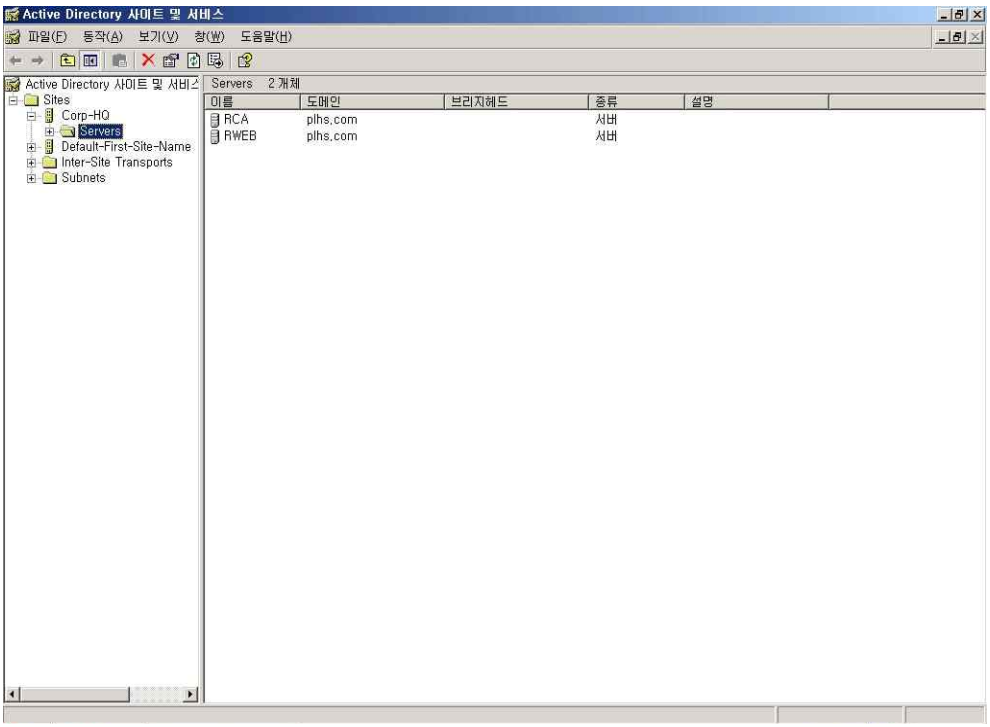
3.2.3 AD (Active Directory)

Microsoft Windows Server System 기반의 네트워크를 올바르게 구축하고 효율적으로 운영하기 위해서는 Active Directory 도메인이 반드시 있어야 한다. 다음 아래 [그림 3-2-3a]은 plhs.com 이라고 하는 공인된 도메인 이름을 Active Directory 도메인의 이름으로 사용하고 도메인 컨트롤러를 DNS 서버로 사용하는 도메인을 생성하여 각 부서 그룹과 사용자를 설정한 것이다.



[그림 3-2-3a]

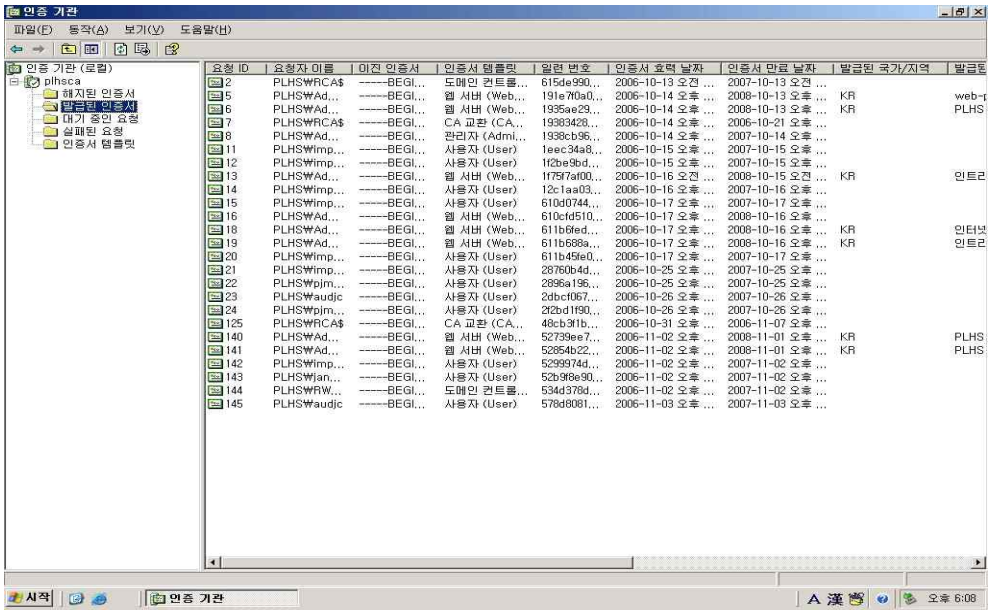
사용자가 Active Directory에서 정보를 찾으려고 할 때나, 로그온 하려고 할 때 도메인 컨트롤러를 찾아야 한다. 만약 도메인 컨트롤러가 여러 대 있다면 물리적으로 가까이에 있는 도메인 컨트롤러에 접근하는 것이 좋다. 아래 [그림3-2-3b]는 사이트 구성을 보여준다.



[그림 3-2-3b]

3.2.4 SSL(Secure Sockets Layer)

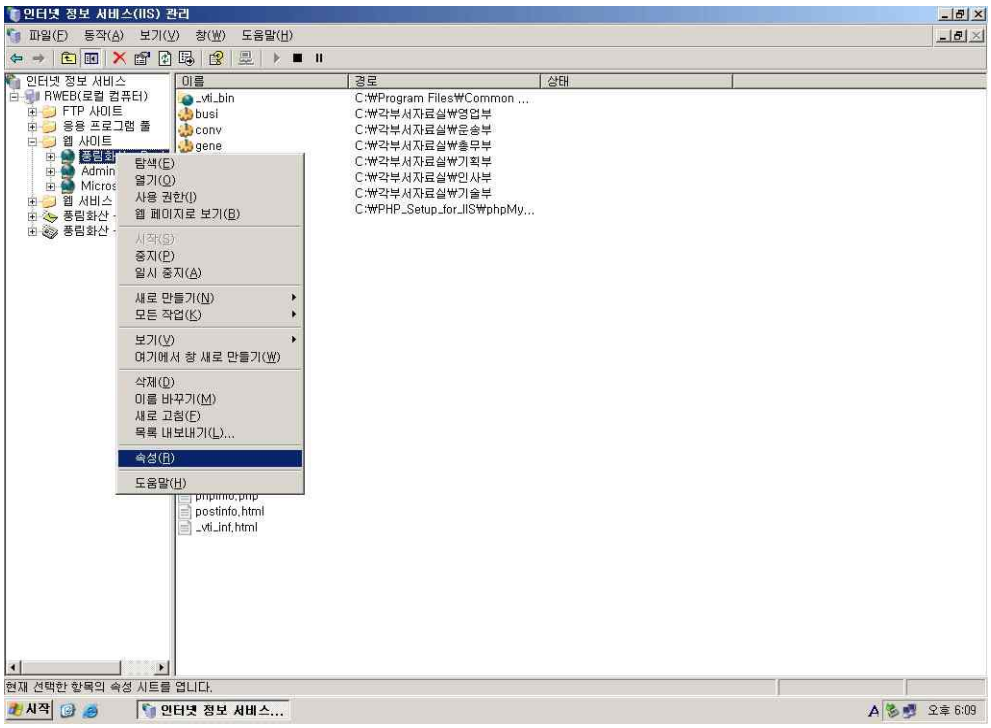
Windows Server 2003은 엔터프라이즈 루트 CA, 엔터프라이즈 하위 CA, 독립 실행형 루트CA, 독립 실행형 하위 CA의 네 가지 종류의 인증기관을 생성할 수 있다. Active Directory 기반의 네트워크에서는 엔터프라이즈 CA를 사용하는 것이 좋다. 다음은 rca에 엔터프라이즈 루트 CA로 구성한 그림이다.



[그림 3-2-4]

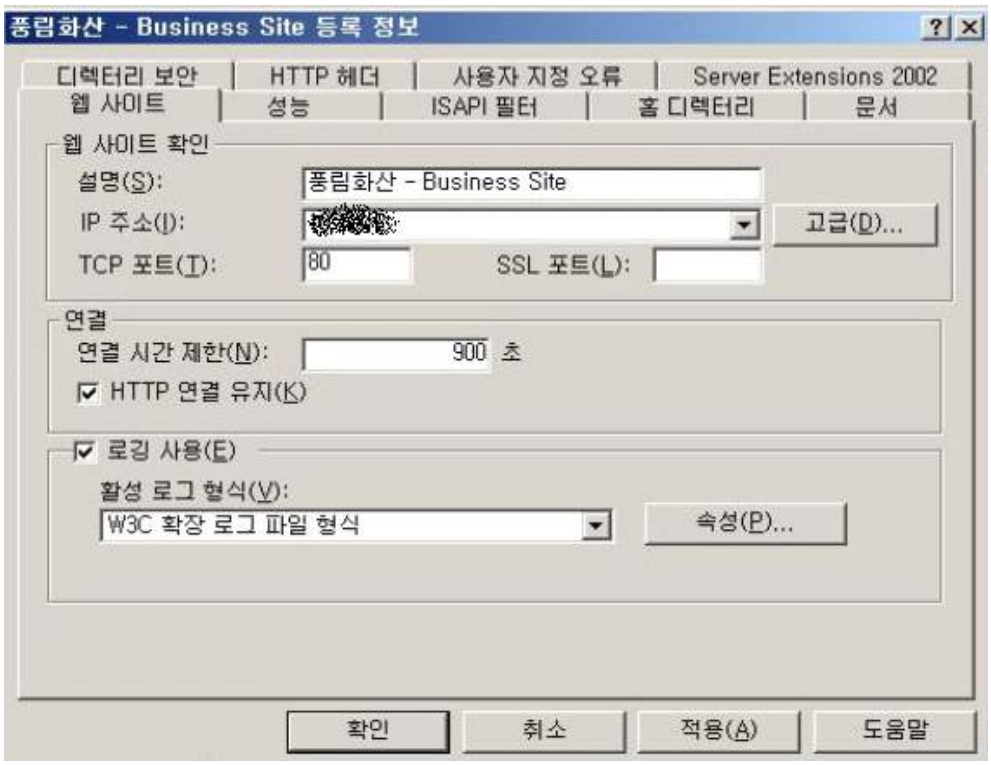
① Sub Server(rweb.plhs.com)의 업무 웹서버에 SSL 사용하기

㉮ Sub Server 로그인 > 시작 > 관리도구 > Internet 정보 서비스 관리 > 웹사이트 > 풍림화산 - Business Site의 등록정보를 연다.



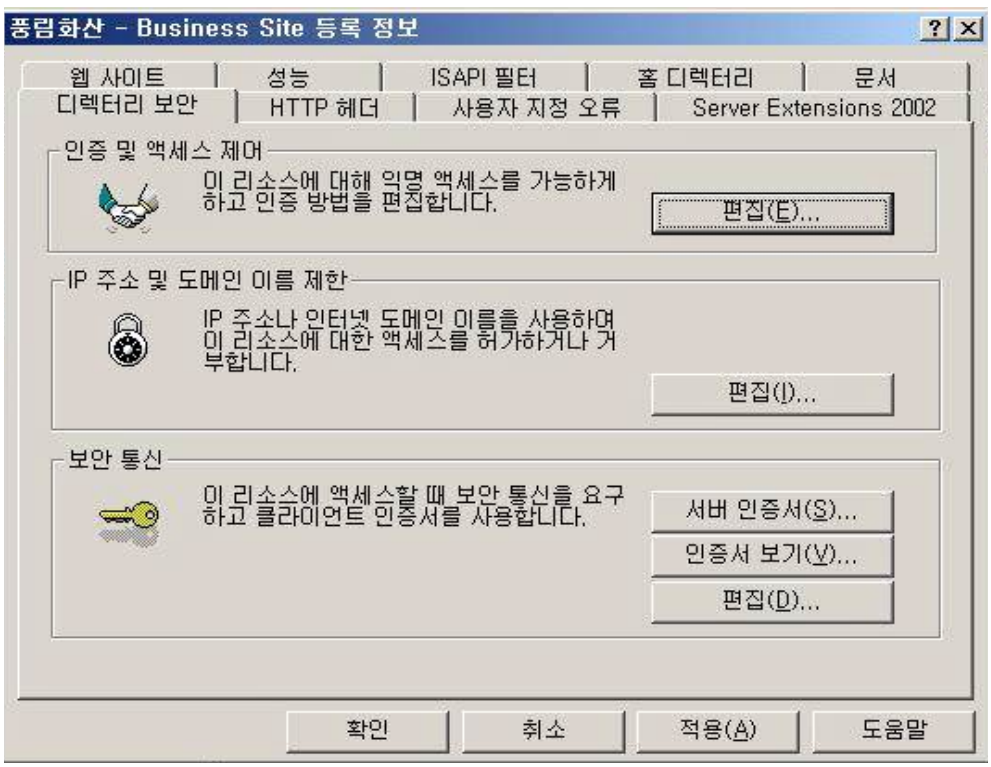
[그림 3-2-4-1-가]

㉰ SSL포트에 아무것도 설정이 안 돼있다는 것을 확인할 수 있다.

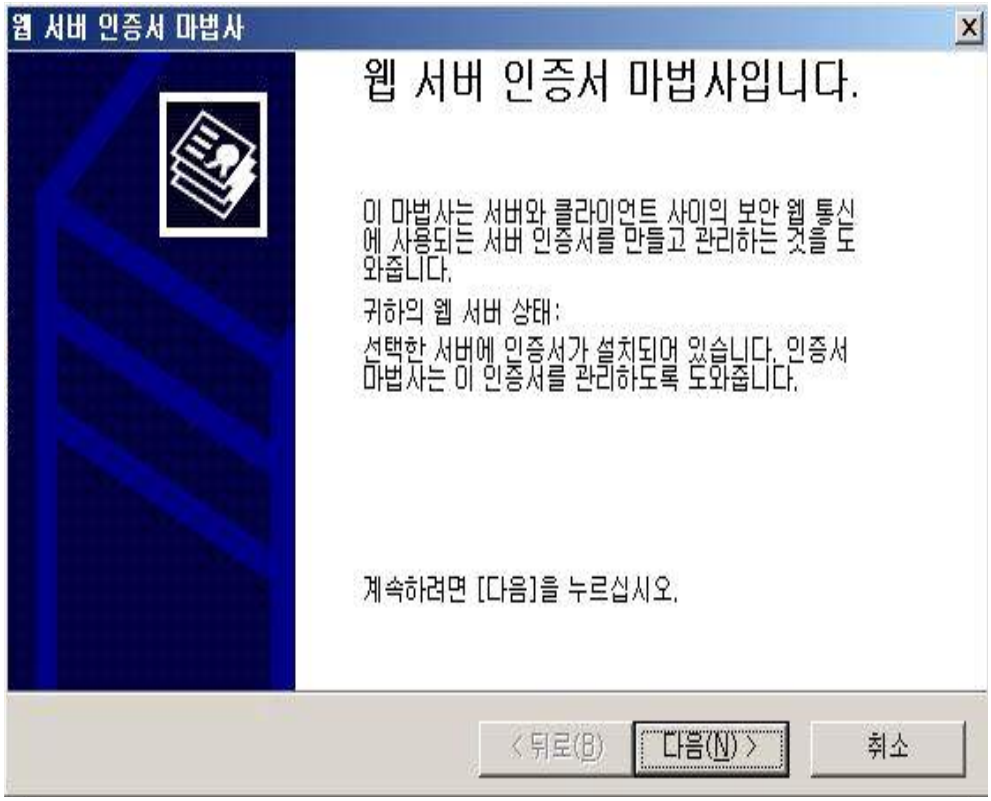


[그림 3-2-4-1-나]

㉱ 디렉터리 보안 창에 서버인증서를 누르면 웹 서버 인증서 마법사가 시작되면 다음을 누른다.

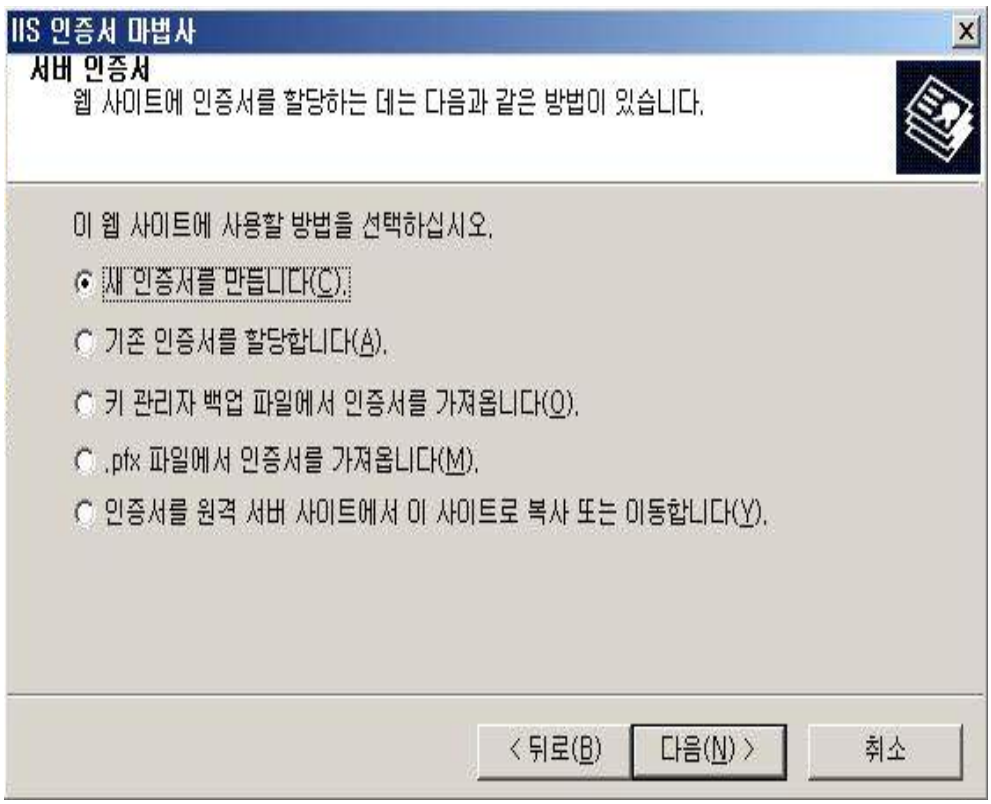


[그림 3-2-4-1-다a]



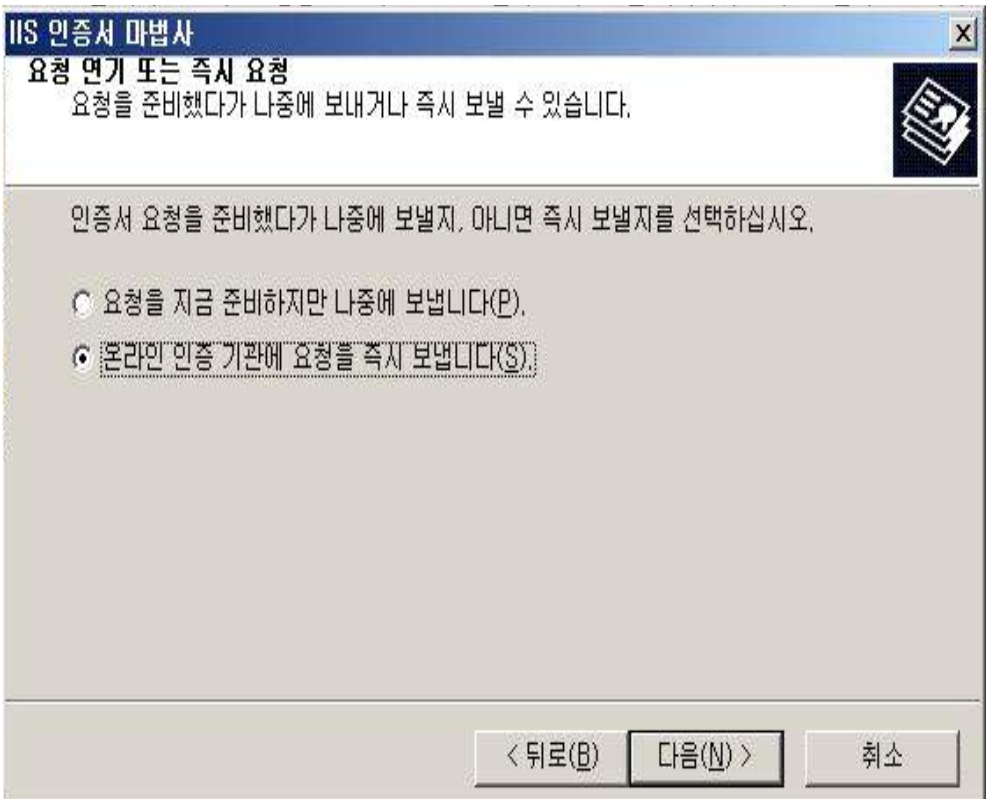
[그림 3-2-4-1-다b]

㉮ 서버 인증서에서 새 인증서를 만듭니다를 선택한 후 다음을 누른다.



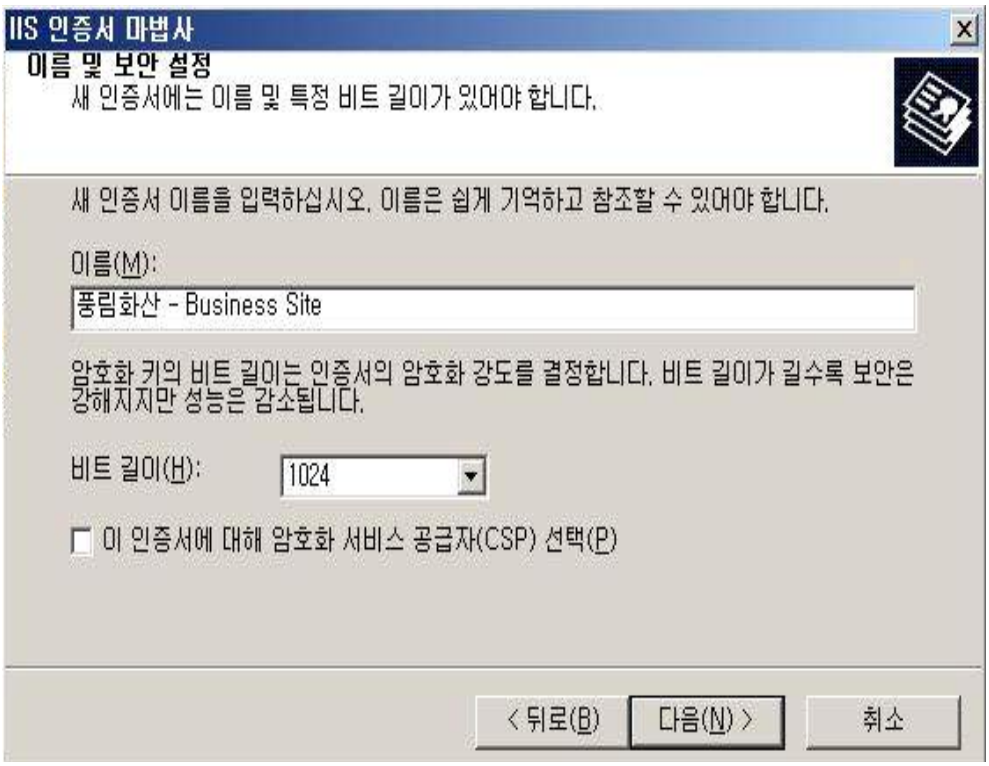
[그림 3-2-4-1-라]

㉮ 요청 연기 또는 즉시 요청에서 온라인 인증기관에 요청을 즉시 보냅니다를 선택한 후 다음을 누른다.



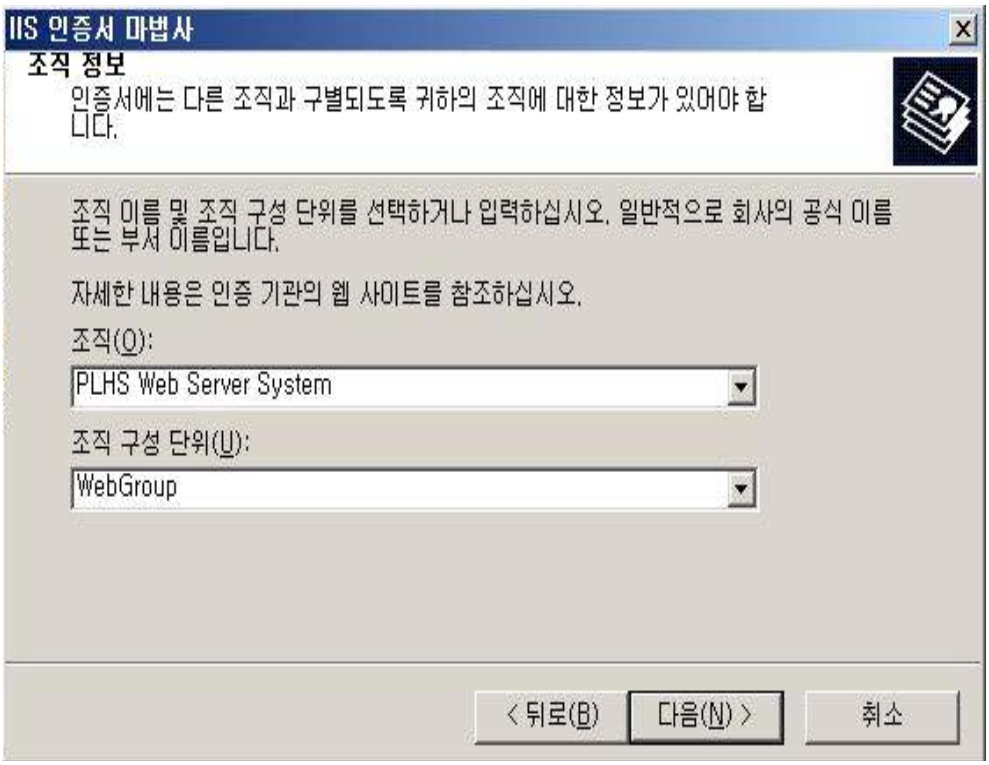
[그림 3-2-4-1-마]

㉯ 이름 및 보안 설정에서 이름에 풍림화산 - Business Site를 확인한 후 다음을 누른다.



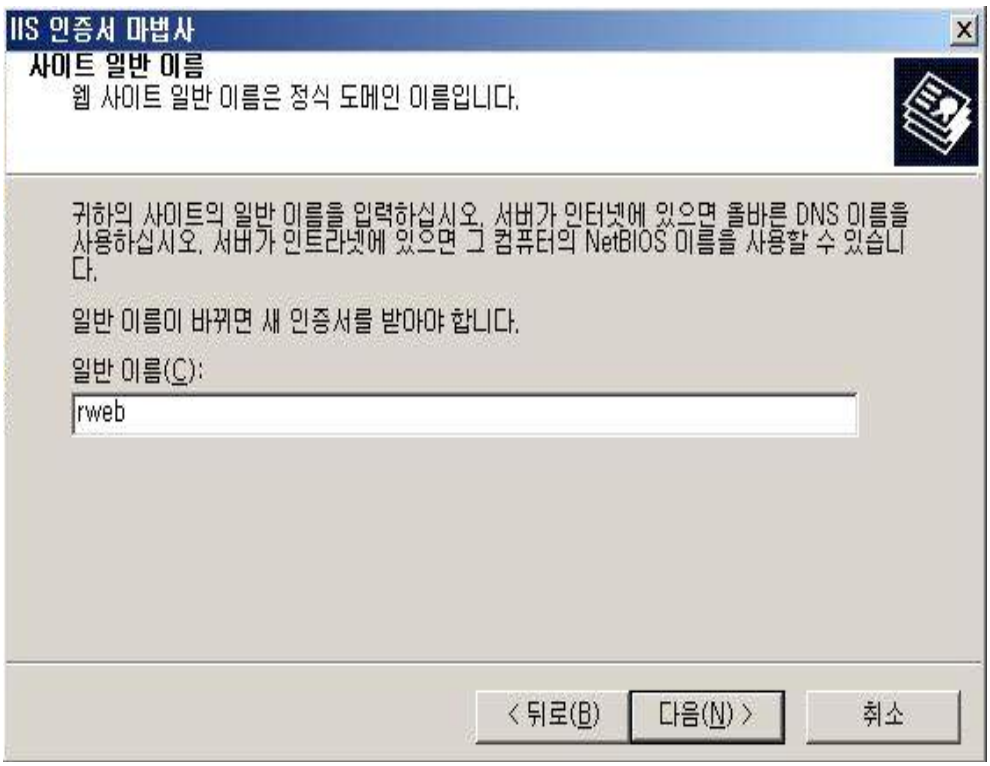
[그림 3-2-4-1-바]

㉮ 조직 정보에서 조직에 PLHS Web Server System, 조직구성단위에 WebGroup인지 확인 후 다음을 누른다.



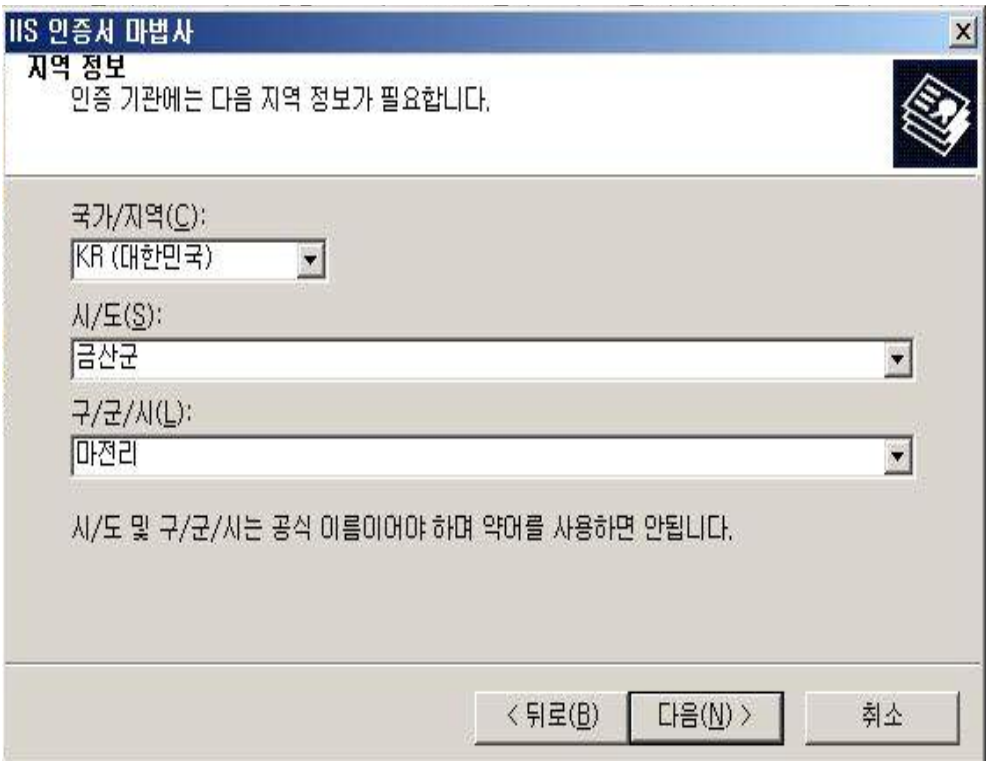
[그림 3-2-4-1-사]

㉯ 사이트 일반 이름에서 일반 이름에 rweb인지 확인 후 다음을 누른다.



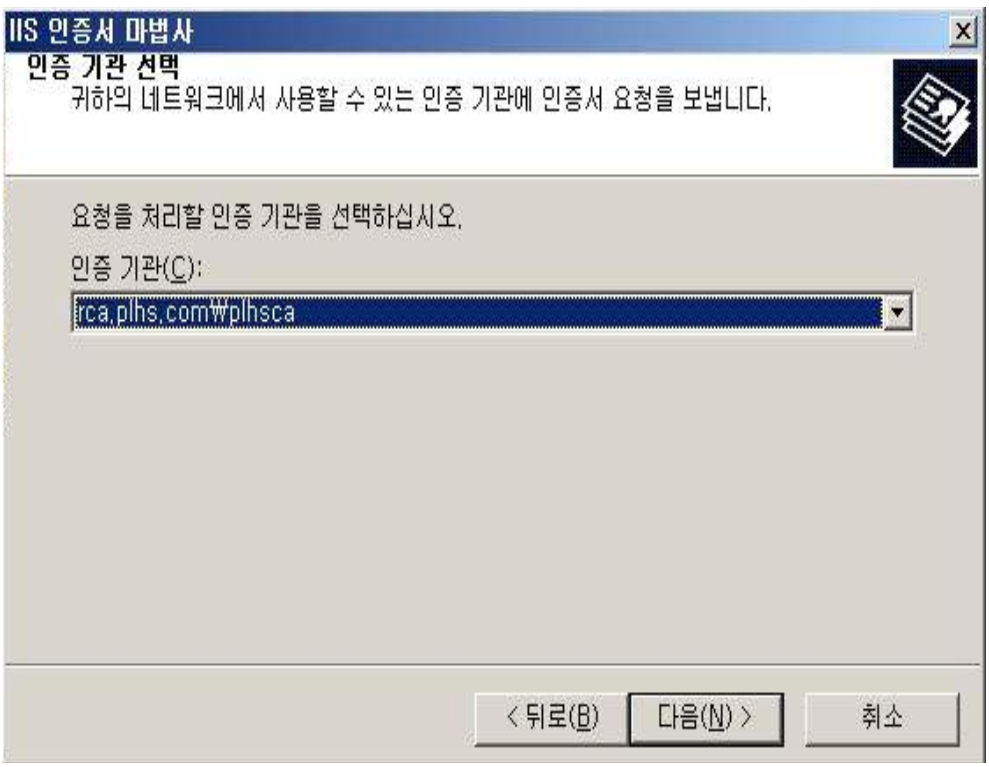
[그림 3-2-4-1-아]

㉦ 지역 정보에서 다음을 누른다.



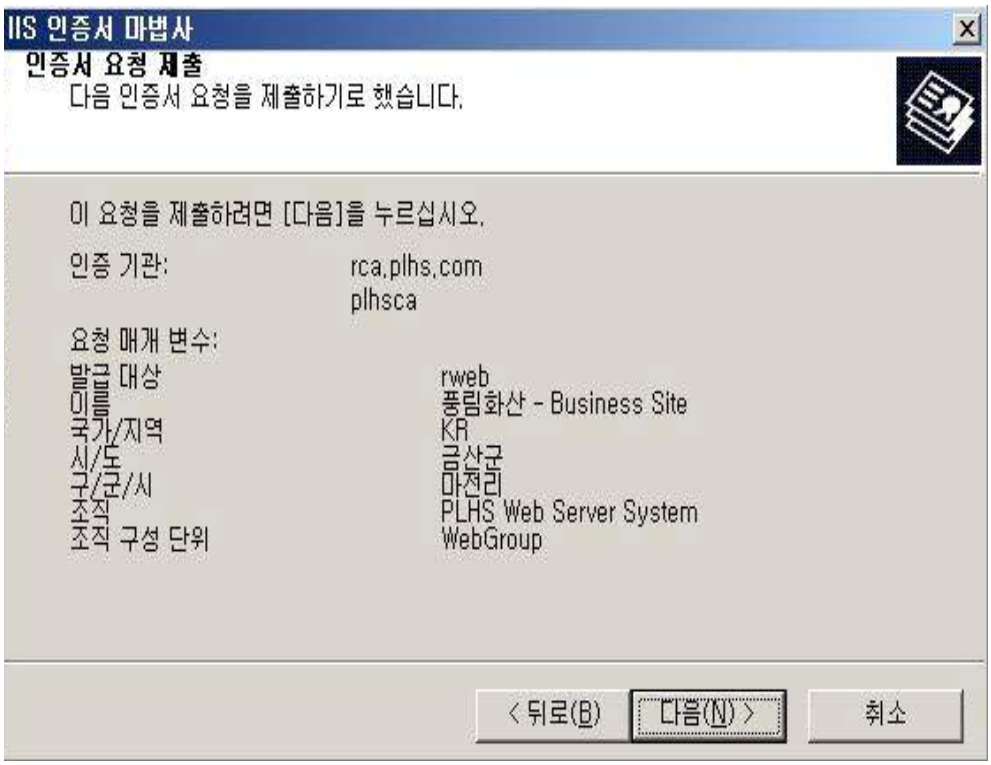
[그림 3-2-4-1-자]

㉧ 인증기관 선택에서 인증기관에 rca.plhs.com₩plhs를 확인하고 다음을 누른다.



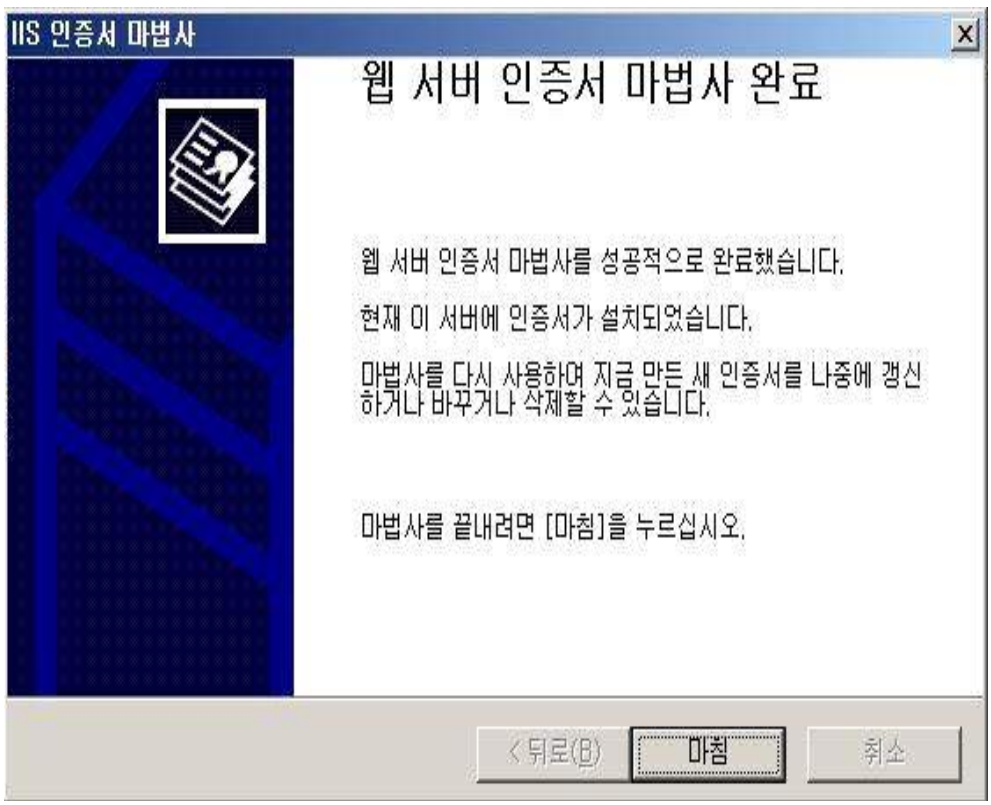
[그림 3-2-4-1-차]

㉮ 인증서 요청 제출에서 다음을 누른다.



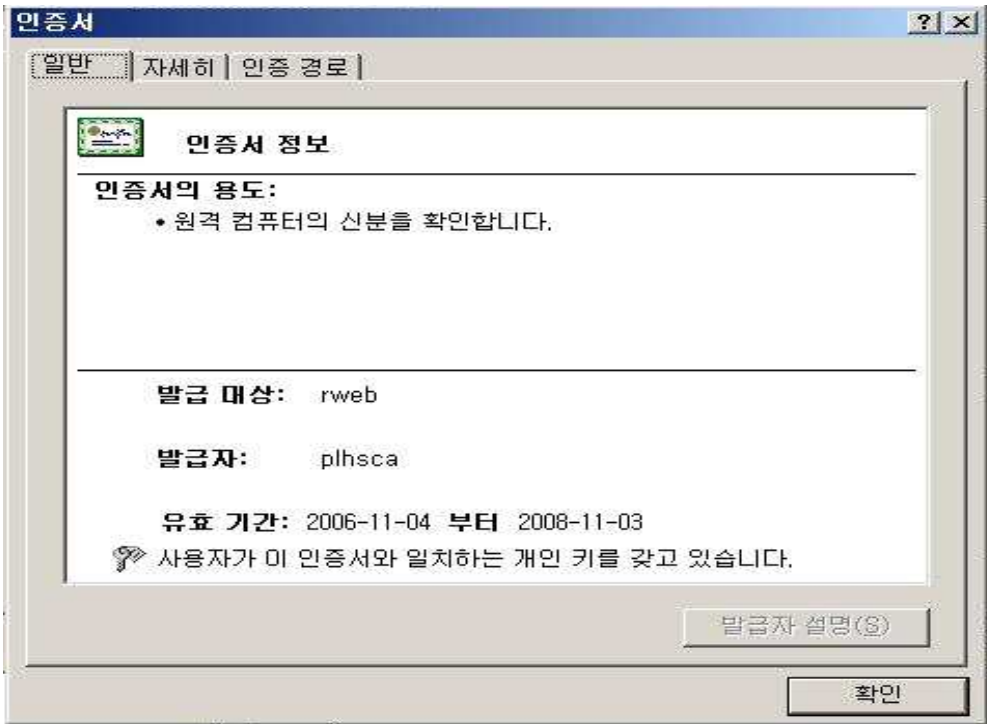
[그림 3-2-4-1-카]

㉯ 웹 서버 인증서 마법사 완료에서 마침을 누른다.



[그림 3-2-4-1-타]

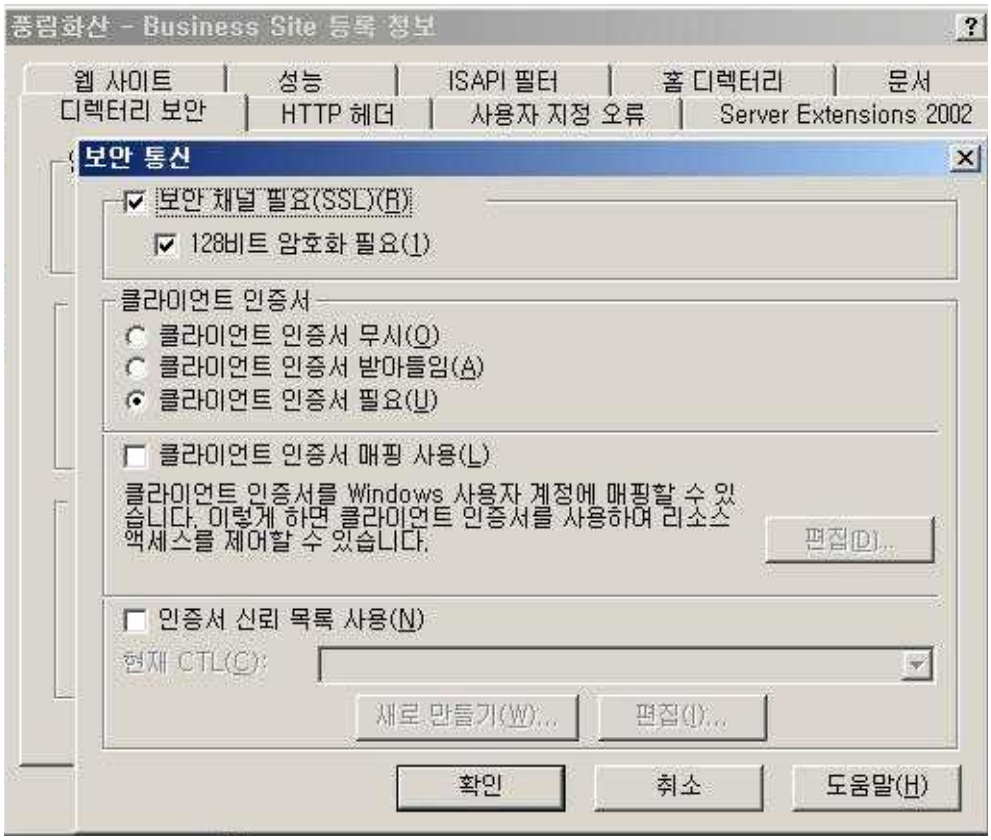
㉮ 디렉터리보안에서 인증서 보기를 누르면 인증서가 있는 것을 확인할 수 있다.



[그림 3-2-4-1-파]

㉯ 등록정보에서 웹사이트에 SSL포트에 443이 지정돼 있는 것을 확인하고 인증서가 있을시 에만 접속할 수 있게 디렉터리보안을 선택하고 보안 통신의 편집을 누르고 보안채널필요(SSL)를 선택, 128비트 암호화 필요를 선택하고 클라이언트 인증서 필요를 선택한다.

[그림 3-2-4-1-하a]



[그림 3-2-4-1-하b]

3.2.5 VPN(Virtual Private Network)

VPN을 이용하기 이전에는 서버와 클라이언트에 모뎀을 전화선을 이용하여 연결한 후 서버의 자원을 이용하였다. 이 방식은 언제 어디서나 이미 구축되어 있는 공중 전화망을 이용하여 접속할 수 있다는 장점이 있는 반면에 낮은 속도와 비싼 전화 사용료를 지불해야 한다는 단점이 있다.

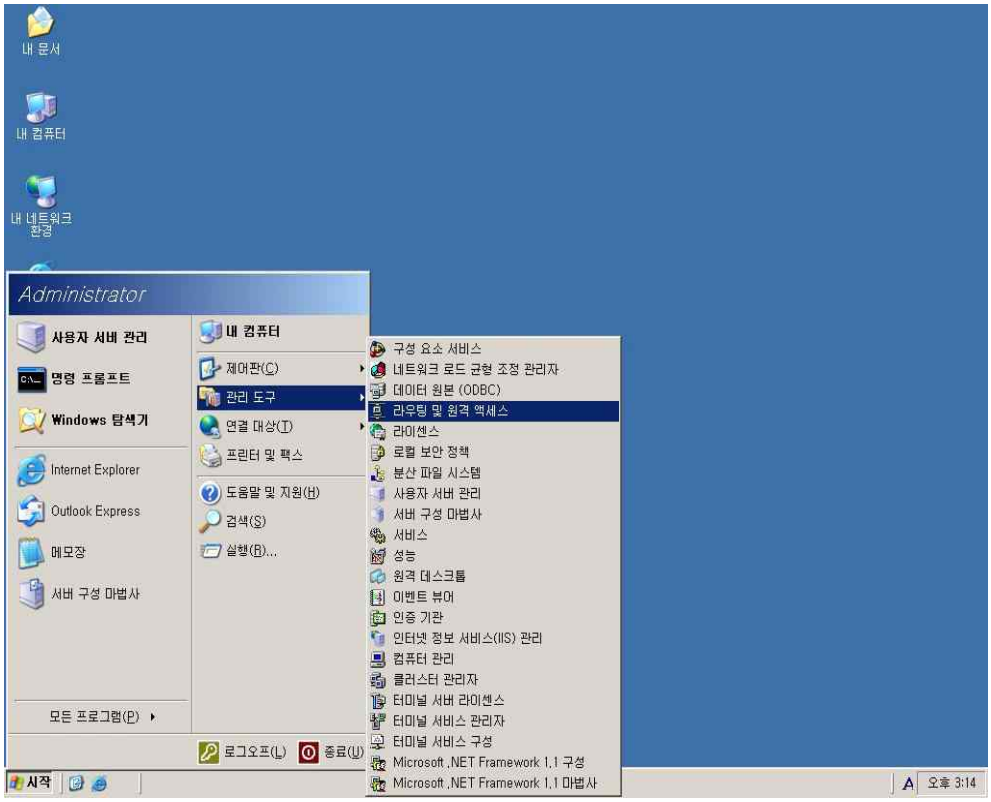
VPN을 이용하면 Internet을 통하여 회사 네트워크에 접근 할 수 있다. 그러나 Internet은 안전이 보장되지 않는 네트워크이다. VPN은 터널링이라는 기술을 통해 Internet에서 가상의 전용 터널을 사용하는 것과 같은 효과를 제공한다. 터널링 기술은 암호화에 의존하고 있다. VPN을 이용하면 고속으로 네트워크를 사용할 수 있고, 네트워크와 네트워크 간의 연결에도 전용선 대신 Internet을 통해서 연결할 수 있다.

Windows Server 2003은 VPN 프로토콜로 PPTP와 L2TP 두 가지를 지원한다. PPTP는 MPPE를 사용하여 연결을 암호화하고, L2TP는 IPSec을 이용하여 연결을 암호화한다. PPTP는 IP 기반의 연결에만 사용할 수 있고, L2TP는 IP, X.25, 프레임 릴레이나 ATM기반의 네트워크에서도 사용이 가능하다.

다음 단계에 따라 라우팅 및 원격 액세스를 이용하여 메인서버(rca.plhs.com)를 VPN 서버로 구성하고 원격 액세스 서버 권한을 부여한다.

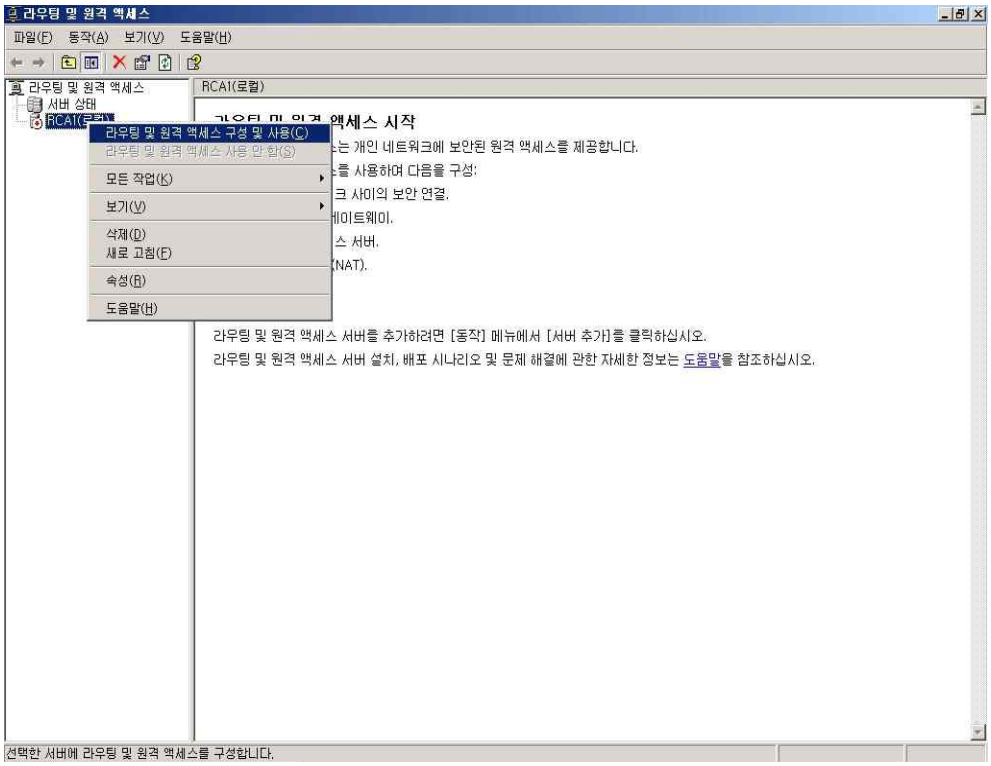
① VPN서버 구축하기

㉮ 시작 > 관리도구 > 라우팅 및 원격 액세스를 선택한다.



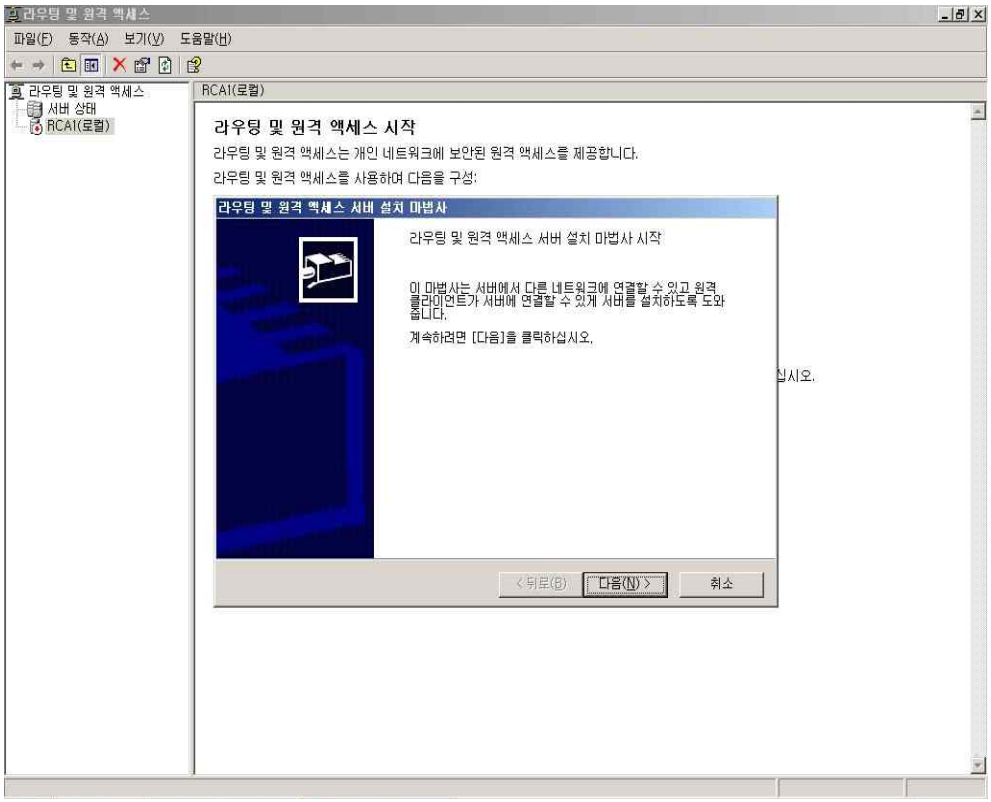
[그림 3-2-5-1-가]

㉯ 라우팅 및 원격 액세스 창에서 RCA를 오른쪽 버튼으로 선택하고 메뉴에서 라우팅 및 원격 액세스 구성 및 사용을 선택한다.



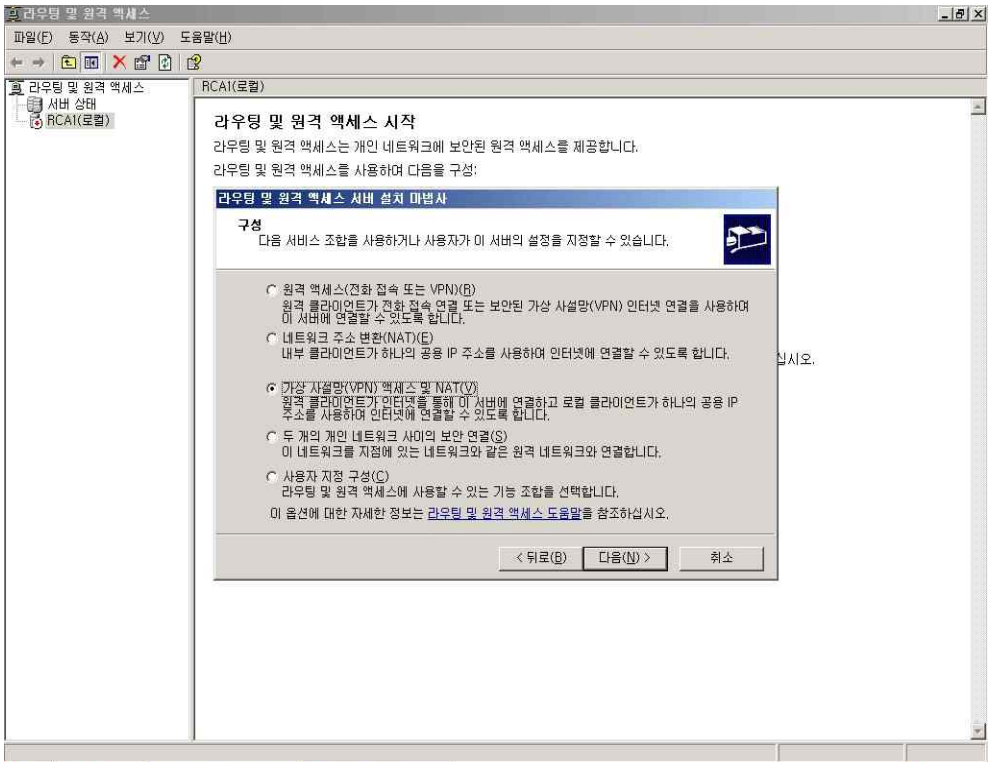
[그림 3-2-5-1-나]

㉰ 라우팅 및 원격 액세스 서버 설치 마법사 창에서 다음을 누른다.



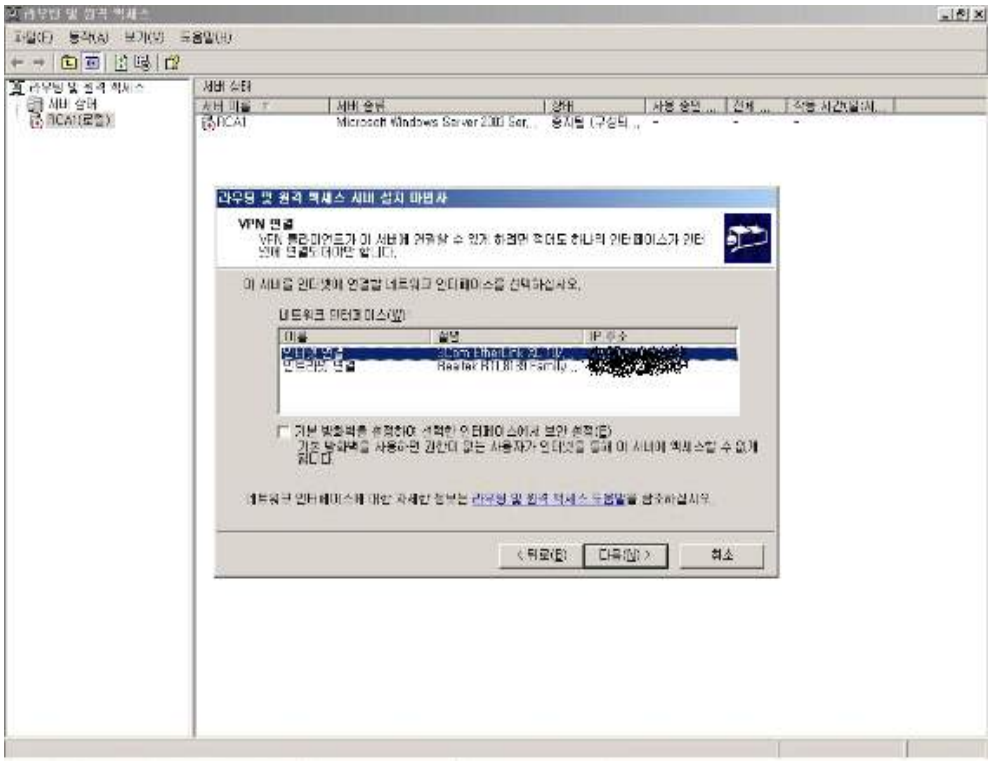
[그림 3-2-5-1-다]

㉱ 구성 페이지에서 가상 사설망(VPN) 액세스 및 NAT을 선택한다.



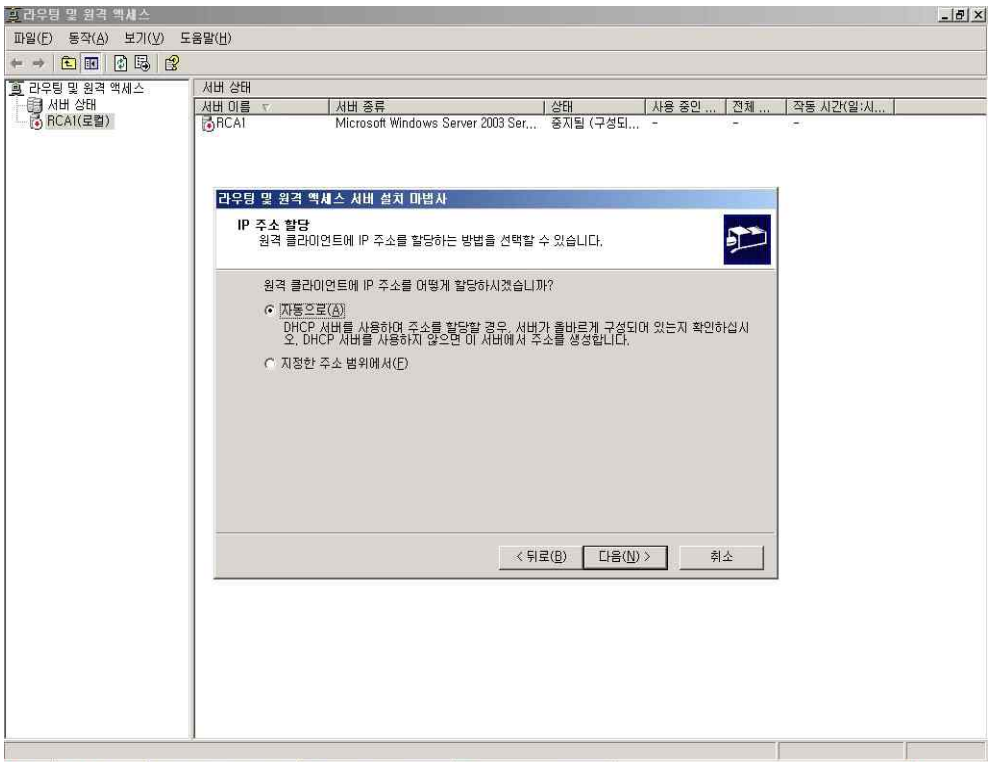
[그림 3-2-5-1-라]

㉮ VPN 연결 페이지의 네트워크 인터페이스 목록에서 Internet 연결을 선택하고 기본 방화벽을 설정하여 선택한 인터페이스에서 보안 설정의 선택을 해제하고 다음을 누른다.



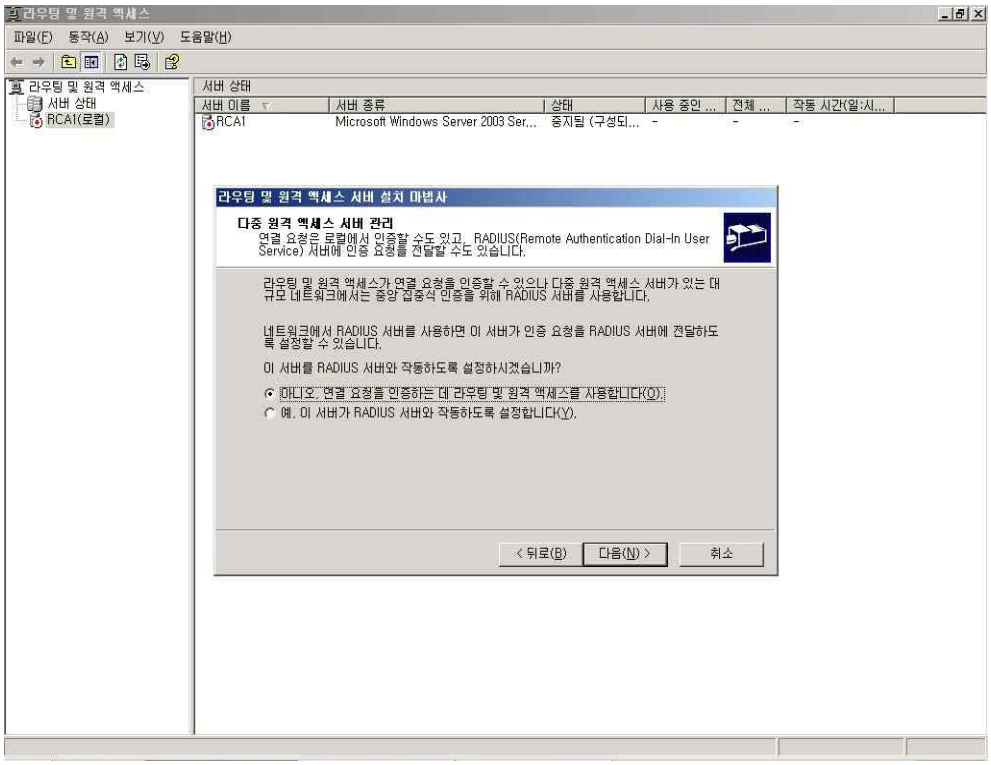
[그림 3-2-5-1-마]

㉯ IP 주소 할당 페이지에서 자동으로를 선택하고 다음을 누른다.



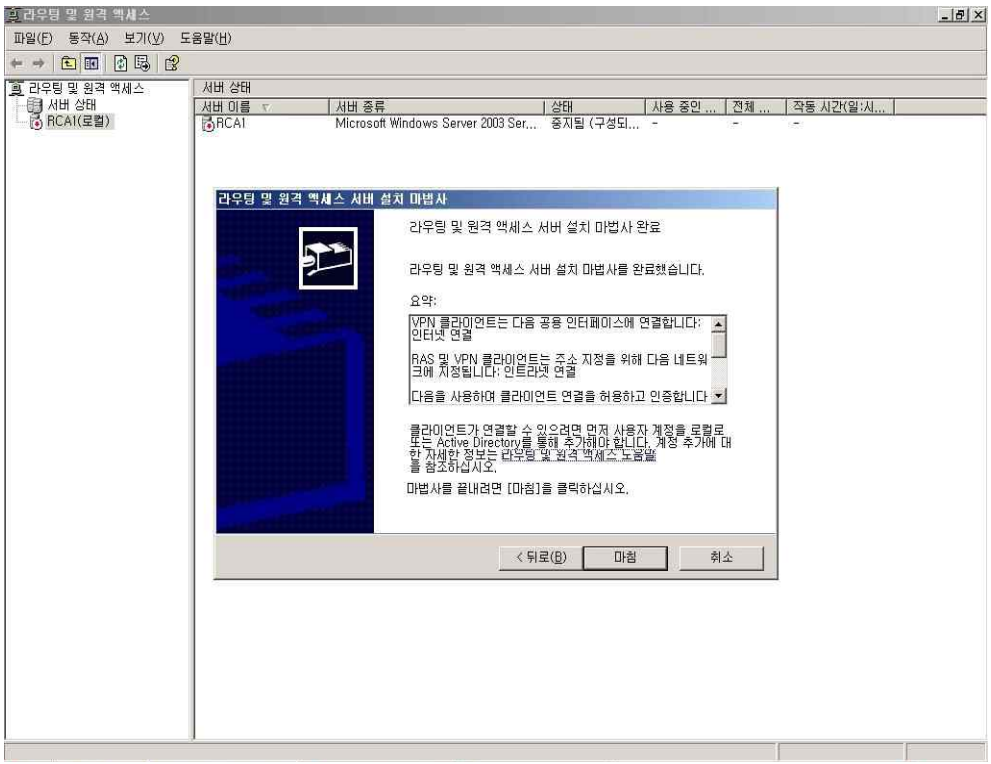
[그림 3-2-5-1-바]

㉮ 이름 및 주소 변환 서비스 페이지에서 나중에 이름 및 주소 서비스 설치를 선택하고 다음을 누른다.
㉯ 다중 원격 액세스 서버 관리 페이지에서 아니오를 선택하고 다음을 누른다.



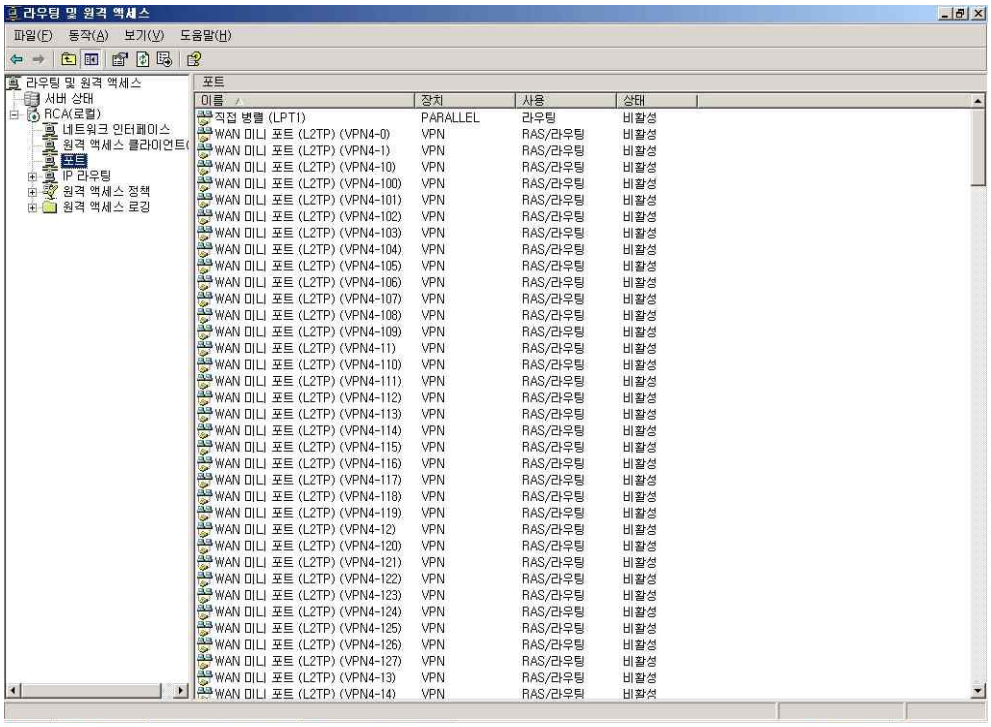
[그림 3-2-5-1-아]

㉰ 라우팅 및 원격 액세스 서버 설치 마법사 완료 페이지에서 마침을 누른다.



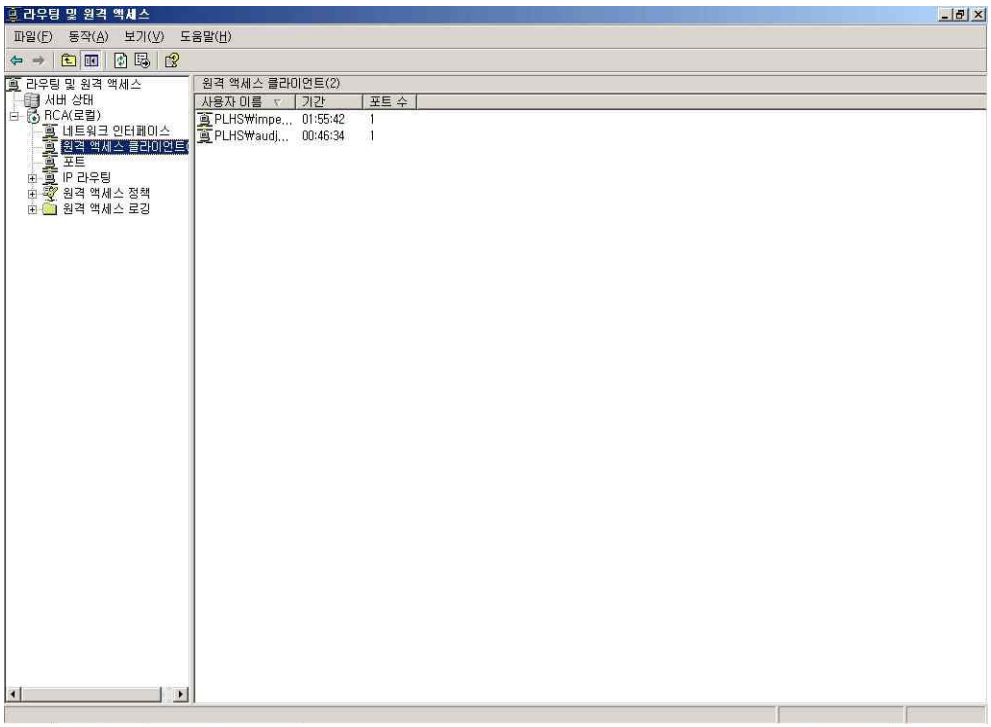
[그림 3-2-5-1-자]

㉦ 라우팅 및 원격 액세스 창에서 RCA를 확장하고 포트를 선택한후 WAN미니 포트(PPTP)와 WAN 미니 포트 (L2TP)가 각각 128개씩 만들어져 있는 것을 확인할 수 있다.



[그림 3-2-5-1-차]

㉧ 라우팅 및 원격 액세스 창에서 RCA를 확장하고 인터페이스 클라이언트를 선택하면 현재 접속중인 사용자와 사용시간을 알 수 있다.



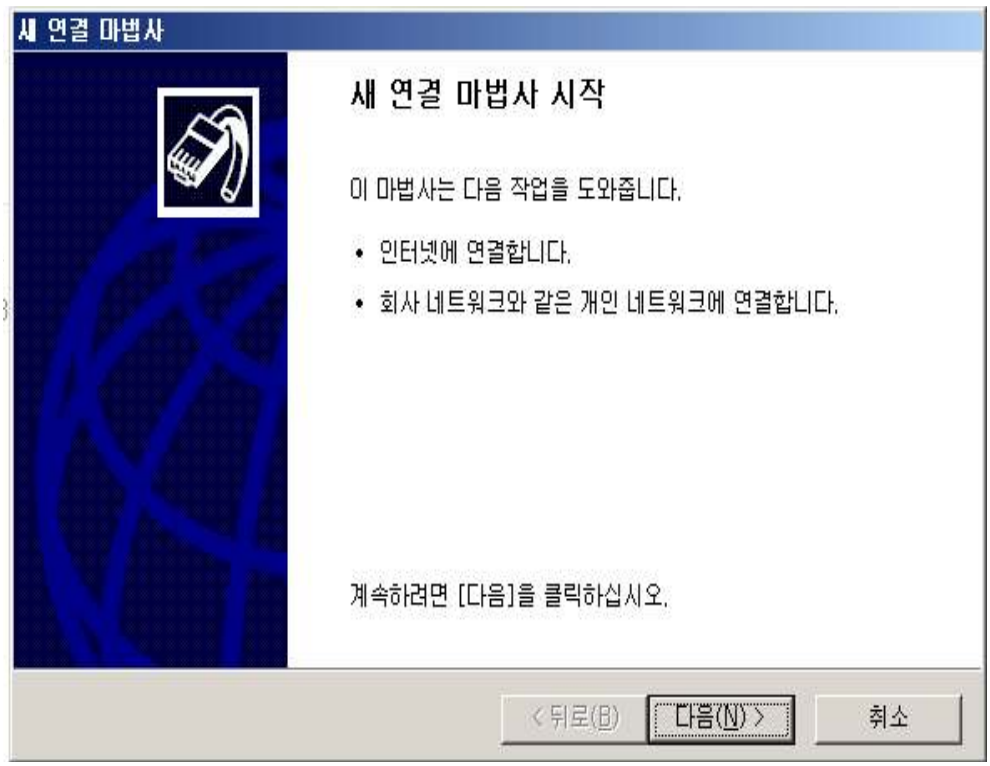
[그림 3-2-5-1-카]

② 클라이언트 컴퓨터에서 VPN서버 연결 설정하기

㉮ 시작 > 제어판 > 네트워크 및 Internet 연결 > 네트워크 연결을 선택한다.

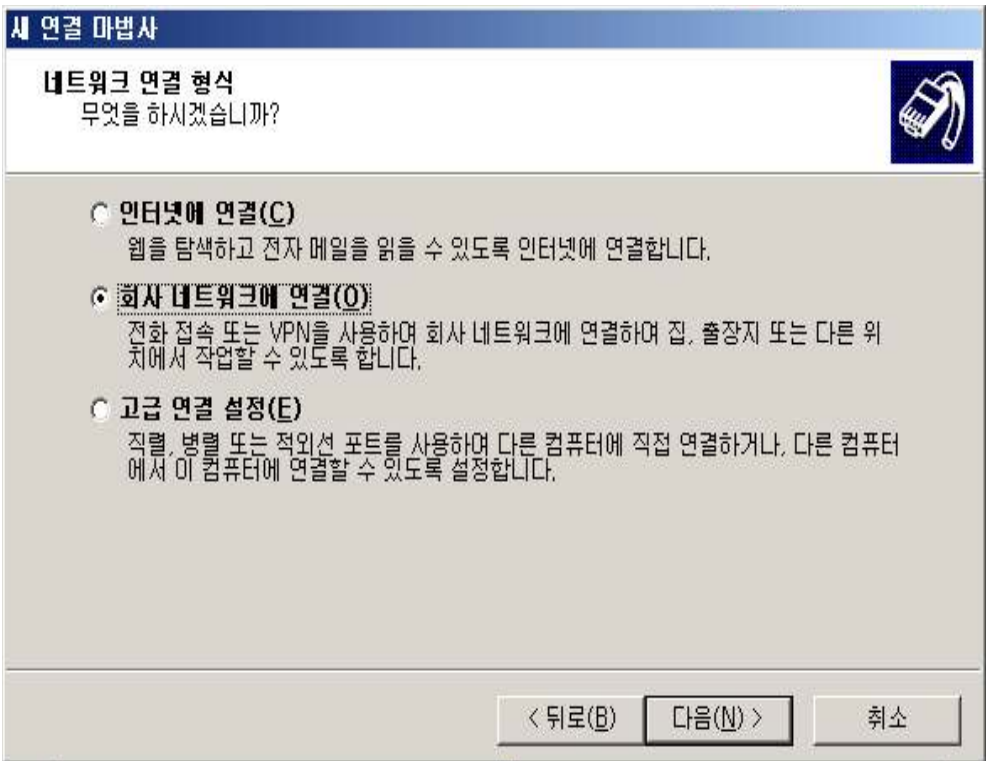
[그림 3-2-5-2-가]

㉯ 새 연결 마법사를 선택한 후 다음을 누른다.



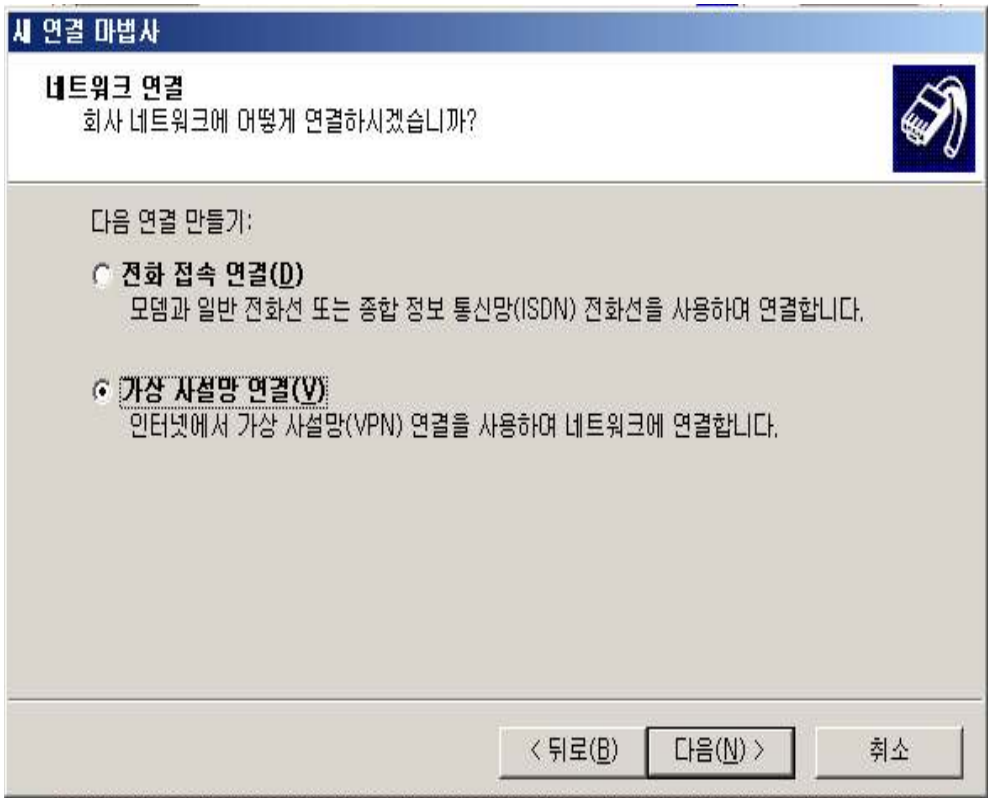
[그림 3-2-5-2-나]

㉰ 네트워크 연결 형식 페이지에서 회사 네트워크 연결을 선택하고 다음을 누른다.



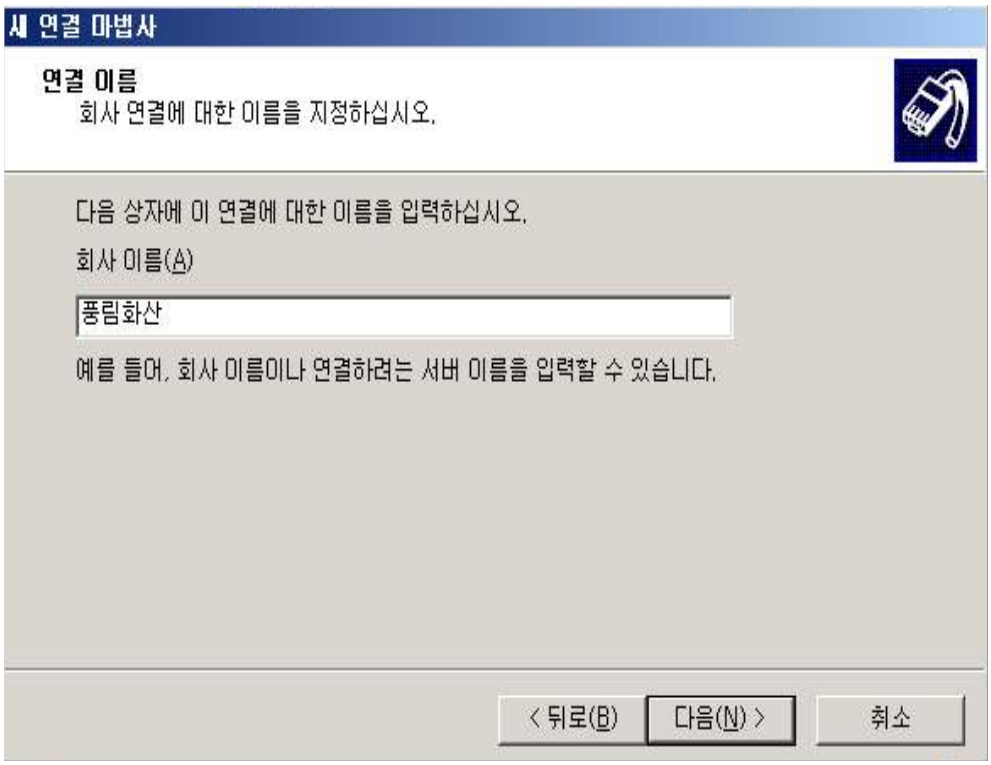
[그림 3-2-5-2-다]

㉱ 네트워크 연결 페이지에서 가상 사설망 연결을 선택하고 다음을 누른다.



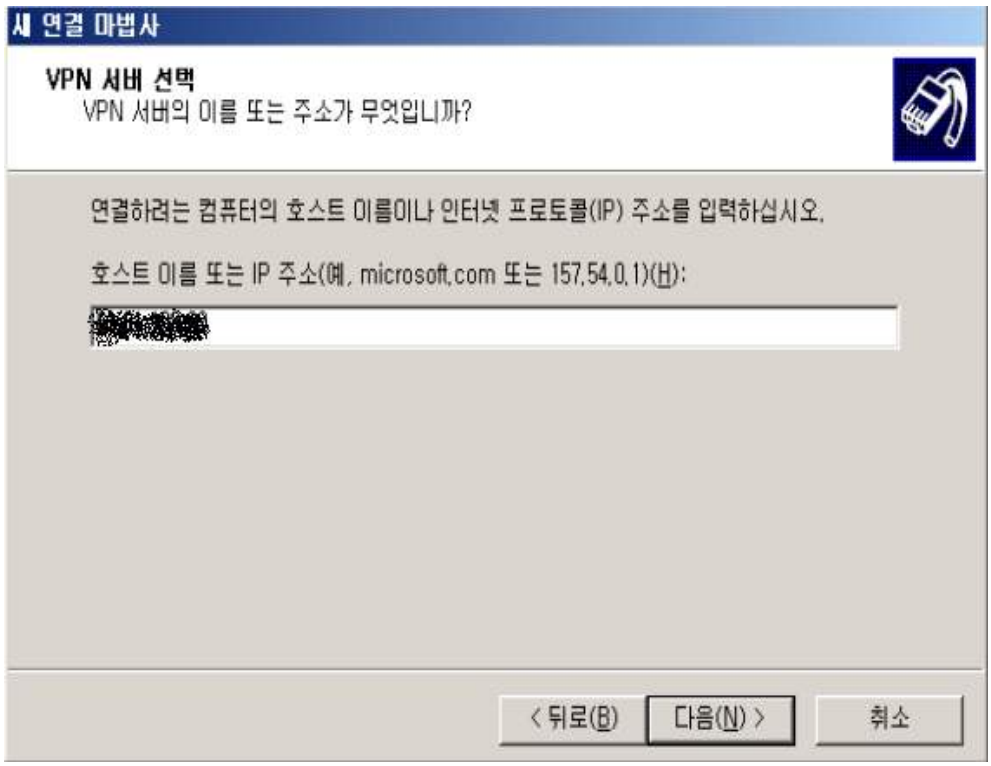
[그림 3-2-5-2-라]

㉮ 연결이름 페이지에서 회사 이름을 풍림화산이라고 입력한 후 다음을 누른다.



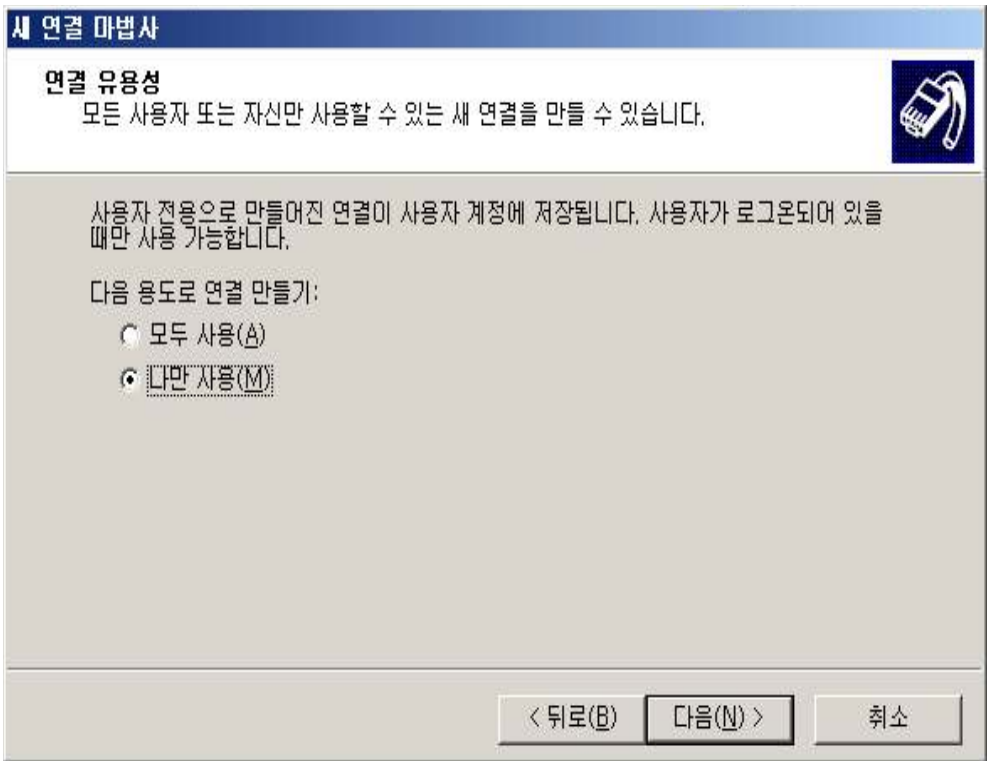
[그림 3-2-5-2-마]

㉯ VPN 서버 선택 페이지에서 호스트 이름 또는 IP 주소에 해당 VPN서버 IP주소를 입력하고 다음을 누른다.



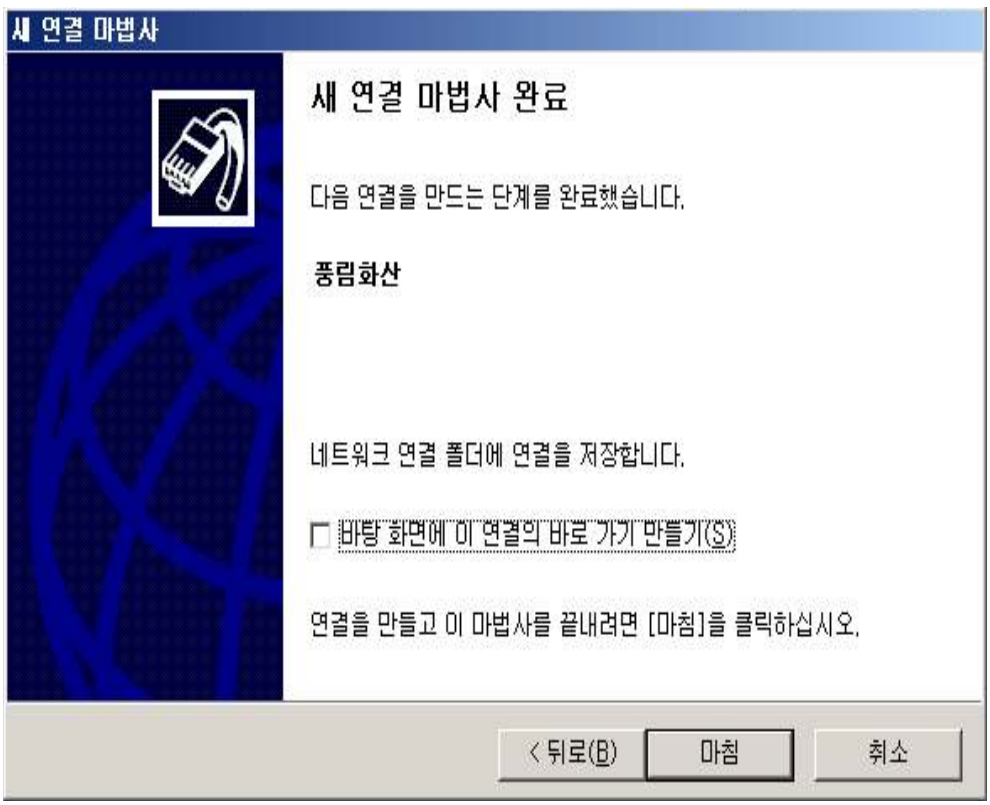
[그림 3-2-5-2-바]

㉮ 연결유용성 페이지에서 나만 사용을 선택하고 다음을 누른다.



[그림 3-2-5-2-사]

㉯ 새 연결 마법사 완료 페이지에서 마침을 누른다.



[그림 3-2-5-2-아]

③ VPN 서버에 연결하기

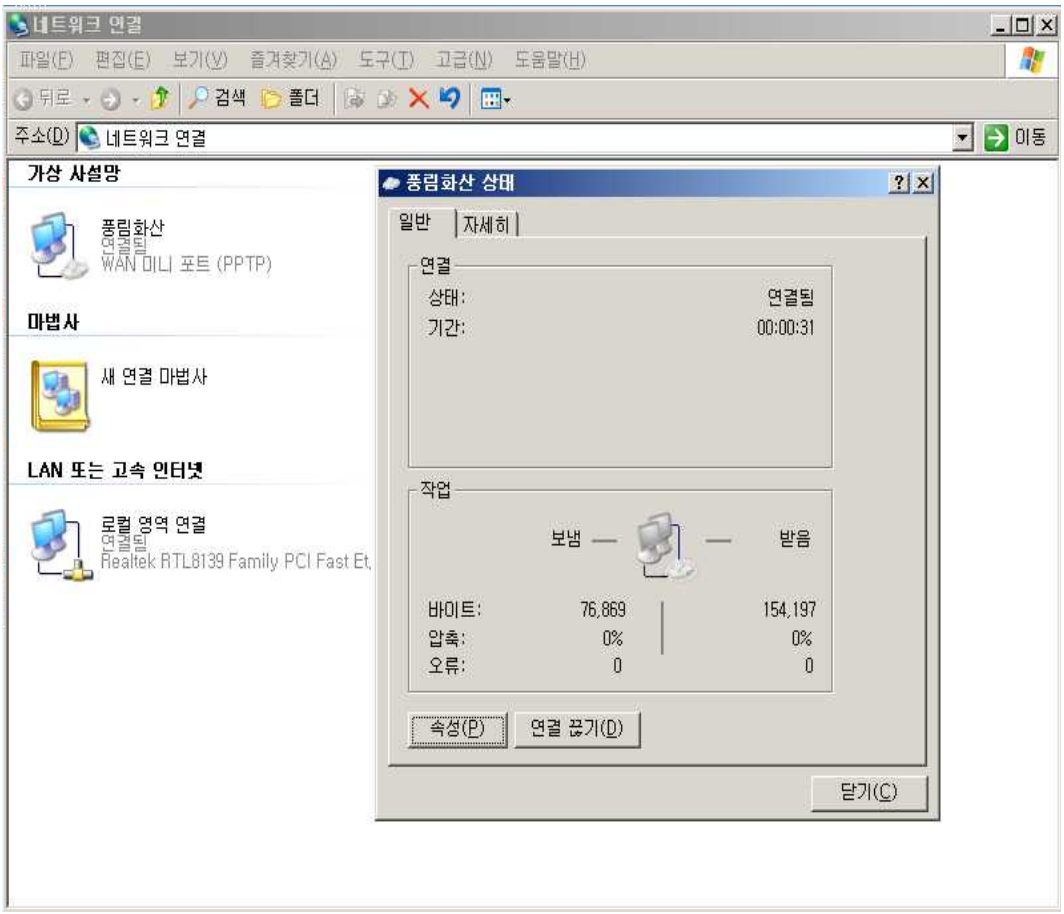
㉮ 네트워크 연결 창에서 가상사설망에 풍림화산을 누른다. 연결 창에서 사용자 이름에 사용자 ID@plhs.com을 입력하고 패스워드를 입력한 후 연결 버튼을 누른다.

[그림 3-2-5-3-가a]

[그림 3-2-5-3-가b]

[그림 3-2-5-3-가c]

㉰ 네트워크 연결 창에서 가상사설망에 풍림화산을 누르면 연결돼 있는 것을 확인할 수 있다.

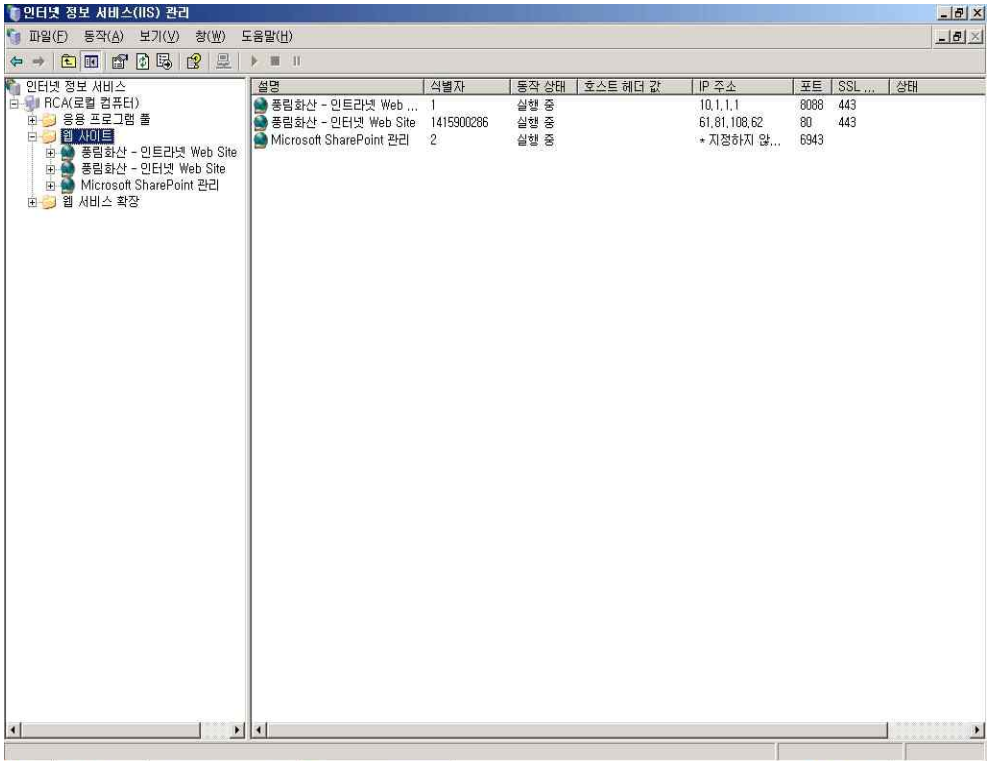


[그림 3-2-5-3-나]

3.2.6 IIS(Internet Information Service)

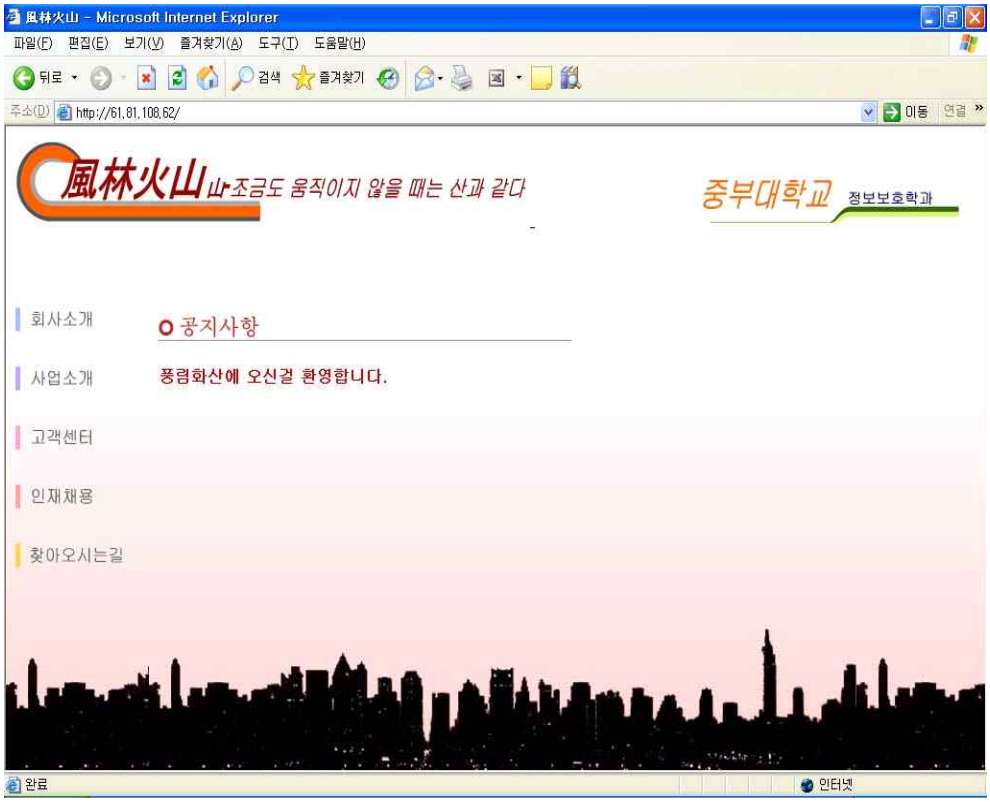
IIS 는 미국 마이크로소프트사가 개발한 Internet / 인트라넷용 서버 소프트웨어. 버전 2.0부터 윈도즈 NT 서버에 표준으로 첨부되어 있다. 운영 체계(OS)와 통합된 것으로 복잡한 절차 없이 월드 와이드 웹 서버를 관리할 수 있다. 본체와 기능 확장 모듈로 구성되는데 하이퍼텍스트 전송 규약(HTTP), 파일 전송 규약(FTP), 고퍼(Gopher)의 각 서비스 및 ASP(Active Server Pages)의 문서 검색 기능, 월드 와이드 웹(WWW) 페이지 작성 기능 등을 제공한다. 데이터베이스나 그룹웨어와 연계해서 SSL(Secure Sockets Layer) 보안성에도 대응한다.

Windows Server 2003의 Web Edition을 제외한 모든 버전에는 Internet 정보 서비스가 설치되어 있지 않다. Internet 정보 서비스를 설치하기 위해서는 Windows 구성 요소 마법사를 이용하거나, 서버 구성 마법사를 이용할 수 있다. [그림 3-2-6a]은 Server 구성마법사를 이용하여 Main Server에 Internet 정보 서비스의 WWW 서비스와 ASP.NET 서비스를 설치하여 Internet 웹 사이트(61.81.108.62)와 인트라넷 웹사이트(Web.plhs.com{10.1.1.1})를 구성했다.



[그림 3-2-6a]

아래 [그림 3-2-6b]은 Internet 웹사이트 (61.81.108.62)의 메인 페이지이다.



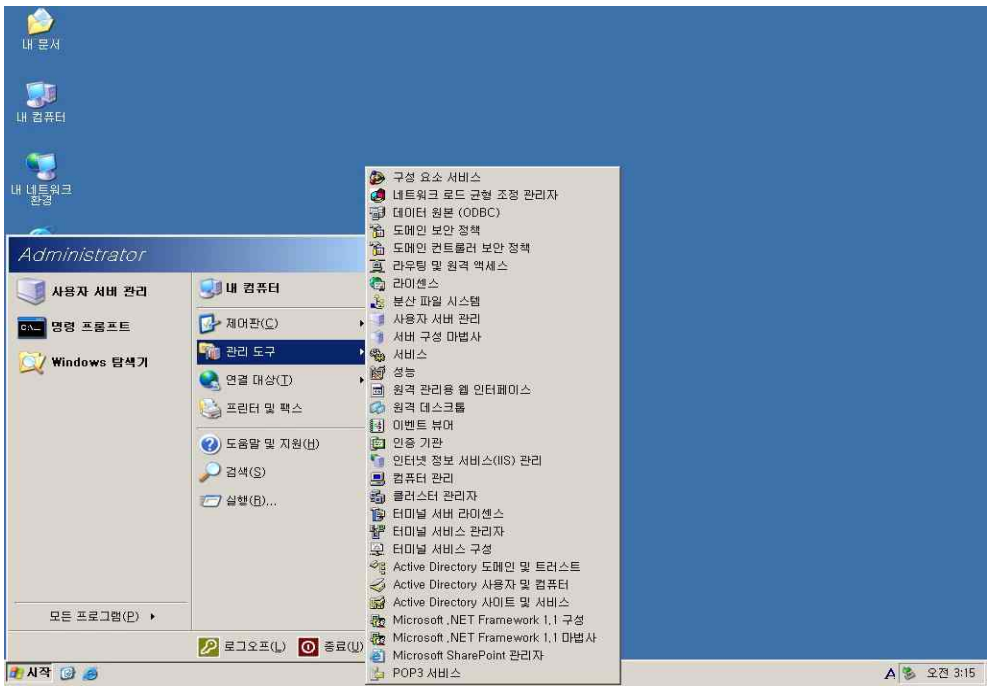
[그림 3-2-6b]

아래 [그림 3-2-6c]은 인트라넷(사내망) 웹사이트 (www.plhs.com = 10.1.1.2)의 메인 페이지이다.

[그림 3-2-6c]

3.3 Sub Server (rweb)

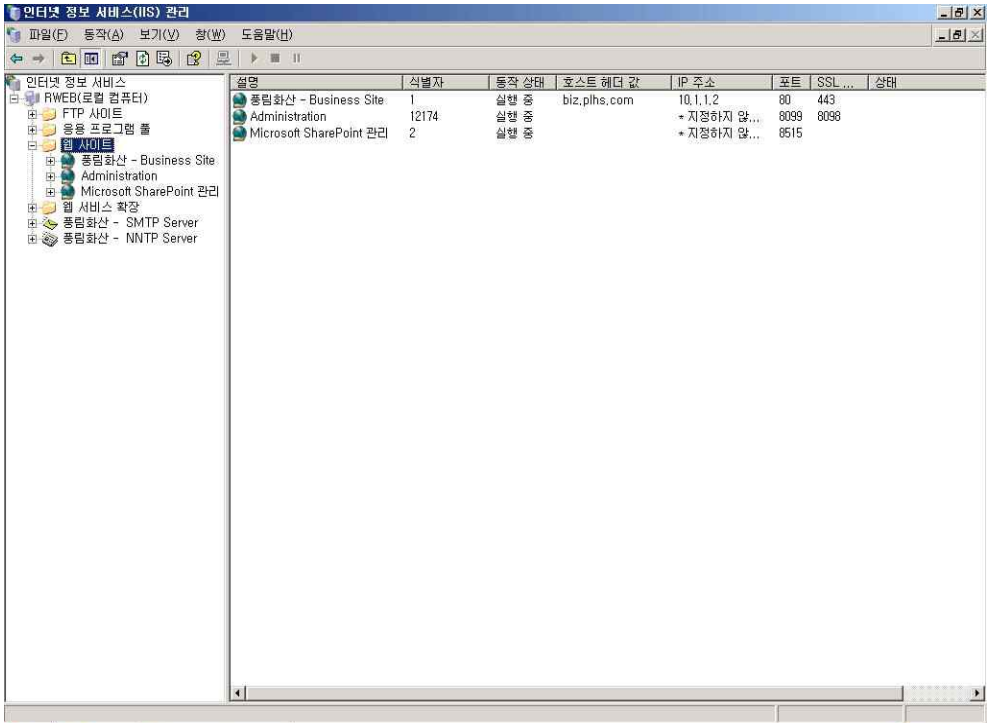
Sub Server 는 IIS(Web Site, SMTP Service, NNTP Service) 자식 Active Drectoy, POP3 Service 로 구성되었다.



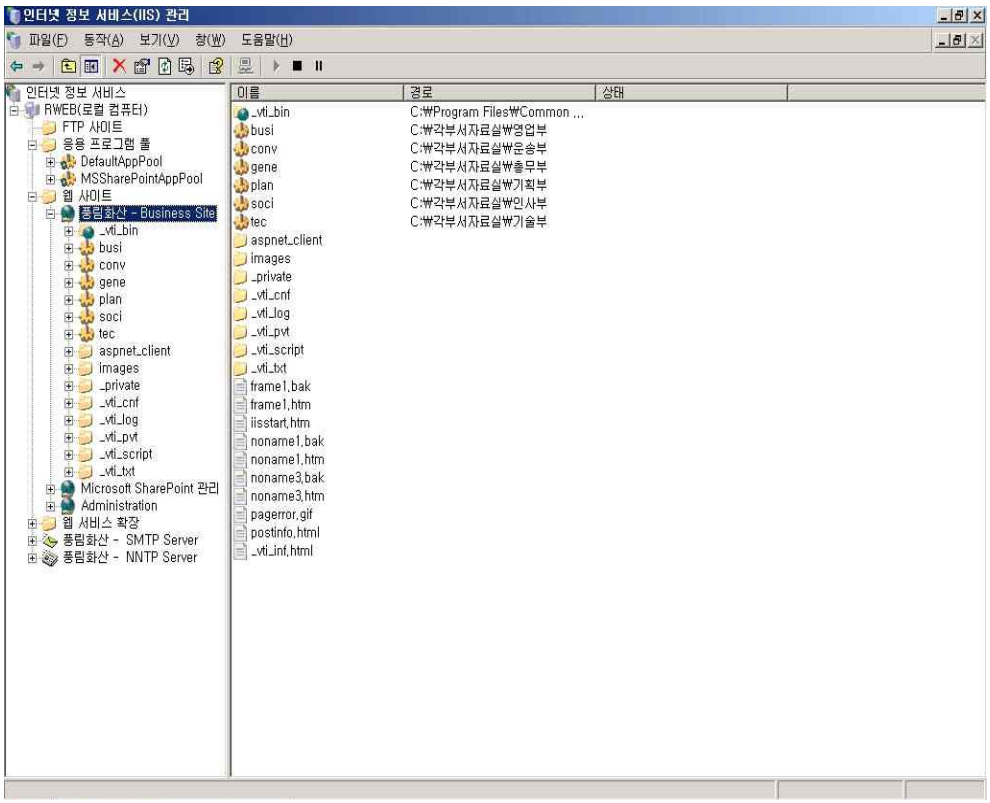
[그림 3-3]

3.3.1 Web Site (biz.plhs.com)

사내망용 업무 웹 사이트인 풍림화산 - Business Site (biz.plhs.com = 10.1.1.2)를 구축한 것을 아래 [그림 3-3-1a]에서 확인할 수 있다.

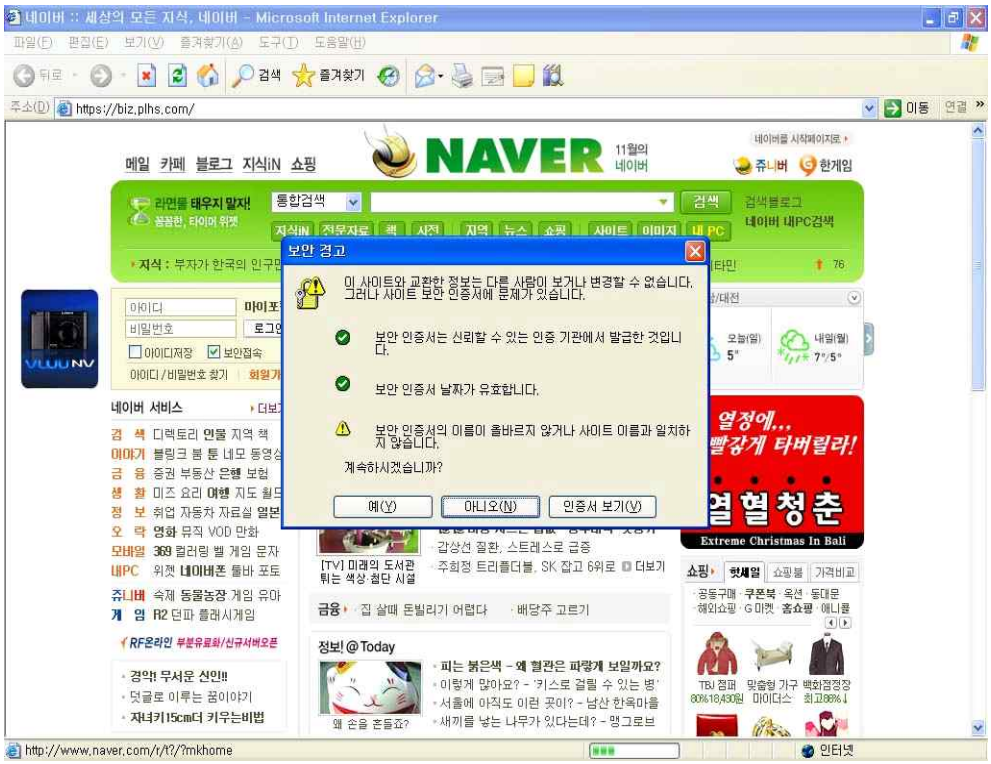


[그림 3-3-1a]



[그림 3-3-1b]

① 주소창에 https://biz.plhs.com를 입력 후 연결 하면 보안 경고창이 출력된다.



[그림 3-3-1-1]

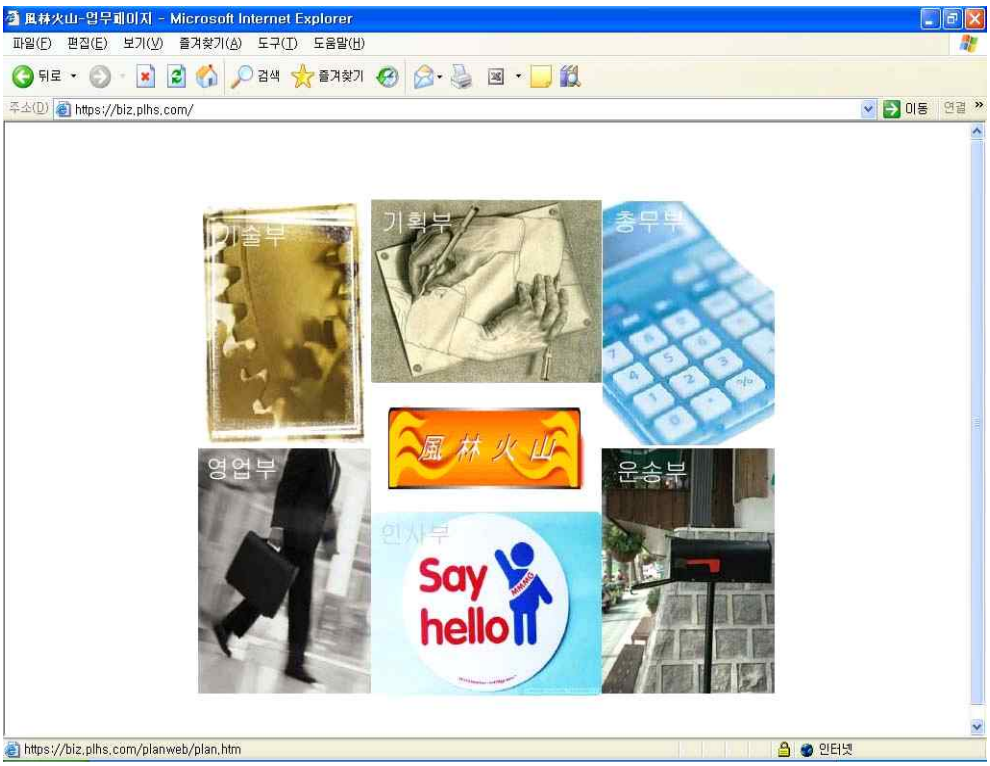
② 디지털 인증서 선택에서 해당 인증서를 선택 후 확인을 누른다.

[그림 3-3-1-2]

③ rweb.plhs.com에 연결에서 사용자이름에 사용자 ID@plhs.com을 입력하고 패스워드를 입력한 후 확인을 누른다.

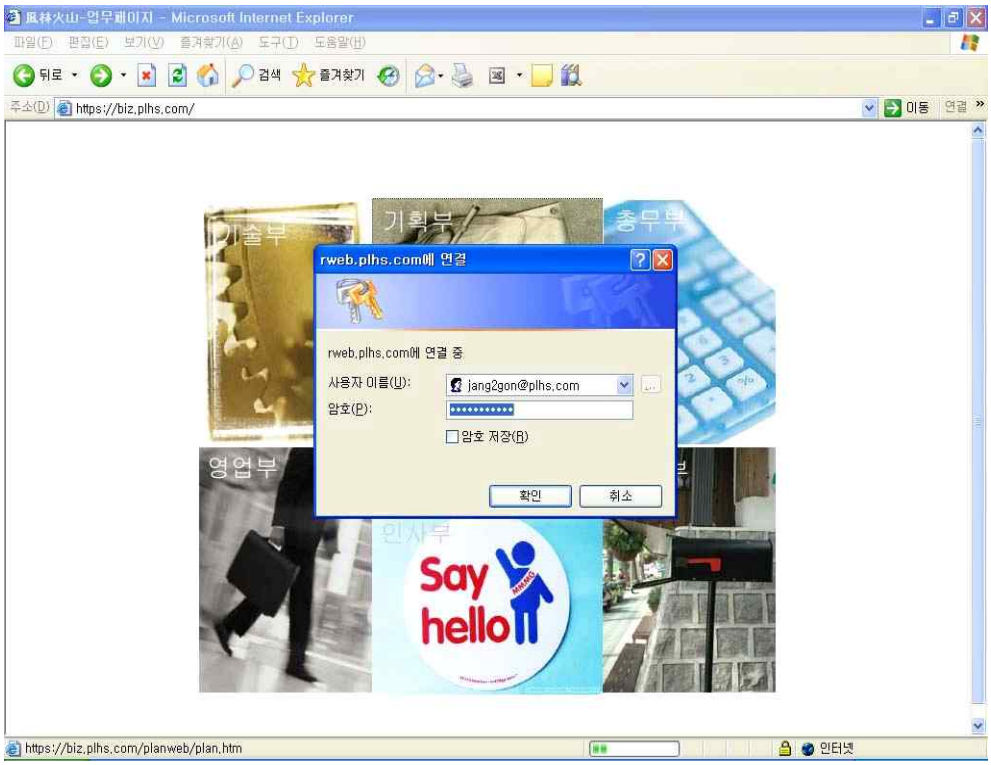
[그림 3-3-1-3]

④ http://biz.plhs.com에 접속한 것을 확인할 수 있다.



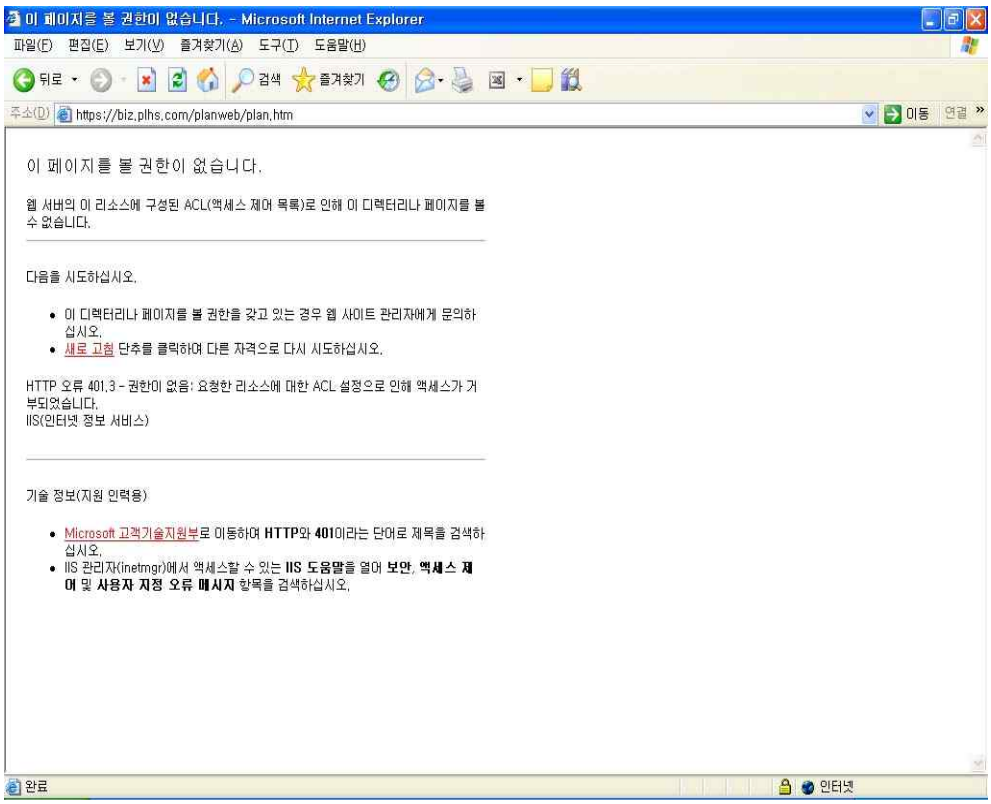
[그림 3-3-1-4]

⑤ 다른 부서를 선택할 시 에는 아래와 같이 재차 로그인을 하는 창이 출력된다.



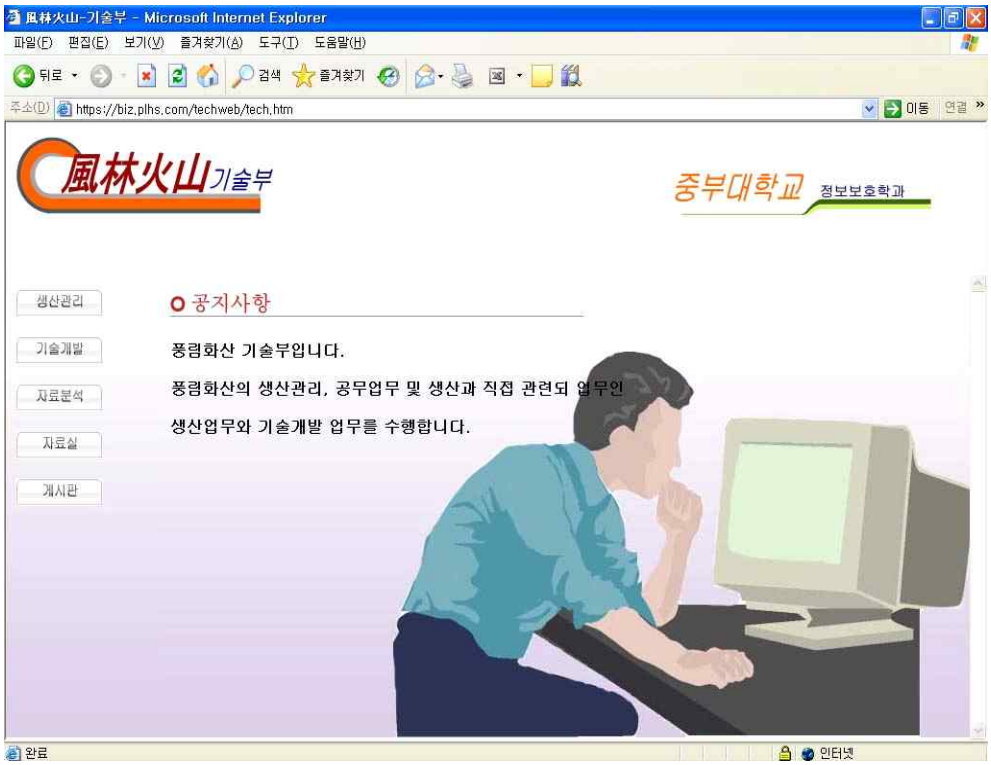
[그림 3-3-1-5]

⑥ 로그인을 실패하였을 경우 이 페이지를 볼 권한이 없습니다. 라고 오류 화면이 출력된다.



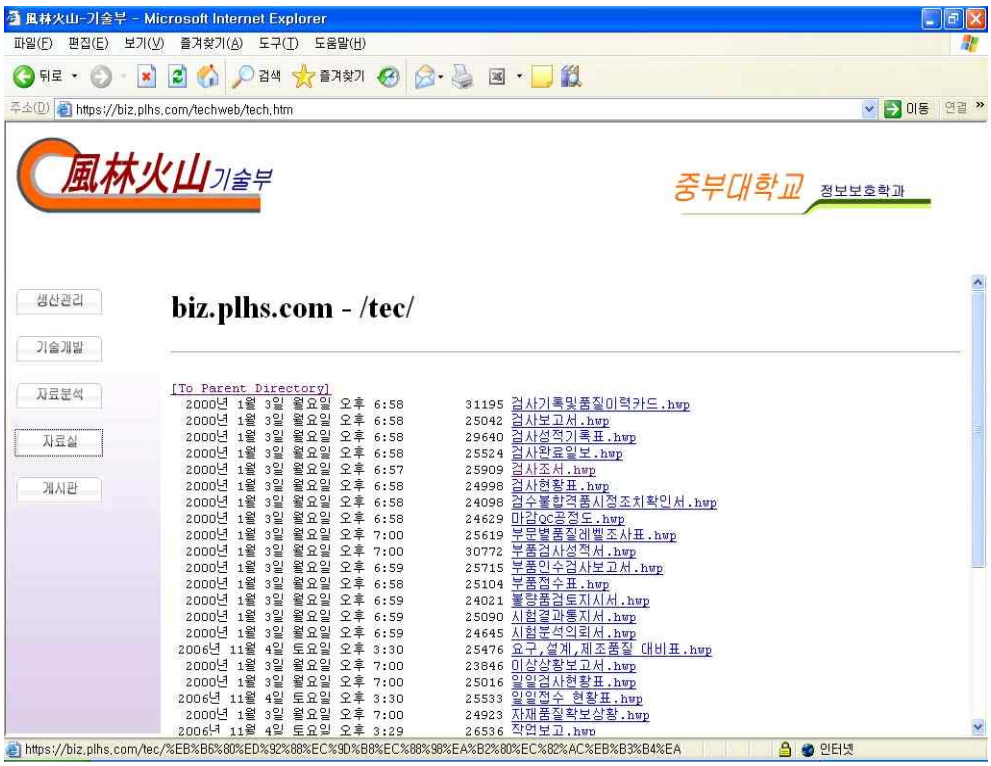
[그림 3-3-1-6]

⑦ 메인페이지에 연결 후 접속 시에 로그인한 사용자의 부서를 누른다.
(지금은 기술부 사원아이디로 로그인 했으므로 기술부를 누른다.)



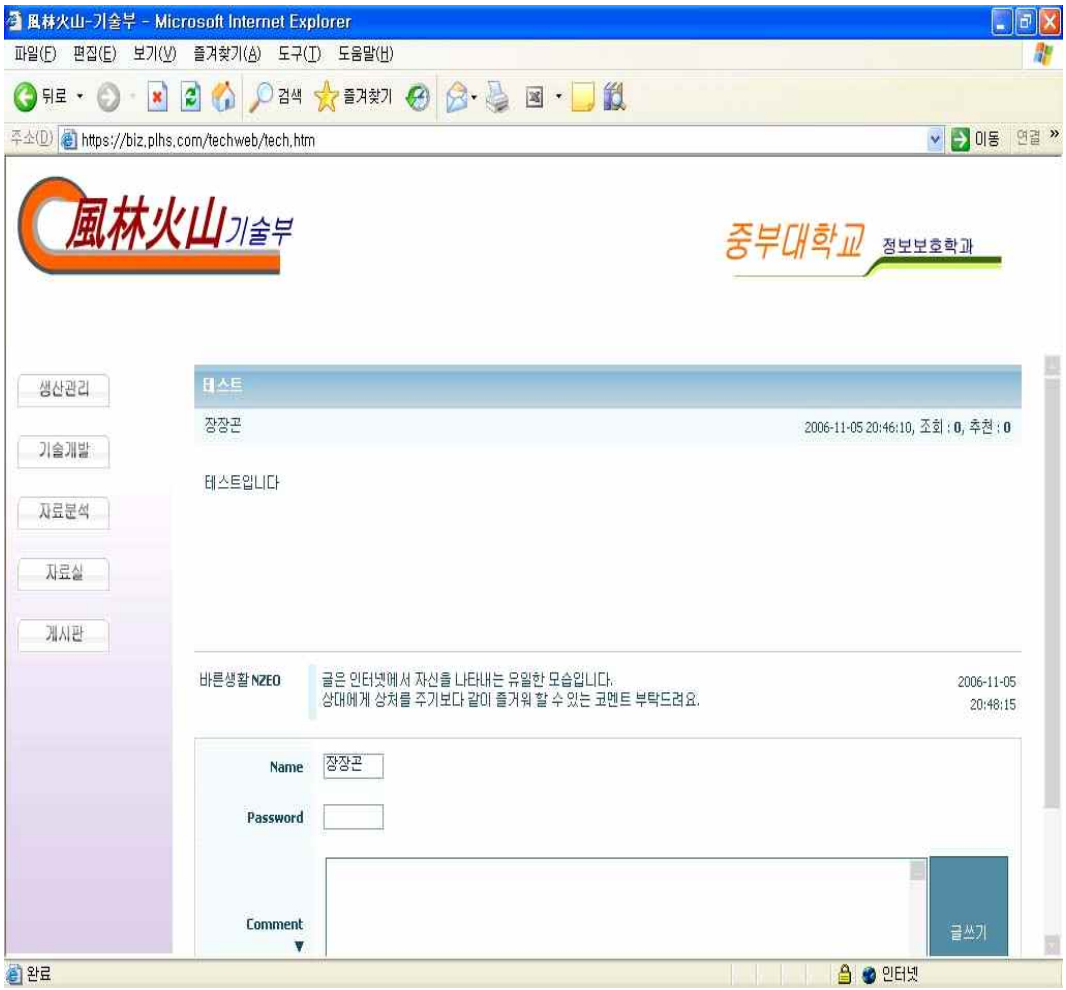
[그림 3-3-1-7]

⑧ 자료실 버튼을 누르면 여러 자료가 있는 것을 확인할 수 있다.



[그림 3-3-1-8]

⑨ 게시판 버튼을 누르면 게시물을 확인하고 글을 올릴 수 있다.
(게시판은 제로보드를 이용하여 만들었다.)



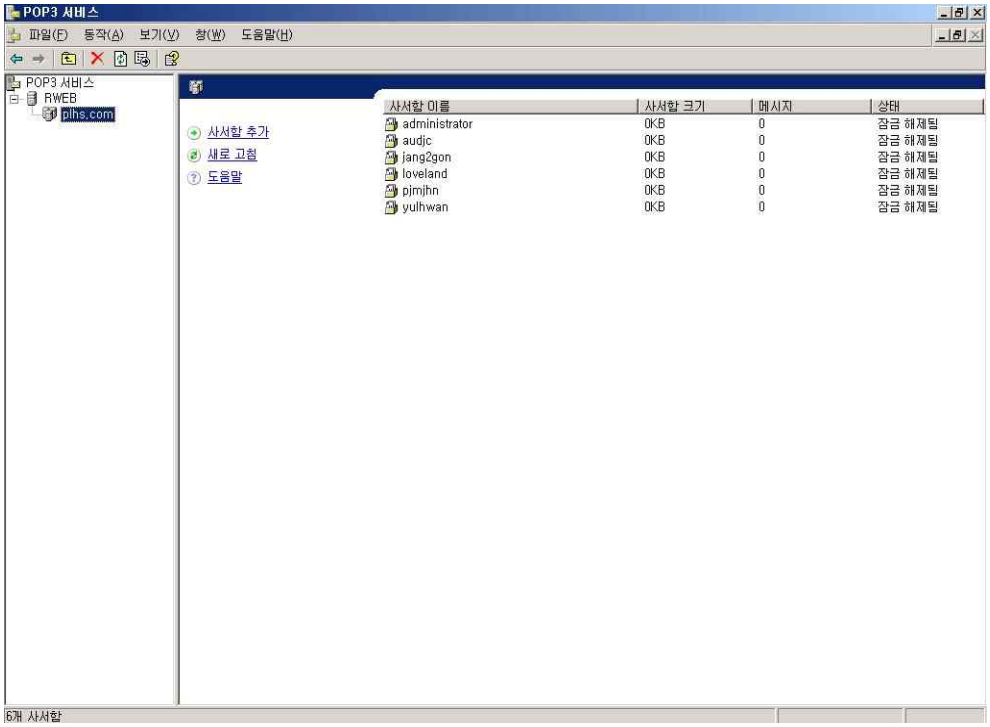
[그림 3-3-1-9]

3.3.2 E-mail Server (mail.plhs.com)

① POP3 Service

POP3 프로토콜은 메일 서버의 사서함에 도착된 메일을 클라이언트 컴퓨터로 다운로드 받아서 볼 수 있도록 하여 주는 기능을 제공한다. POP3 서비스는 로컬 Windows 계정 인증, Active Directory 통합 인증, 부호화된 암호 파일 인증의 세 가지 인증 방법을 제공한다. 로컬 Windows 계정 인증은 로컬 사용자 계정을 사서함과 통합하여 사용할 수 있다. Active Directory 통합 인증을 사용하면 Active Directory 의 계정을 사서함에 대한 계정으로 사용할 수 있다. 부호화된 암호 인증은 Active Directory가 없거나 로컬 계정을 사용하지 않고 인증할 수 있다.

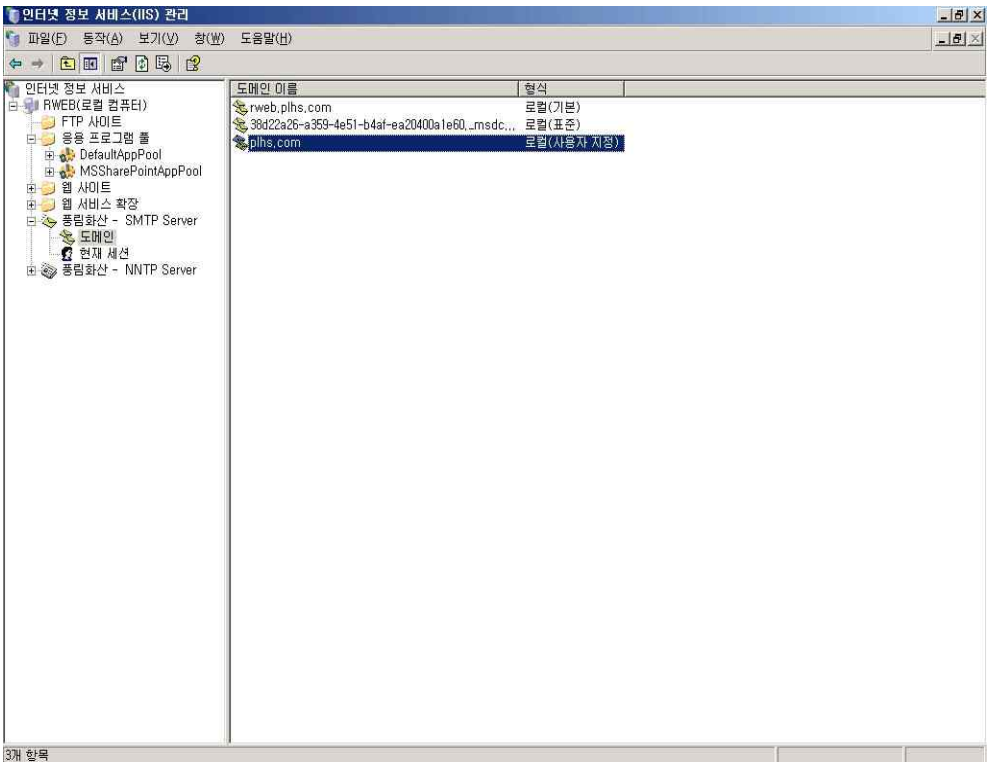
멤버 컴퓨터에 설치된 POP3 서비스는 세 가지 인증 방법을 모두 사용할 수 있고, 도메인 컨트롤러에 설치된 POP3 서비스는 Active Directory 통합 인증과 부호화된 암호 파일 인증을 사용할 수 있고, 독립 실행 형 서버에 설치된 POP3 서비스는 로컬 Windows 계정 인증과 부호화된 암호 파일 인증을 사용할 수 있다. [그림 3-3-2-1]은 사용자의 사서함 추가가 되어 있는 것 을 보여준다.



[그림 3-3-2-1]

② SMTP (Simple Mail Transfer Protocol)

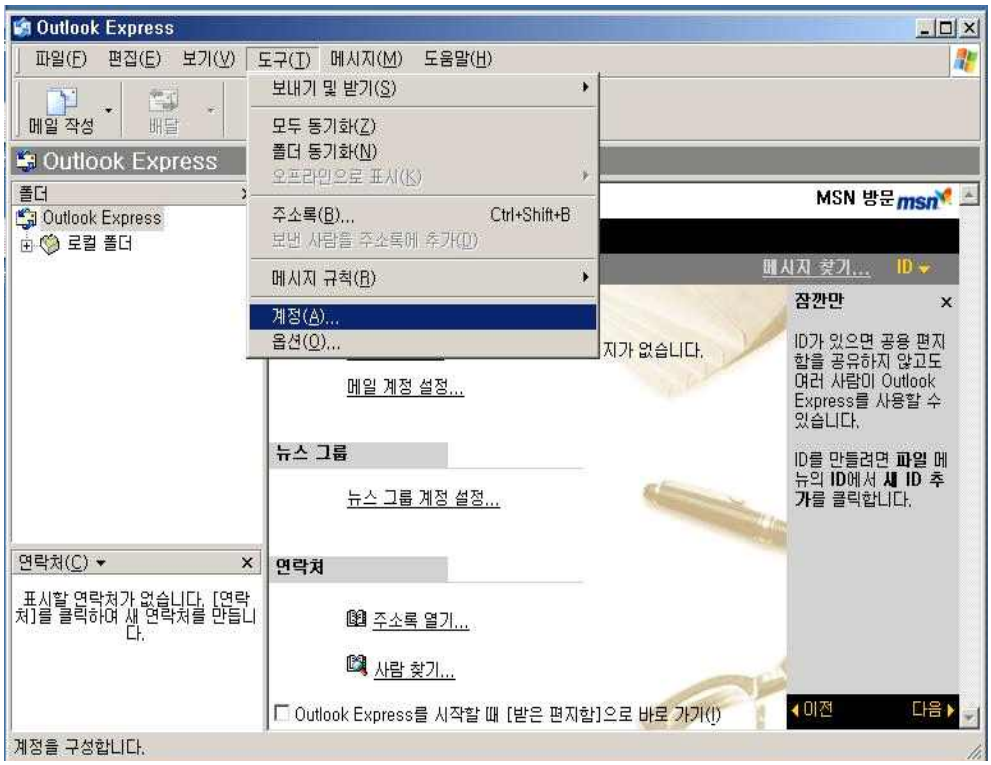
SMTP 프로토콜은 Internet 상 에서 메일을 주고받을 수 있는 기능을 제공한다. rweb를 이용하여 메일을 주고받을 수 있도록 rweb 에 SMTP 가상 서버를 구성한다. 또한, 클라이언트들이 보내는 서버의 이름을 쉽게 기억할 수 있도록 DNS 서버에 rweb의 별칭을 mail로 생성 하였다.



[그림 3-3-2-2]

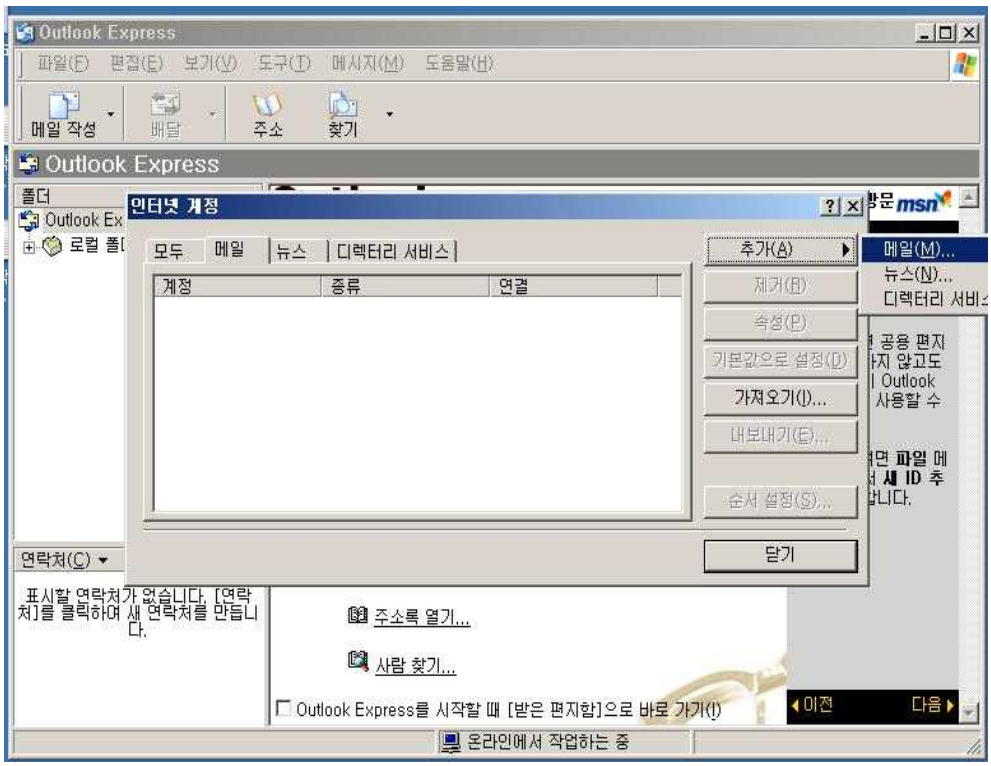
㉮ 클라이언트의 Outlook Express의 E-mail 계정 설정하기

㉠ Outlook Express창에서 도구 > 계정을 선택한다.



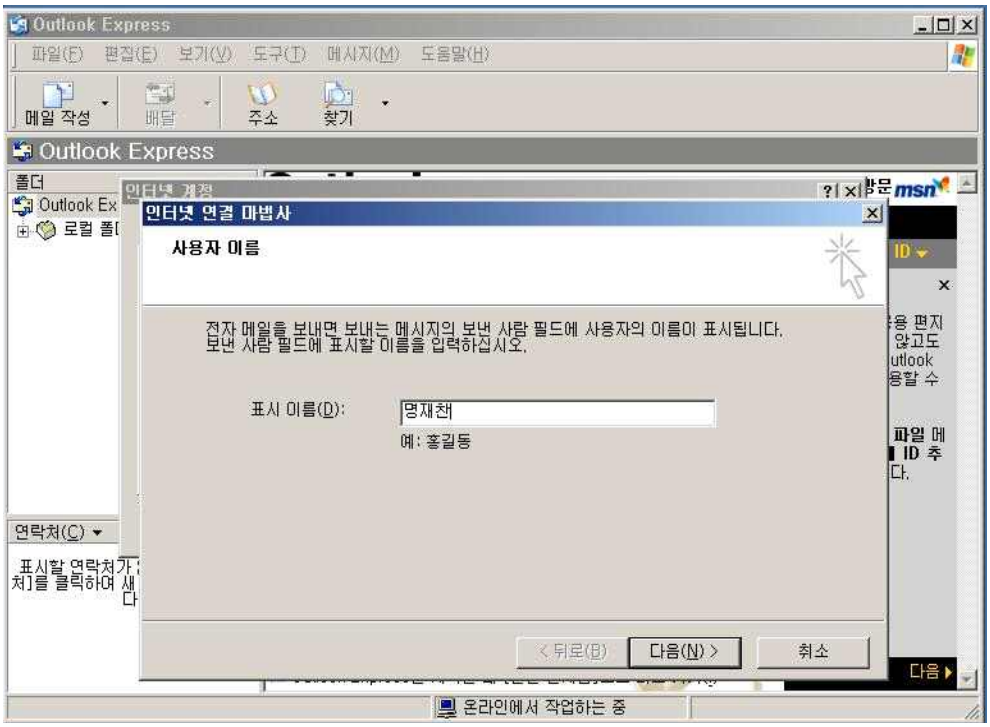
[그림 3-3-2-2-가-ㄱ]

㉡ Internet 계정 창에서 추가> 메일을 선택한다.



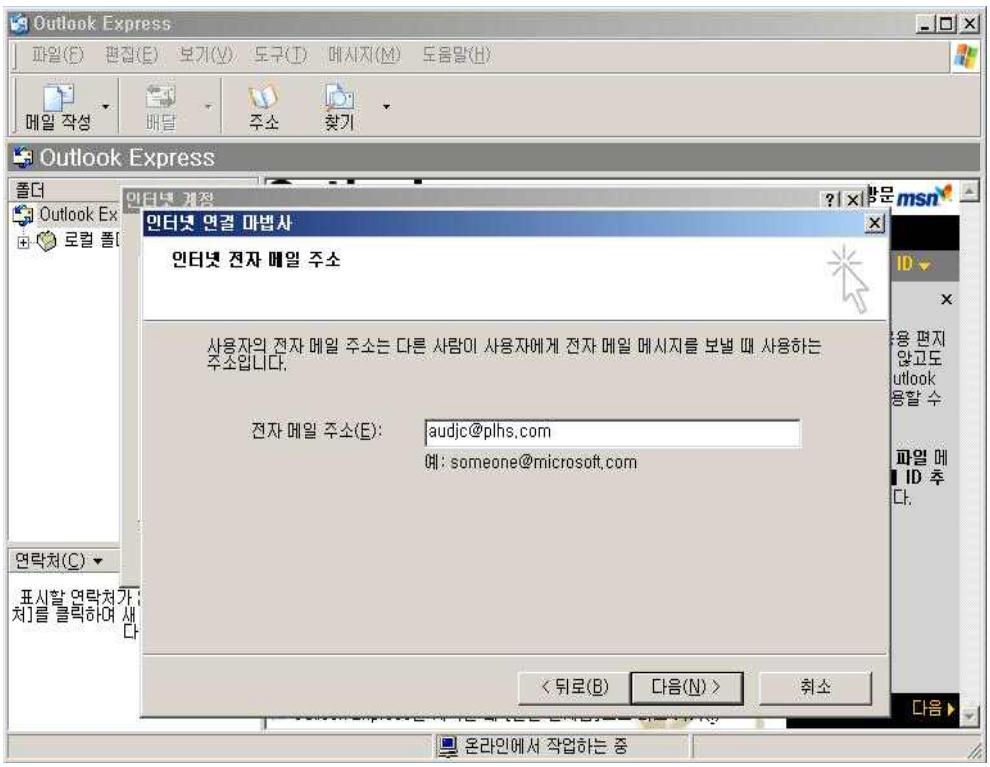
[그림 3-3-2-2-가-ㄴ]

㉢ Internet 연결 마법사의 사용자 이름 페이지에서 표시 이름에 사용자 이름을 입력하고 다음을 누른다.



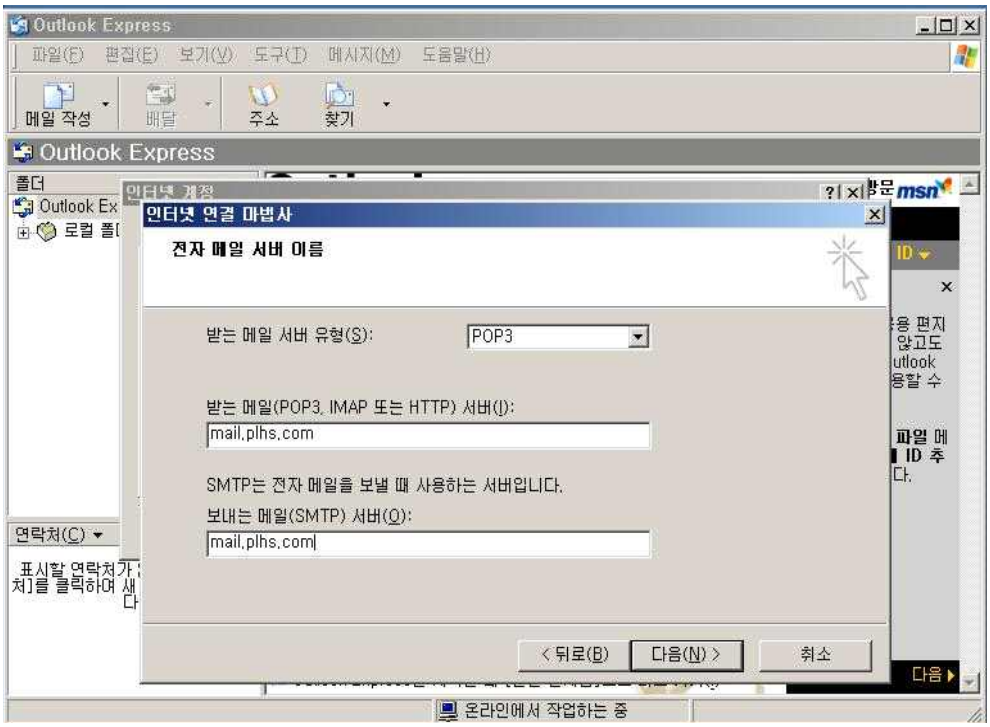
[그림 3-3-2-2-가-ㄷ]

㉣ Internet 전자 메일 주소 페이지에 전자 메일 주소에 사용자 ID@plhs.com 이라고 입력하고 다음을 누른다.



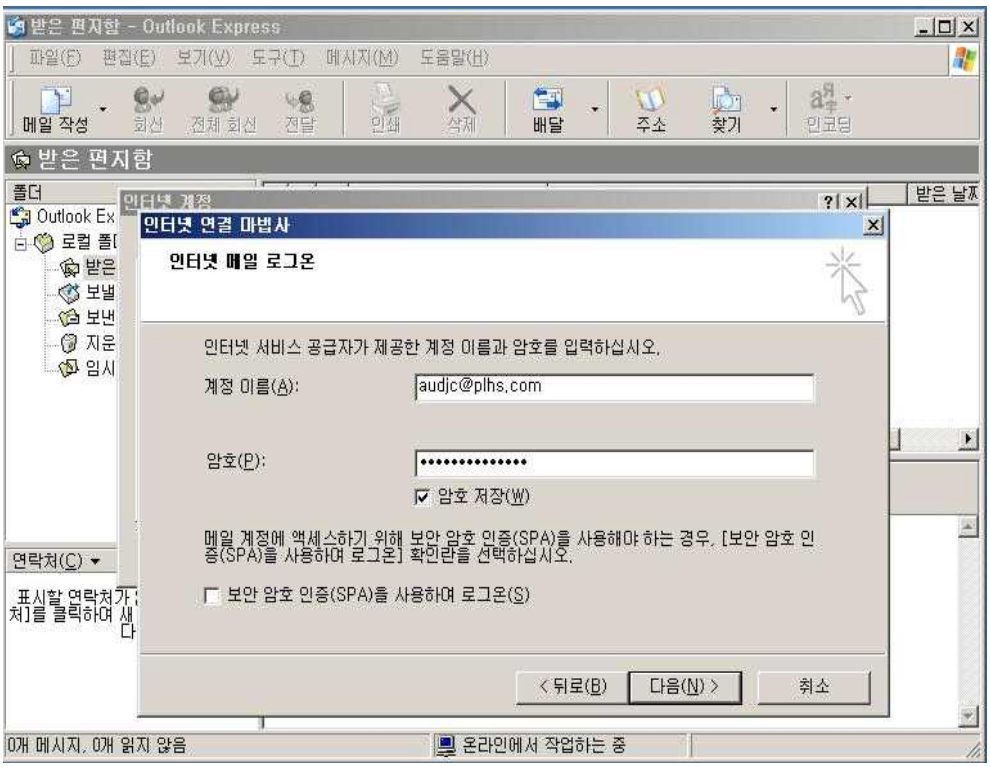
[그림 3-3-2-2-가-ㄹ]

ⓜ 전자 메일 서버 이름 페이지에서 받은 메일 서버 유형에 POP3를 선택하고 받는 메일 서버와 보내는 메일 서버에 mail.plhs.com 이라고 입력하고 다음을 누른다.



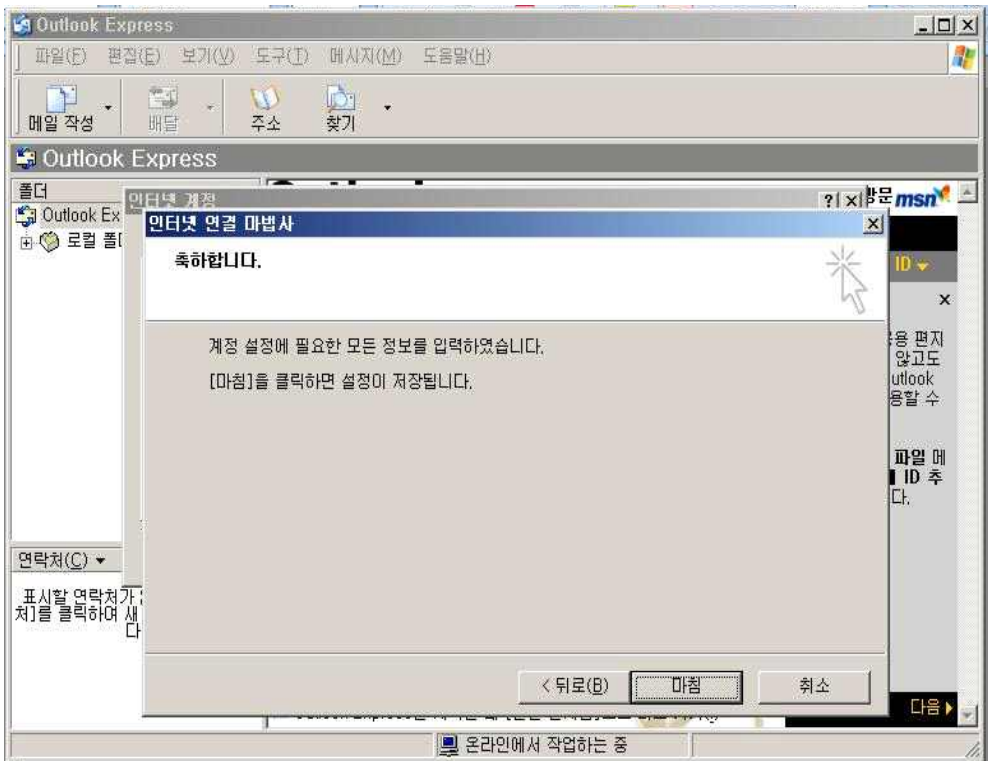
[그림 3-3-2-2-가-ㅁ]

ⓗ Internet 메일 로그온 페이지에서 계정 이름에 사용자 ID@plhs.com 암호에 패스워드를 입력 하고 암호 확인이 선택되어 있는 것을 확인하고 확인을 누른다.



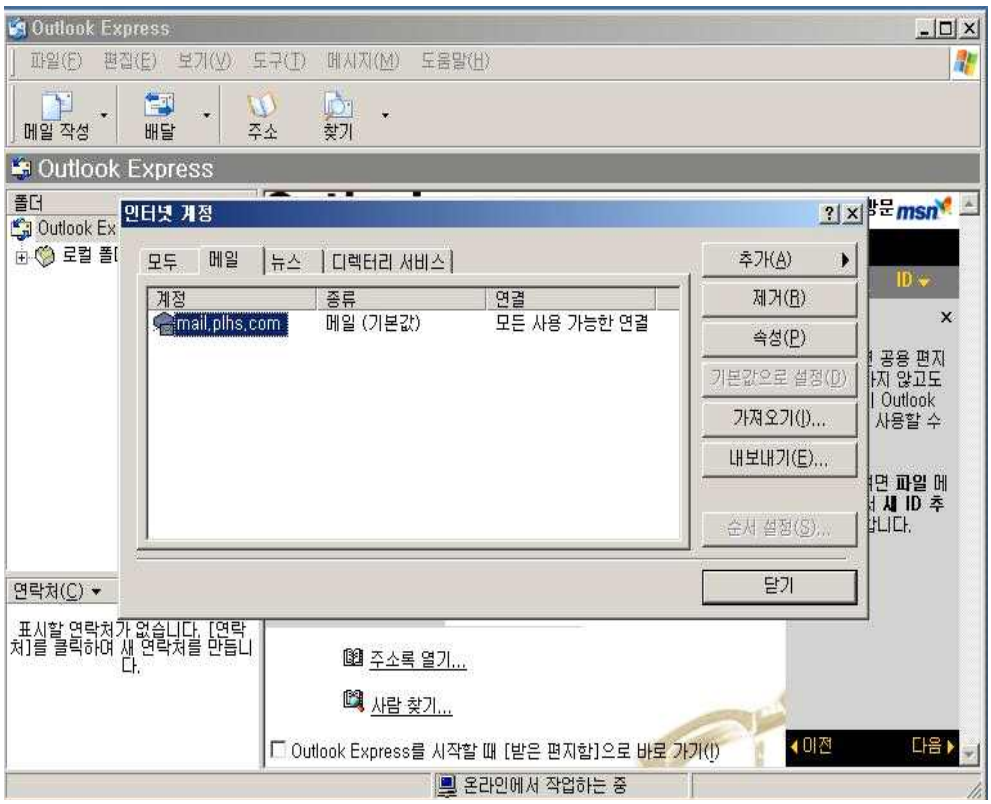
[그림 3-3-2-2-가-ㅂ]

ㅅ) 축하합니다. 페이지에서 마침을 누른다.



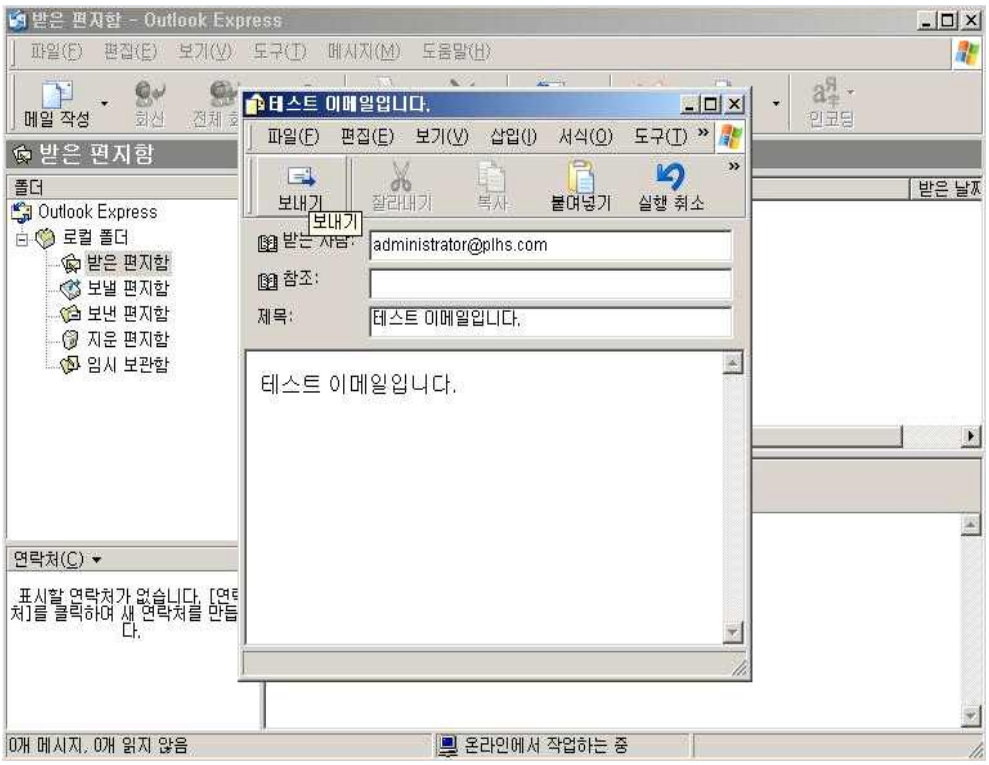
[그림 3-3-2-2-가-ㅅ]

ㅇ) mail.plhs.com 계정이 추가된 것을 확인할 수 있다.



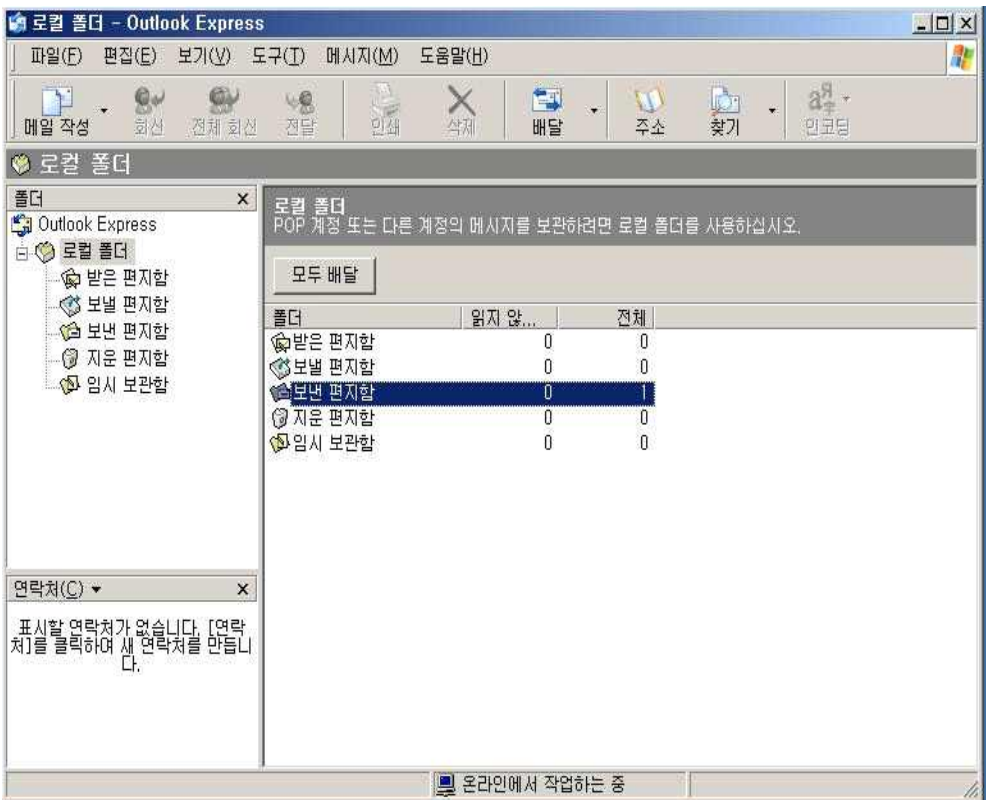
[그림 3-3-2-2-가-ㅇ]

ㅈ Administrator.plhs.com 으로 확인 메일을 보내는 그림이다.



[그림 3-3-2-2-가-ㅈ]

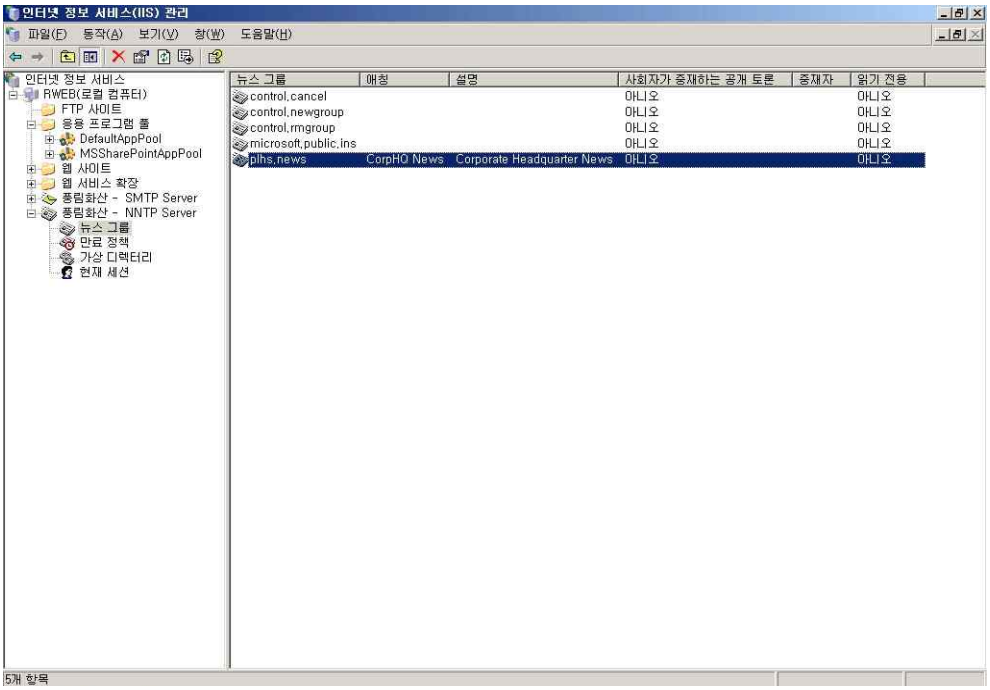
ㅊ 메일이 보내진 것을 확인할 수 있다.



[그림 3-3-2-2-가-ㅊ]

3.3.3 NNTP (Network News Transfer Protocol - news.plhs.com)

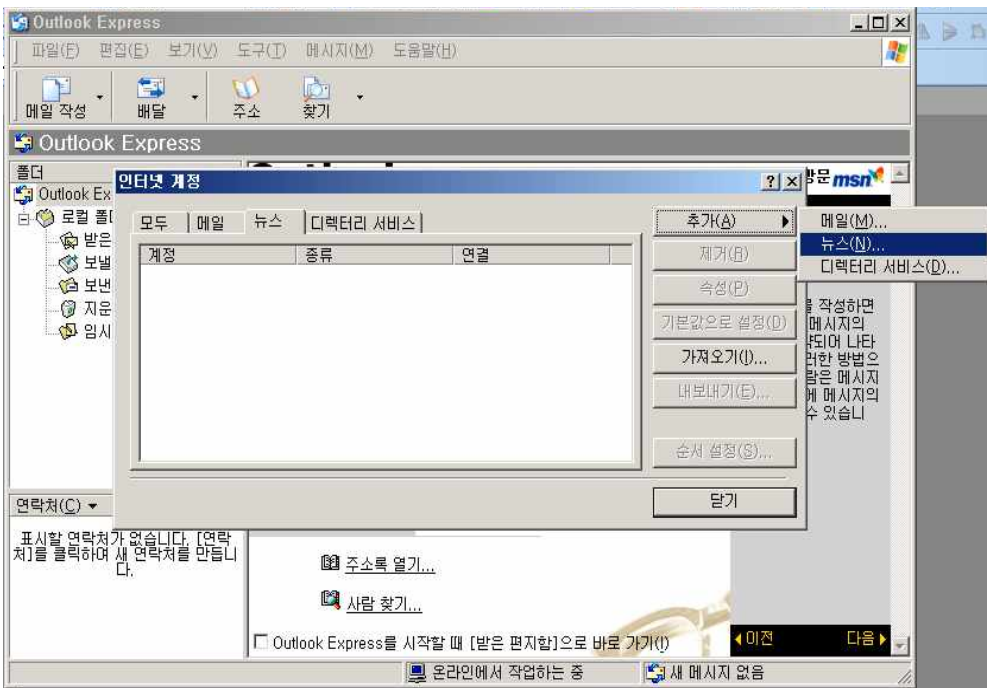
Windows Server 2003의 NNTP 서비스만 가지고도 회사 전체나 부서별 게시판으로 훌륭하게 사용할 수 있다. 그러나 전용 뉴스 클라이언트를 사용해야한다는 단점이 있다. [그림 3-3-3]은 rweb에 NNPT 서버를 구성한 그림이다.



[그림 3-3-3]

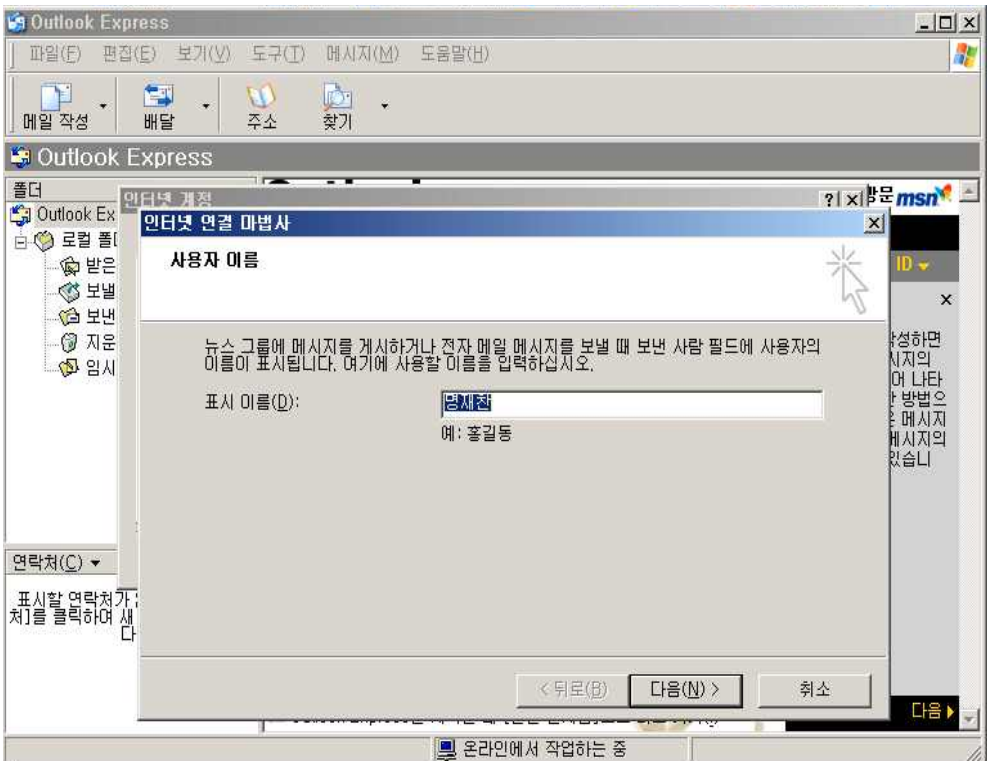
① 클라이언트의 Outlook Express의 뉴스계정 설정하기

㉮ Outlook Express 창에서 도구 > 계정을 선택한다.



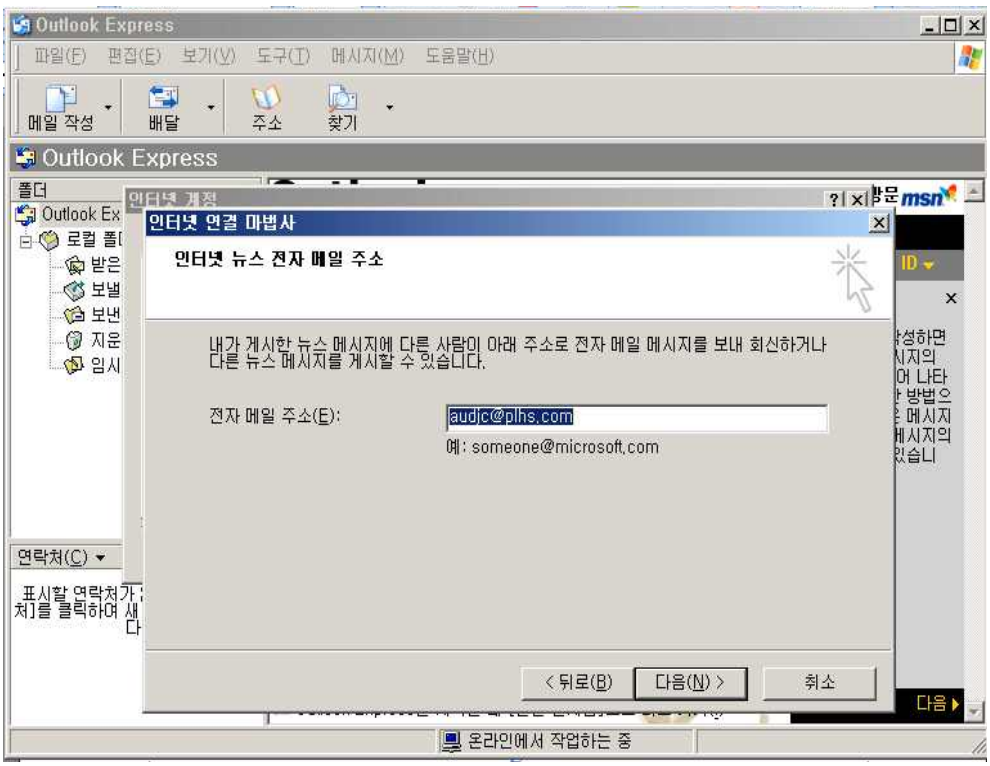
[그림 3-3-3-1-가]

㉰ Internet 연결 마법사 창에서 표시 이름에 해당 사용자 이름을 입력하고 다음을 누른다.



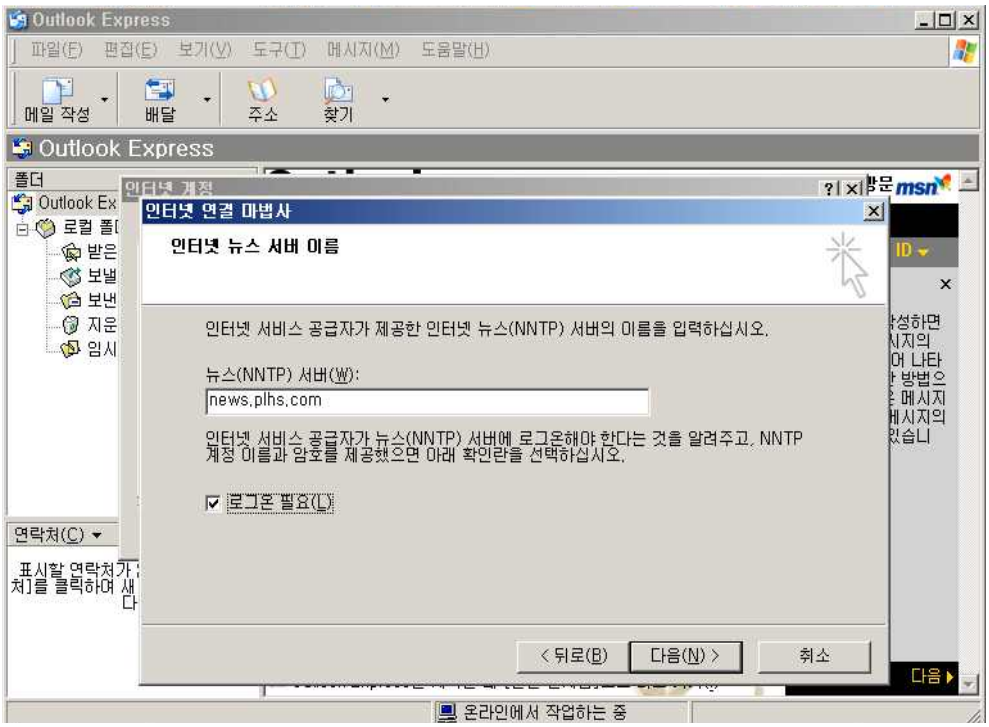
[그림 3-3-3-1-나]

㉱ Internet 뉴스 전자 메일 주소 페이지에서 전자 메일 주소에 사용자 ID@plhs.com 이라고 입력하고 다음을 누른다.



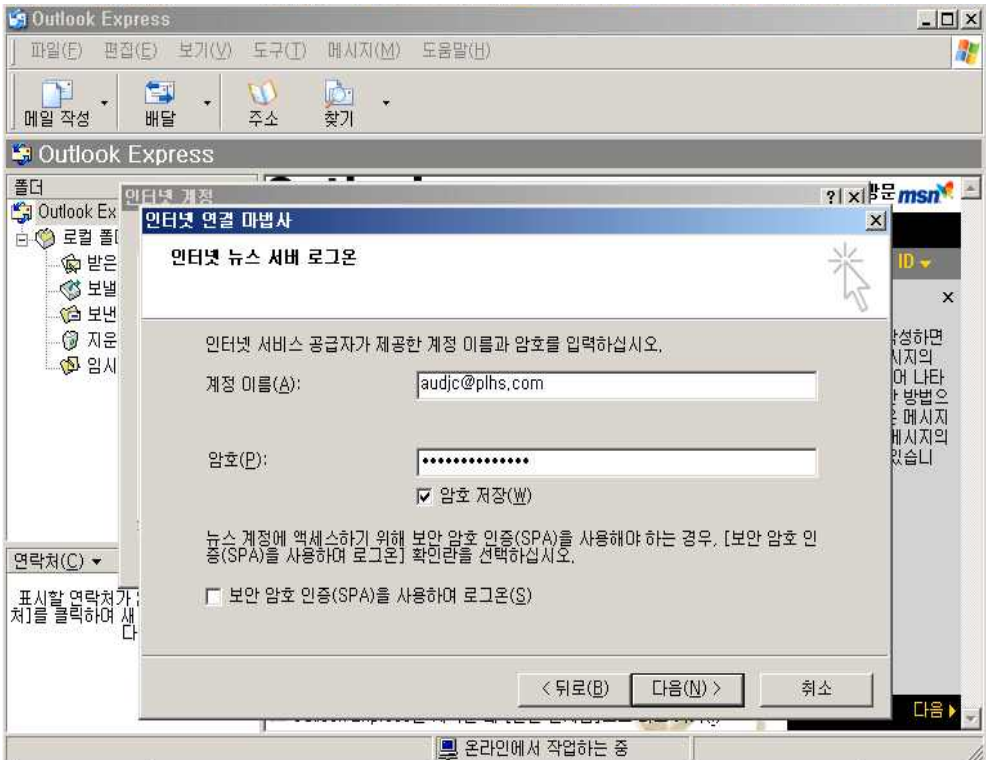
[그림 3-3-3-1-다]

㉲ Internet 뉴스 서버이름 페이지에서 뉴스(NNTP) 서버에 news.plhs.com 이라고 입력하고 로그온 필요를 선택한 후 다음을 누른다.



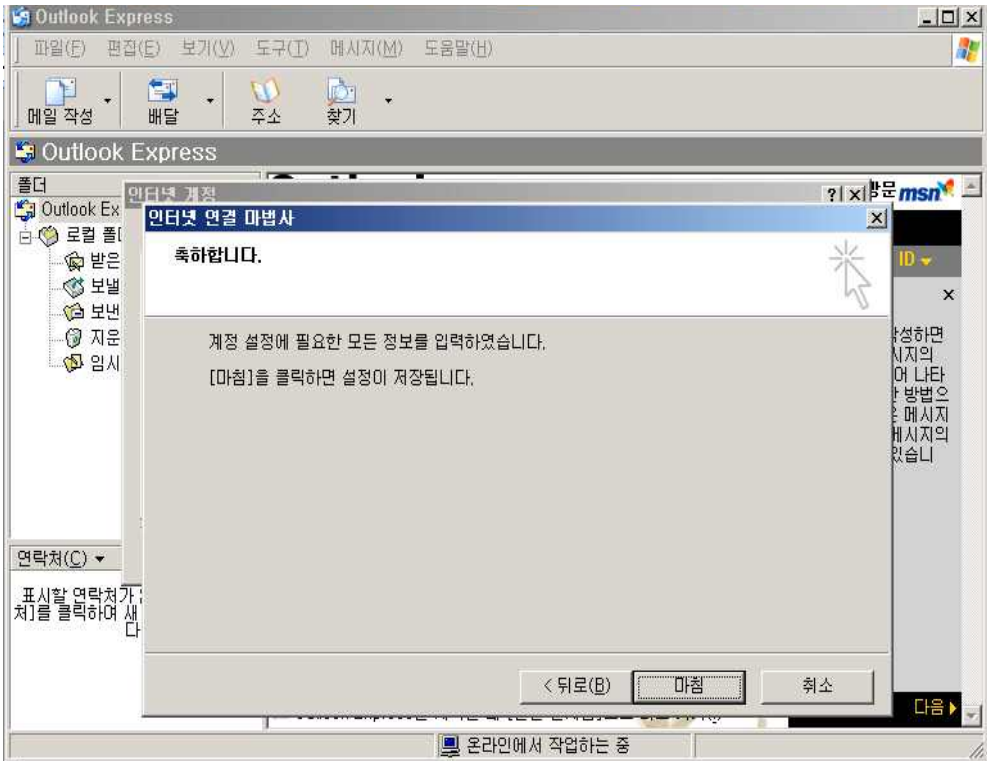
[그림 3-3-3-1-라]

㉳ Internet 뉴스 서버 로그온 페이지에서 계정 이름에 사용자 ID@plhs.com, 암호에 패스워드를 입력 하고 암호 저장이 선택되어 있는 것을 확인 후 다음을 누른다.



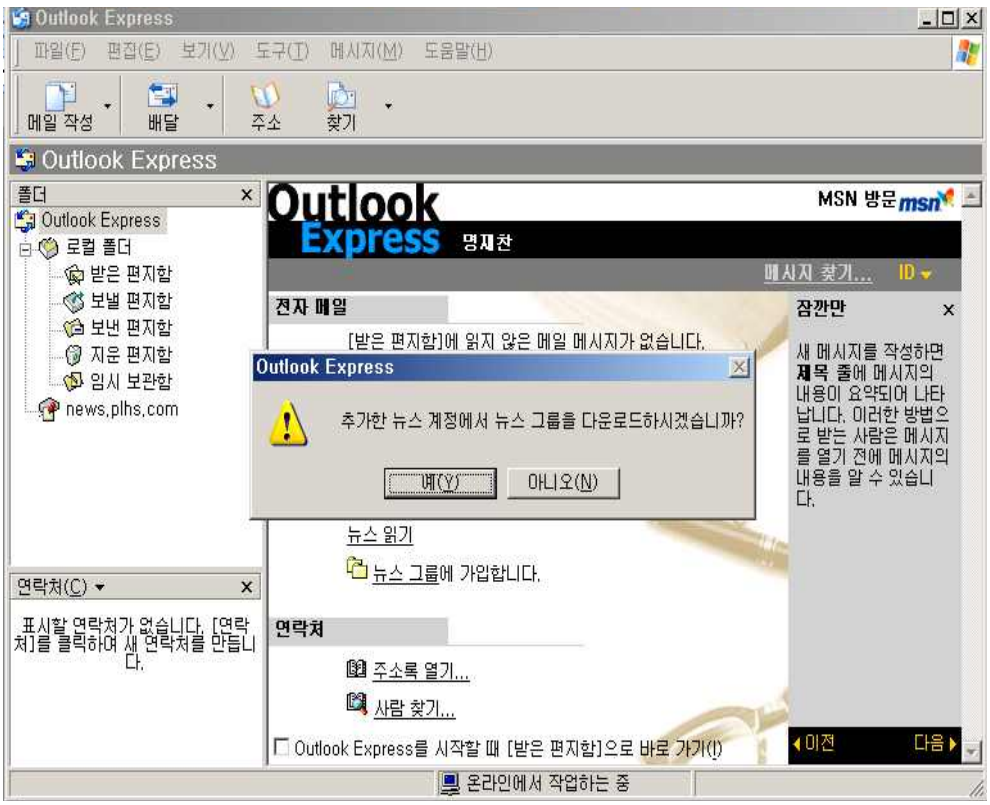
[그림 3-3-3-1-마]

㉰ 축하합니다 창에서 마침을 누른다.



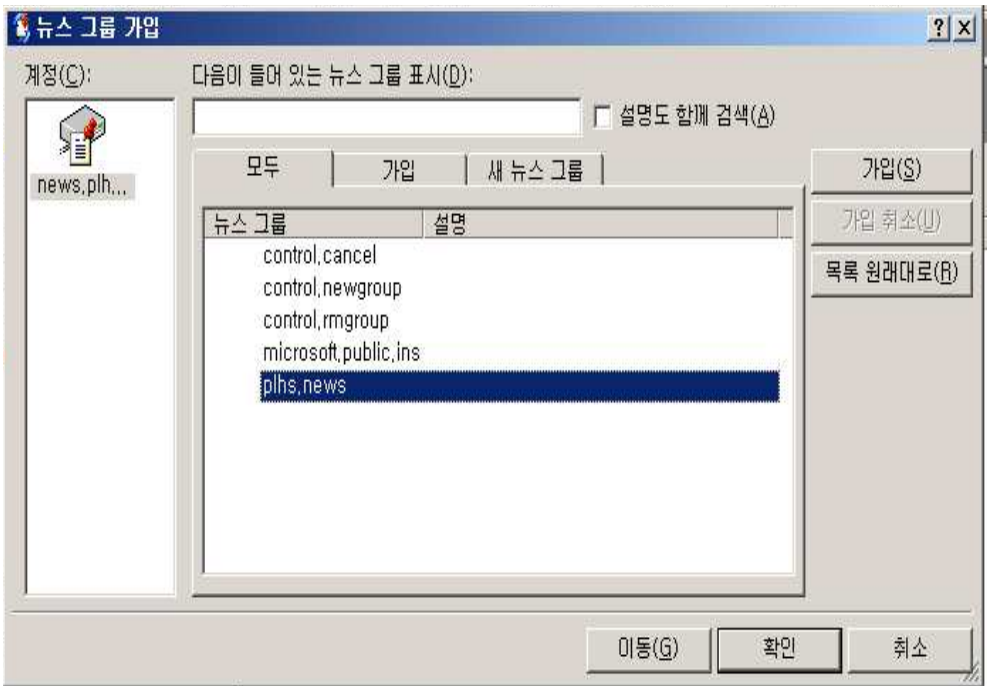
[그림 3-3-3-1-바]

㉱ Outlook Express 창에서 '예'를 누른다.



[그림 3-3-3-1-사]

㉮ 뉴스 그룹 가입 창의 뉴스 그룹 목록에서 plhs.news 를 선택하고 가입을 누른 후 확인을 누른다.

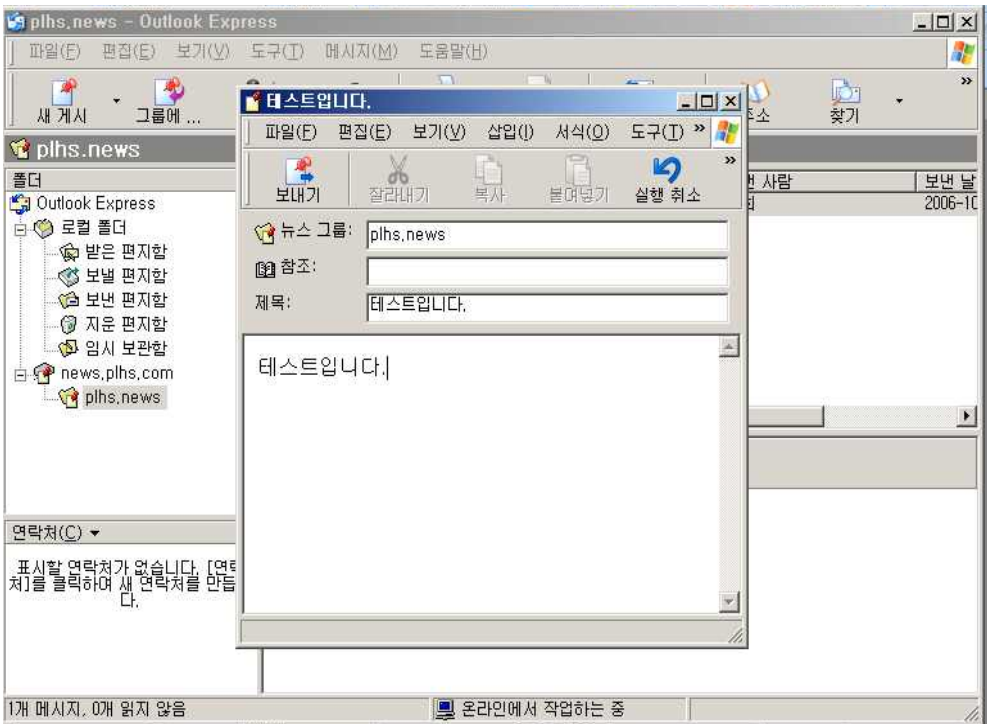


[그림 3-3-3-1-아]

② News 개재하기

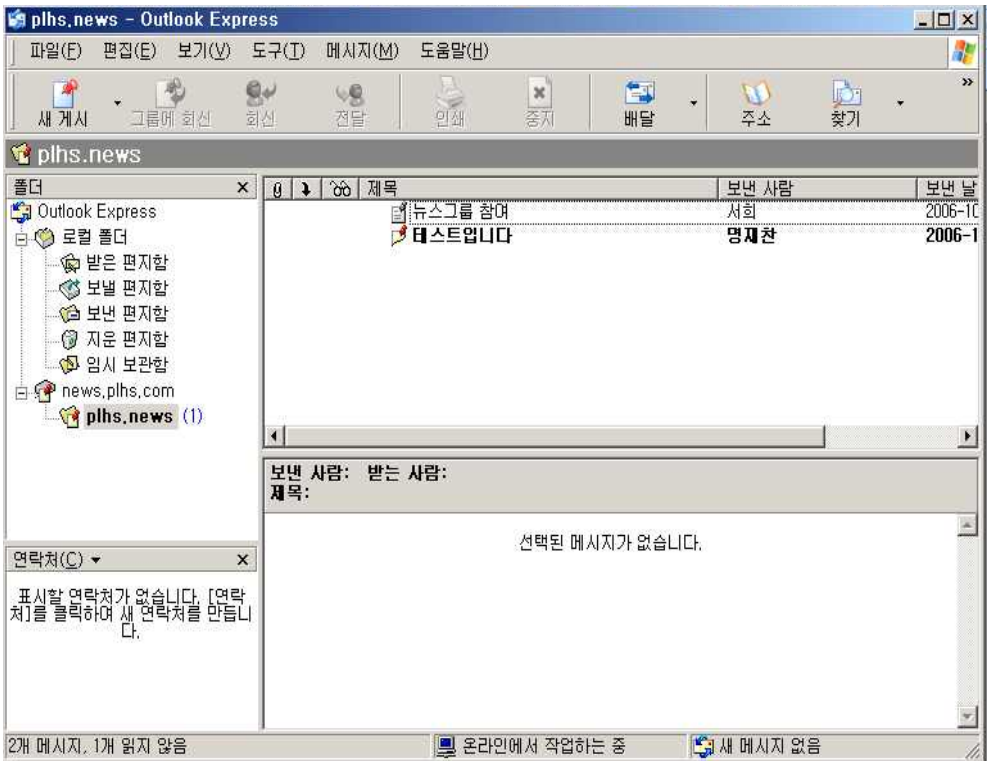
㉮ Outlook Express 창에서 news.plhs.com > plhs.news 를 선택한다.

㉯ Outlook Express 창에서 도구 모음의 새 게시를 누른 후 제목과 내용을 입력 하고 도구 모음의 보내기를 누른다.



[그림 3-3-3-2-나]

㉰ 메시지가 입력된 것을 확인할 수 있다.



[그림 3-3-3-2-다]

4. 결　　론

이번 졸업 작품으로 회사 내 인트라넷을 구축하고 VPN을 이용하여 원격지에서 사내망을 이용할 수 있게 VPN Server를 구축하여 운영해 본 결과 원격지에서 Windows XP이상의 운영체제가 설치되어있는 PC를 이용하여 간단한 설정만으로 회사 서버의 AD에 입력된 사용자 ID와 패스워드, 인증기관에서 발급 받은 인증서를 이용하여 사내망에 접속하여 인트라넷 웹사이트, E-mail, NNTP, 업무사이트 등을 이용할 수 있었다. 이는 기존 사설망 구축에 드는 장비, 회선비용을 획기적으로 절감할 수 있다. 그리고 경제적인 데이터 전송은 모든 회사에게 중요하다. VPN 서비스의 경제적인 효과는 시설 투자비용과 운영, 관리 측면에서의 일상적이고 반복적인 비용의 최소화를 통해서 충분히 보장된다.

보안 측면으로서 VPN은 EAP, MS-CHAP v2, MS-CHAP, CHAP, SPAP, PAP와 같은 인증방법을 이용하여 서버에서 원격시스템을 인증할 수 있고 Windows Server 2003에는 PPTP 외에 업계 표준인 L2TP도 포함되어 있어서 IPSec과 함께 안전한 가상 사설망 연결을 만드는데 사용된다. 또한 원격 액세스 정책으로 네트워크 관리자가 더욱 신축성 있게 원격 액세스 사용 권한과 연결 제한을 설정할 수 있도록 하는 조건 및 연결 설정을 할 수 있다. 또한 회사 내 업무사이트는 SSL을 이용하여 정보유출 방지, 데이터 변조 방지 등과 같은 보안을 한층 강화 하였다.

그러나 Internet이라는 공중망을 기본으로 하기 때문에 적절한 통신속도 및 대역폭의 보장과, 무엇보다 정보에 대한 보안이 확실하지 않다는 점이 큰 단점이라고 할 수 있다. 정보의 완벽한 보안을 보장받지 못한다면 서비스로서의 의미를 가질 수 없기 때문이다. 따라서 암호화, 전자인증과 같은 방식을 사용하여 전용사설망과 같은 안전한 자료전송을 모색해야 한다.

5. 부　　록

5.1 사　례

5.1.1 VPN

① 현재 국내에서는 가상사설망(VPN)의 도입을 검토하는 단계기 때문에 구체적인 VPN 적용사례를 찾아보기 어렵다. 상당수의 기업이 VPN을 도입하려는 움직임을 보이고 있어 올해 말부터는 국내에서도 실제적인 도입사례를 찾아볼 수 있을 것으로 예상된다. VPN 도입과 관련해 실제적인 적용사례는 대부분 외국기업에서 찾아볼 수 있다. 우선 미국의 세이버 랩스(Saber Labs)사는 미국 전역에 약 1천개의 지점망을 통해 여행 예약 시스템을 갖추고 있는 회사로 VPN을 도입하기 전까지는 1천여 개의 지점을 모두 다이얼업 접속 시스템으로 연결했으며 이를 위해 사내에 리모트액세스서비스(RAS) 시스템을 구축하고 별도로 5백여 개의 모뎀을 사용해 리모트 액세스 사용자들을 수용했다. 또한 이 회사는 회사 내부적으로 문서 교환에 따른 보안을 위해 별도의 Internet망을 보유하고 있었다. 이처럼 최근까지 가장 보편적이면서도 안정적이고 저렴한 비용으로 활용 가능했던 것으로 평가됐던 세이버 랩스사의 이러한 네트워킹 방법은 시간이 흐름에 따라 몇 가지 문제점이 발견되게 된다. 우선 모뎀에서 발생하는 속도 지연 등의 많은 장애를 극복해야 하며 모뎀의 전송 기술이 향상될 때마다 서비스의 질적 향상을 위해서는 기존 모뎀을 교체해야 했다. 또한 리모트 액세스망의 관리를 위해서는 네트워크 관리자 외에 별도로 리모트 액세스 망 관리자가 배치돼야 했다. 특히 일반 전화요금이 전용선 비용보다 저렴하기는 하지만 미국 전역의 1천여 개 지점에서 사용하는 시외전화요금도 무시할 수 없는 수준에 도달하게 됐다. 결국 세이버 랩스사는 VPN을 도입해 기존의 다이얼업 접속망을 Internet에 연결시켰으며 이를 통해 연간 40% 이상의 통신비용을 절감했다. 또한 중앙 본사에 VPN 게이트웨이를 설치함에 따라 기존의 모뎀 풀 장비를 철수시켰으며 모뎀장비로 가득 찼던 전산실의 공간을 효율적으로 활용할 수 있게 됐다. 특히 리모트 액세스를 이용하는 여행사들의 접속 불만이 해소되고 서비스 품질 향상에 대한 요구 사항들은 각 지역의 Internet서비스업체(ISP)들이 담당함에 따라 세이버 랩스사는 운영상의 부담을 줄일 수 있었다. 이 밖에 각 지역의 여행사들은 비싼 시외전화요금을 부담하지 않고 자신의 지역에 있는 ISP의 망을 이용하므로 시내요금으로 업무를 처리할 수 있어서 본사와 지사 양측에서 비용절감 효과가 있었으며 신기술의 수용에 적극적인 ISP에 의해 세이버 랩스사는 오히려 신기술의 변화에 신속하게 대처할 수 있게 됐다.

② 세이버 랩스사와 비슷한 환경을 가지고 있었던 미국의 「피델리티(Fidelity)투자회사」는 미국 전역에 있었던 투자자들과 협력회사, 이동이 많은 직원들을 위해 본사에 RAS를 구축해 전화 접속으로 리모트 액세스를 활용하고 있었다. 하지만 이 회사 역시 운영상의 어려움과 통신비용 절감을 위해 VPN을 도입했으며 일반 전화망을 이용했던 기존의 모든 POP(Point of Present) 접속을 각 지역의 ISP의 망을 이용함에 따라 피델리티사 역시 전체 경비의 40% 이상을 줄일 수 있게 됐다.

③ 현재 국내 기업이 가상사설망(VPN)을 도입해 효과적으로 활용중인 사례를 찾아보기는 어렵다. 국내에서는 VPN이 이제 막 도입 단계에 와 있기 때문이다. 따라서 현재 VPN 도입을 검토 중인 기업과 VPN을 활용할 경우 상당한 효과가 예상되는 기업의 「VPN 도입 시나리오」를 살펴보겠다.　여러 지역에 대리점을 가지고 있는 국내 기업들의 상당수는 전용선 또는 다이얼업 접속을 통해 대리점과 통신하고 있으며 이들 업체들은 모두 VPN을 도입함으로써 통신비용을 절감할 수 있다. 전국에 2천여 개의 대리점을 보유하고 있는 A사는 대리점과의 통신을 위해서 중앙에 대형 라우터를 설치하고 각 대리점과 중앙센터를 56kbps 속도의 라우터 전용선으로 연결해 프레임 릴레이 망을 이용하고 있다. VPN 개념이 도입되기 전까지는 이 방법이 최선이었지만 전문가들은 A사가 VPN을

도입할 경우 현재 소요되는 비용의 50% 이상을 절감할 수 있을 것으로 보고 있다. 지난번에 언급한 외국의 도입 사례가 다이얼 접속 비용을 절감하는 것이었다면 A사는 전용회선의 비용을 줄일 수 있다는 것이 다른 점이다. A사가 VPN을 도입하면 2천여 개의 대리점들은 현재 서울의 중앙센터로 연결된 56kbps 전용선을 철거하고 단지 대리점과 가장 가까운 Internet서비스업체(ISP)들과 56kbps 전용선으로 연결해 본사와 VPN 통신을 이용하면 된다. VPN 도입에 따른 효과로는 우선 회선비용 절감을 꼽을 수 있으며 아울러 전용선 백업을 위한 종합정보통신망(ISDN)이나 다이얼 업 망도 가까운 ISP의 망을 이용한다면 훨씬 더 안정되고 저렴한 백업 망까지 확보할 수 있다.

정유회사와 주유소를 연결해 각종 업무를 서비스하고 있는 B사는 정유회사들을 위해 하나의 서버를 구성하고 공통된 업무를 취급하고 있다. 또한 전국에 산재해 있는 정유회사와 주유소를 연결하기 위해서 별도의 전용선망을 설치 운영하고 있다. B사 역시 VPN을 도입함으로써 전용선 비용을 크게 줄일 수 있다.

이처럼 다이얼업 접속비용을 줄이는 외국사례와 전용회선 비용 절감에 초점을 둔 국내 시나리오들에서 볼 수 있듯이 그동안 통신을 사용하는 업무의 빈도수 또는 접속 통계에 따라 전용선을 구성할지 아니면 다이얼업 접속을 이용할 것인지에 대해 고민해왔지만 VPN을 도입하면 이 문제를 간단히 해결할 수 있고 비용도 크게 줄일 수 있다. 이 밖에 VPN을 도입할 수 있는 대상으로는 학교를 꼽을 수 있다. 일반적으로 학교들은 자매 결연을 맺은 다른 학교와의 통신을 위해 VPN을 적용할 수 있으며 교직원 및 직원들의 재택근무에도 활용할 수 있다.

이처럼 단일지역에서 다중을 대상으로 회선 서비스를 하고 있는 업체와 기관에서는 VPN을 활용하면 다양한 이점을 얻을 수 있다. 다만 VPN을 API까지 제공되는 기술로 이용한다면 각각의 특수한 환경을 구성해야 한다는 점에 유의해야 한다.

5.1.2 IPSec-VPN

① IPSec 가상사설망(VPN)을 대체할 신제품으로 주목받았던 SSL(secure sockets layer) VPN이 당초 전망과 달리 IPSec-VPN을 보완하는 보안 장비로 자리 잡고 있다. SSL-VPN은 특정 프로그램을 단말기에 미리 설치할 필요 없이 Internet 접속이 가능한 환경이라면 어디에서나 VPN에 접속이 가능해 편리성이 높다. 이와 달리 IPSec-VPN은 미리 정해진 단말기와 네트워크 등 상호 신뢰할 수 있는 양쪽 네트워크를 연결할 때 높은 보안성을 제공한다. 하지만, 시간과 장소, 단말기 여부에 관계없이 기업의 중요 애플리케이션과 데이터에 접속해야 하는 상황이 늘어나면서 IPSec-VPN이 한계에 부딪혔다. 개발 기업들은 SSL-VPN이 IPSec-VPN을 대체할 것이라 전망했지만 SSL-VPN이 상용화된 후 3년여가 지나면서 주로 원격접속 용도로 새로운 시장을 창출하고 있다. 최근 기업이나 기관들은 내부 네트워크는 IPSec-VPN을, 원격접속은 SSL-VPN을 이용하는 조합형으로 VPN을 구축하고 있다. 최근 SSL-VPN을 도입한 동국제강그룹은 본사와 지사 간 네트워크는 IPSec-VPN으로 구축했으며, 외부 출장자 및 협력사의 내부망 접속을 위해 별도로 SSL-VPN을 도입했다. VPN 업체인 나노엔텍(대표 장준근, 김광태)은 동국제강 외에도 주택금융공사, 신동아건설, 한국 신용정보, 증권예탁결제원, 롯데건설, 현대푸드시스템, 롯데마트 등 20여 곳이 이 같은 형태의 VPN을 구축했다고 밝혔다. 넥스지(대표 주갑수) 역시 많은 기업들이 SSL-VPN과 IPSec-VPN을 혼합해 구축하는 사례가 증가했다고 설명했다. 넥스지는 자체 개발 솔루션인 IPSec-VPN ‘V포스 시리즈’와 아벤테일의 SSL-VPN을 동시에 영업해 상반기에만 50억원이 넘는 매출을 올렸다고 밝혔다. 김광태 나노엔텍 보안사업부문 사장은 “외부 접속자를 위한 원격 전송 용도로 SSL VPN을 구축하는 기업이 늘어나고 있다”며 “SSL VPN이 IPSec VPN을 대체하기보다 서로 기능을 보완하는 형태로 발전하고 있다”고 설명했다.

5.1.3 SSL-VPN

① 보안 시장의 관심이 통합보안 솔루션인 UTM(Unified Threat Management)으로 옮겨가면서 UTM의 시장 잠재성을 검증받고 있는 가운데, 그동안 엔터프라이즈를 겨냥해 왔던 SSL-VPN 제품이 새로운 IT 기능을 대거 탑재하고 전열을 가다듬고 있다. 특히 액티브X 또는 자바 플러그인 기반 애플리케이션의 사용이 크게 증가하면서 웹 브라우저를 이용한 원격지 접속에 대한 보안 솔루션으로 SSL-VPN이 각광을 받고 있다. Internet 접속이 가능한 사용자의 웹 브라우저에 내장된 SSL(Secure Sockets Layer) 기능을 이용한 VPN(Virtual Private Network) 기술이 엔터프라이즈 시장에서 여전히 강세다. 네트워크 자원에 대한 안전한 액세스를 비용 효과적으로 확장해주고 기업의 생산성 향상과 더불어 IT 비용을 크게 절감시켜주고 있기 때문이다. 이달 중순 미국 시장조사 업체인 시너지 리서치 그룹이 발표한 '올 1분기 세계 네트워크 시큐리티 솔루션 시장' 분석 보고서에 따르면 SSL-VPN 시장이 지난 4분기 연속 고속 성장을 했다고 발표했다. 이런 성장세는 매년 큰 증가세를 유지하고 있는데 연 39%의 성장률을 보이고 있는 것으로 내다봤다. 이런 시장 분석 자료가 아니더라도 SSL-VPN 시장의 고공세는 각 벤더의 제품 업그레이드 발표에서도 찾아 볼 수 있다. 현재 국내 시장에서 SSL-VPN 관련 솔루션을 판매하는 벤더는 10여 개에 달한다. 대부분 외산 제품이지만, 이들 벤더는 최근 몇 개월에 걸쳐 기술과 기능을 크게 업그레이드한 SSL-VPN 솔루션을 경쟁으로 발표했다. 그리고 지난 5월 중순에는 마이크로소프트가 SSL-VPN 제품을 포함하는 시큐어 액세스 제품을 공급하는 웨일 커뮤니케이션을 인수하면 이 시장에 발을 내디뎠다. 하지만 SS- VPN 시장에 대한 부정적 전망도 쏟아져 나오고 있다. 이는 요즘 보안 시장의 화두로 등장한 UTM 때문이다. 통합보안 솔루션인 UTM(Unified Threat Management)은 보안 위협이 고도화됨에 따라 기존의 한두 가지 보안 솔루션으로 대응하기 어렵다는 인식에서 출발해 하나의 장비에 VPN, 파이어 월, 침입탐지, 안티바이러스 등의 여러 보안 기능 전부, 혹은 일부를 동시 통합 구현한 제품을 말한다. UTM은 중소규모, SSL-VPN은 엔터프라이즈 겨냥한다. 그러나 이 솔루션은 엔터프라이즈 시장이 아닌 중소 규모의 환경에서 도입 적용하기가 적당하다는 의견이 지배적이다. 실례로 최근 미국 보안 시장서 발표되고 있는 UTM 솔루션은 대부분 50명 이하의 사용자를 둔 기업 시장을 겨냥하고 있다. 이에 따라 기존 파이어 월이나 VPN 등의 특화되고 엔터프라이즈 규모의 보안 전문 시장을 급속히 잠식하지는 않을 것으로 전망된다.

참고 자료

문 헌

How To Windows Server 2003
(출판사: On좋은강의 좋은Off / 저자: 이주원 이항주 저)
Windows Server 2003
(출판사: 정보문화사 / 저자: 마크미나시 외 공저 송원석, 신명식, 이종진, 김태훈 공역)
Windows 2000 Server
(출판사: 한빛미디어 / 저자: 이병훈, 조문영, 한정혜)

사이트

한국 마이크로 소프트: http://www.microsorft.co.kr
한국 전자인증: http://www.crosscert.com
(주)코리아 휴먼 리소시스: http://www.koreahr.co.kr
(주)프리렉: http://www.freelec.co.kr
ITBANK: http://www.itzzang.co.kr
해커즈뉴스: http://www.hackersnews.org