윈도우 보안 지침

Ver 1.0
작성일 : 2005.08.01
작성자 : 100dedi.com

== 목 차 ==

[12] FTP 익명 접속 거부

[13] MS-SQL 서비스팩 설치

[14] 윈도우 보안도구

1. MBSA
2. IIS Lockdown
3. URLScan

[15] 네트워크 보안

1. NetBIOS 비활성화
2. SMB 비활성화
3. TCP Stack 강화하기

[16] 홈페이지 보안 관리

1. 관리자페이지 접근통제 취약점
2. 디렉토리 리스팅 취약점
3. 파일 다운로드 취약점
4. 크로스 사이트 스크립트 취약점
5. 파일 업로드 취약점
6. SQL Injection 취약점

[17] 터미널서비스 포트변경하기

[18] 후기

[1] 보안 체크리스트

1. 파일시스템은 NTFS로 포멧되었는가?
2. OS부분과 데이타(웹서비스,DB) 파티션이 분리되어 있는가?
3. 서비스에 필요한 필수 구성요소만을 설치하고, 불필요한 서비스는 정지하였는가?
4. Administrator 계정 그룹에 대한 계정명 변경 및 강력한 패스워드정책을 적용하였는가?
5. 불필요한 계정(Guest)은 사용하지 않는가?
6. 계정 잠금정책이 있는가?
7. 파일 및 디렉토리 보호정책이 있는가?
8. 익명접속으로부터 레지스트리가 보호되는가?
9. LSA 정보에 대한 접근이 보호되는가?
10. 공유폴더를 사용하고 있지는 않는가?
11. 서비스팩 및 최신보안패치를 설치하였는가?
12. 자동 업데이트 실행 설정을 하였는가?
13. IPSec 필터링 설정을 하였는가?
14. 바이러스 방역제품을 설치 및 설정하였는가?
15. 에러에 대한 이벤트 로그 설정을 하였는가?
16. 모니터링 솔루션을 설치 및 설정하였는가?
17. 백업 설정을 하였는가?
18. IIS 서비스 설치 및 설정
    1) IIS 서비스에 필요한 구성요소만을 설치하였는가?
    2) 웹서비스확장은 필수적인 것만 enable 하였는가?
    3) 컨텐츠을 독립적인 파티션에 저장하고 있는가?
    4) NTFS 퍼미션을 적용하였는가?
    5) IIS 웹사이트 퍼미션을 설정하였는가?
    6) 기본서비스 익명계정을 사용자지정 계정으로 변경하였는가?
    7) IIS 로깅을 설정하였는가?

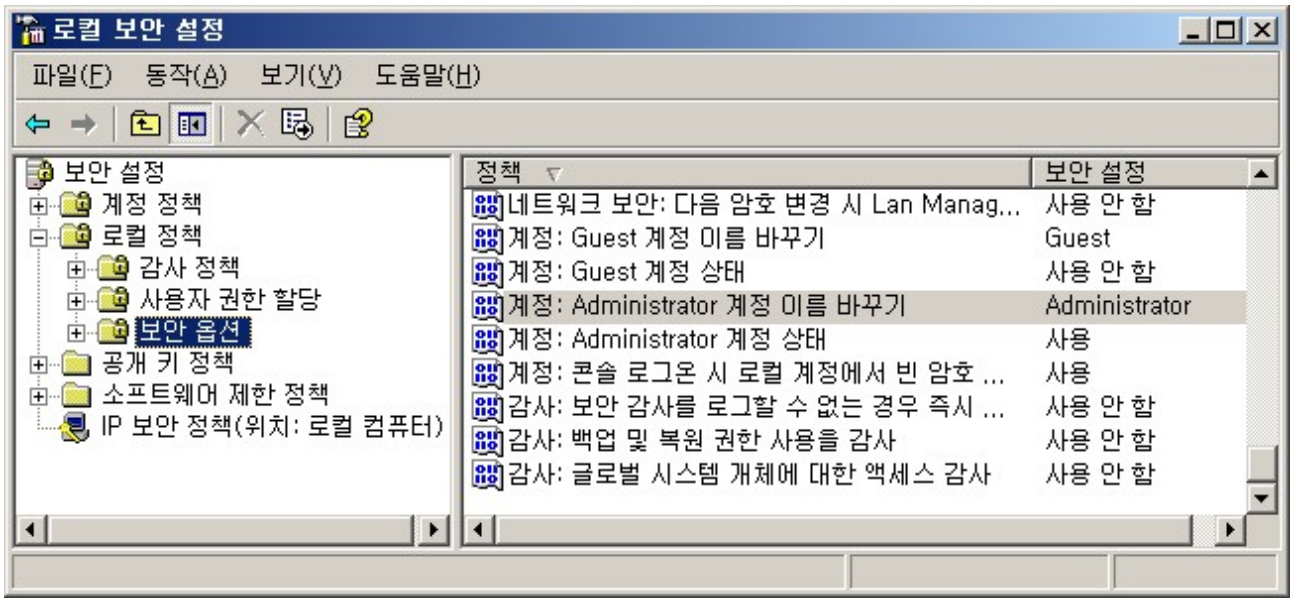
[2] 계정관리

1. 기본계정명 변경

시스템설치시 기본적으로 생성되는 두 기본계정의 이름을 변경한다.

1) Administrator 계정 이름 변경

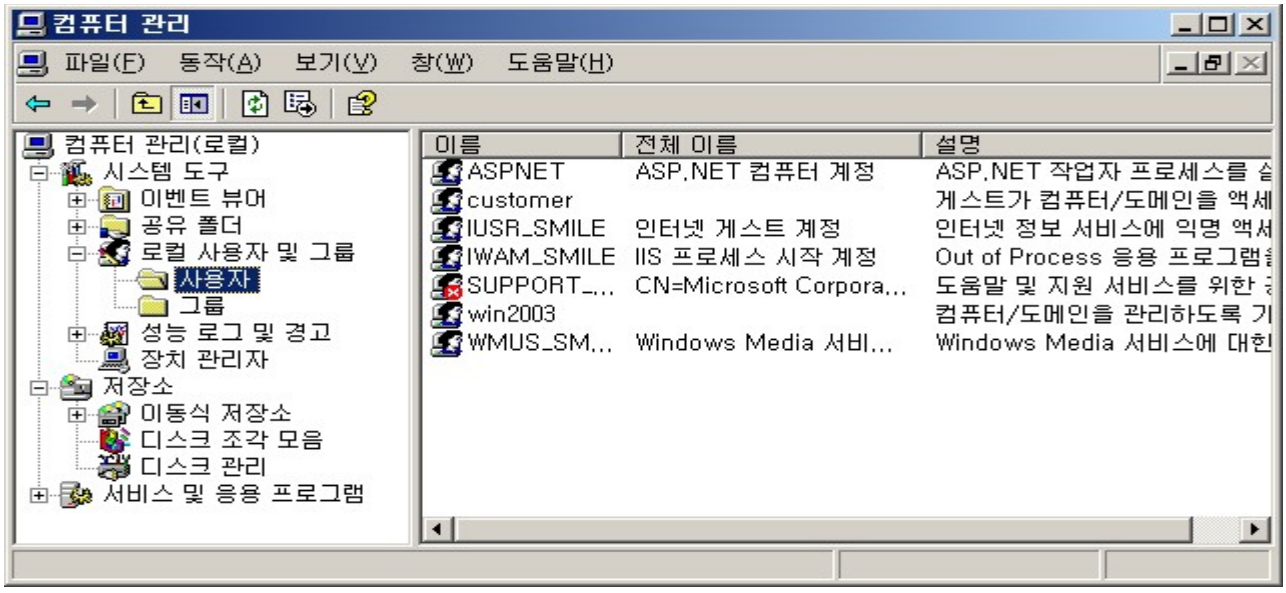
Adminitrator : [시작] -> [설정] -> [제어판] -> [관리도구] -> [로컬보안설정] -> [로컬정책] -> [보안옵션]
-> [계정:Adminitrator 계정 이름 바꾸기] -> [속성] 에서 이름 변경



2) Guest 계정 이름 변경

Guest : [시작] -> [설정] -> [제어판] -> [관리도구] -> [로컬보안설정] -> [로컬정책] -> [보안옵션] -> [계정: Guest 계정 이름 바꾸기] -> [속성] 에서 이름 변경

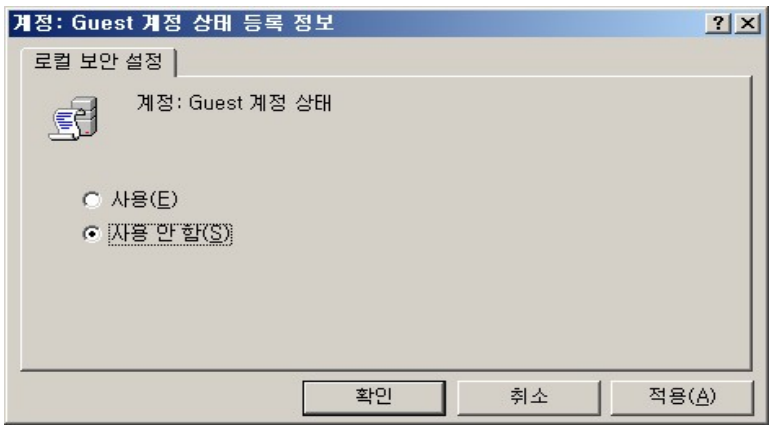
변경된 정보 확인 : [시작] -> [제어판] -> [관리도구] -> [컴퓨터관리] -> [로컬사용자및그룹] -> [사용자]



2. Guest 계정 비활성화

Guest 계정은 컴퓨터에 익명 접속을 연결할 때 사용되는데 이를 비활성화하여 익명 연결을 제한한다.

[시작] -> [설정] -> [제어판] -> [관리도구] -> [로컬보안설정] -> [로컬정책] -> [보안옵션] -> [계정: Guest 계정 상태] -> [속성] 에서 사용 안 함으로 변경



3. 사용하지 않는 계정 제거

서버에서 사용되지 않는 계정들은 공격자가 이 계정을 이용해서 접근할 수 있으므로 제거한다.
또한 단순하거나 유추하기 쉬운 패스워드는 무차별 대입 공격(brute force)이나 사전 공격(dictionary attack)에 취약하므로 복잡한 패스워드를 사용한다.
계정관리는 최소한의 계정과 최소한의 권한만을 부여한다.

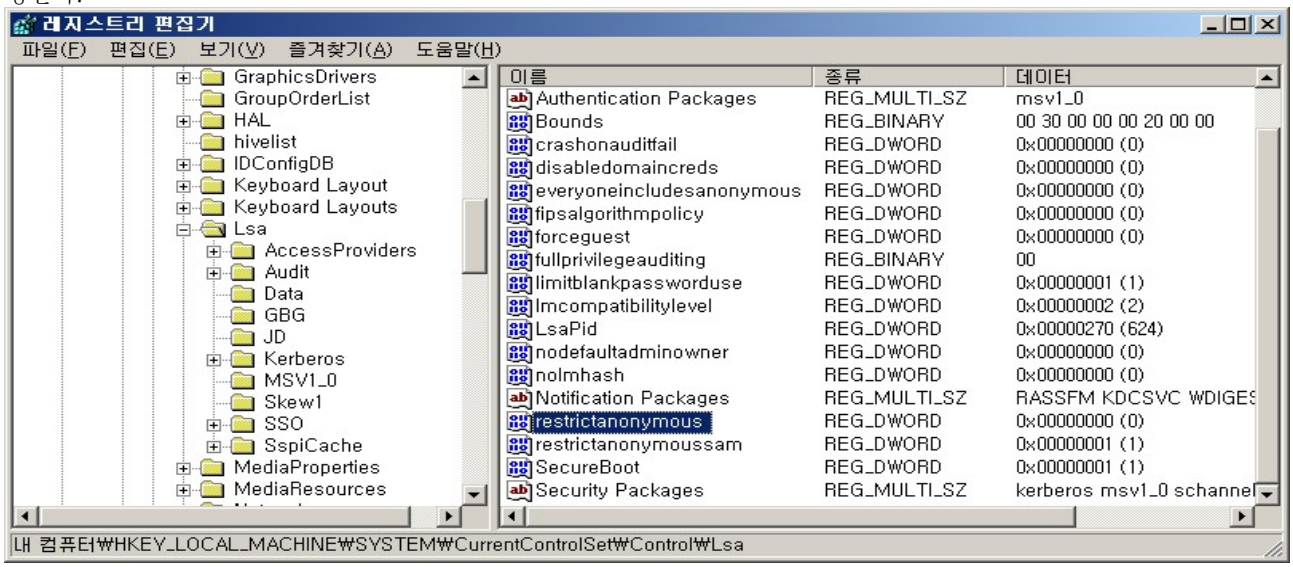
4. 기본 익명 계정(IUSR_Machine) 대신 사용자 정의한 계정 사용

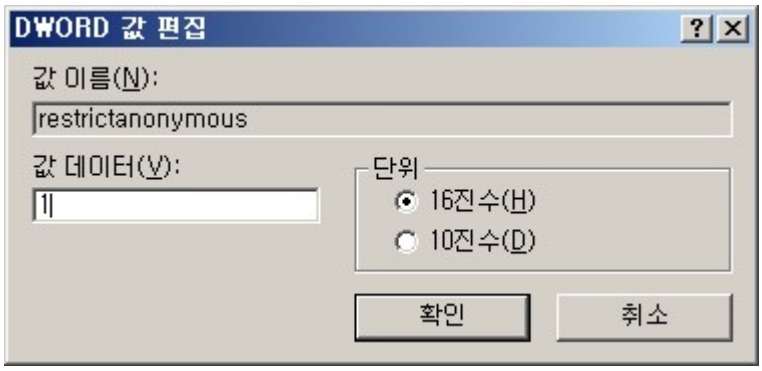
인터넷으로 익명 접근하는 사용자들은 IIS 설치시 기본적으로 생성되는 IUSR_Machine (서버의 NetBIOS명) 계정으로 접근하게 된다. 예를 들어 'SMILE'라는 이름의 서버에는 'IUSR_SMILE'이라는 계정이 생성된다. 이 계정을 비활성화하고 웹 서버의 익명 접속에 사용할 계정을 직접 재정의한다.
웹 애플리케이션의 기능을 제공하는데 필요한 최소한의 권한을 가지는 계정을 만들고, 인터넷 정보 서비스 관리에서 웹 애플리케이션 별로 직접 정의한 계정을 지정하면 서버상에 여러 개의 웹 사이트를 운영하는 경우 로그 분석에도 용이하다.

[인터넷정보서비스관리] -> [해당사이트의 속성] -> [디렉토리보안] -> [인증 및 액세스] -> [편집] -> 익명사용자 계정변경

5. 익명 로그온(null session) 비활성화

널 세션(Null Session) 접속은 인증을 받지 않은 상태에서 해당 컴퓨터에 접근하는 것을 의미하며, 해커들은 이를 이용해서 원격 컴퓨터의 정보를 제공 받을 수 있고, 특정 권한으로 승격하거나 DoS 공격을 수행할 수도 있다. 널 세션 접속을 허용하지 않으려면 레지스트리 편집기([시작] -> [실행] -> [regedit])를 이용해서 'HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Lsa' 키의 restrictanonymous 값을 '1'로 설정한다.





[3] 패스워드 관리

계정 암호에 대한 무차별 대입 공격이나 사전 공격을 막기 위해 암호의 최소 길이나 특수문자의 사용여부 등을 지정하여 보다 강화된 정책을 사용한다.
패스워드는 C:₩WINDOWS₩system32₩config₩SAM 파일에 저장되며 운영체제가 동작중에는 시스템계정외에는 접근이 금지된다.

1. 암호정책

[시작] -> [제어판] -> [관리도구] -> [로컬보안설정] -> [계정정책] -> [암호정책]

아래 표와 같이 설정을 권장한다.

암호 정책	기본 설정	최소 권장 설정
암호 복잡성 만족	사용 안함	사용
최근 암호 기억	0개	24개
최대 암호 사용 기간	42일	42일
최소 암호 길이	0문자	8문자
최소 암호 사용 기간	0일	2일
해독 가능한 암호화를 사용하여 암호저장	사용 안함	사용 안함

패스워드 생성규칙 : 최소 8자 이상, 영문(대소)+ 숫자+ 기호 혼용, 이전 암호와 다른 암호 사용, 자신의 정보와 관련된 내용 사용 금지, 사전단어 사용 금지.

2. 계정 잠금 정책

[시작] -> [제어판] -> [관리도구] -> [로컬보안설정] -> [계정정책] -> [계정잠금정책]

아래 표와 같이 설정을 권장한다.

계정 잠금 정책	기본 설정	최소 권장 설정
계정 잠금 기간	적용할 수 없음	30분
계정 잠금 임계값	0번의 잘못된 로그온 시도	5번의 잘못된 로그온 시도
다음 시간후 계정 잠금수를 원래대로 설정	적용할 수 없음	30분

패스워드 추출도구 : http://limestone.truman.edu/pub/win32/apps/pwdump3/pwdump3v2.zip
shadow 파일 크랙도구 : http://openwall.com/john/c/john-16w.zip

[4] 시스템 실행명령어 권한 설정

C:₩WINDOWS 밑에 explorer.exe 와 링크파일인 explorer 의 속성을 선택한 뒤 [보안]탭에서 Administrator을 제외하고 나머지 계정은 삭제한다. 특히 바이러스의 경우 해당 explorer.exe 를 변경을 시키거나 복제를 시켜 윈도우 사용에 지장을 초래하거나 사용자가 모르는 불법적인 코드가 explorer.exe에 첨부될수가 있으니 권한 재조정을 통해 바이러스 감염 및 침입자의 이용으로부터 막도록 한다.

C:₩WINDOWS₩systerm32₩cmd.exe 등의 시스템 명령어도 Administrator 계정외에는 접근을 제한한다.
실제적으로 서버관리자를 제외하고는 대부분의 사용자들은 위의 파일을 실행시킬 필요성이 없다. 각종 웜바이러스 및 코드 레드의 경우 cmd.exe 파일을 복제하여 권한을 획득하는 경우가 다반사이기 때문에 근본적으로 접근자를 제외하고는 나머지 권한은 제거해주는 것이 좋다.
예) %systemroot%₩system32₩cmd.exe -> [속성] -> [보안]탭 -> Administrator 외의 계정 제거

[5] 레지스트리 보호

레지스트리의 원격 액세스 권한은 관리자에게만 부여되어 있는지 확인한다.

HKEY_LOCAL_MACHINE₩System₩CurrentcontrolSet₩Control₩SecurePipeServers₩winreg 의 키값이 생성되어 있는지, 사용권한은 Adminitrator외의 사용자나 그룹이 등록되어 있지는 않는지 확인한다.

[6] 공유

서버에서 사용되지 않는 공유를 제거하고 사용중인 공유 자원에 대해서는 NTFS 권한을 부여하여 자원을 보호한다. 특히 기본적으로 공유가 생성될 때 모든 사용자들에게 모든 권한이 부여되므로 NTFS 권한을 적용해서 필요한 사용자에게만 접근을 허용하도록 관리해야 한다.
또한 관리목적에서 사용되는 C$, ADMIN$와 같은 관리 공유를 사용하지 않는다면 제거하는 것이 권장된다. 관리 공유를 사용하지 않으려면 레지스트리 편집기를 이용해서
'HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩lanmanserver₩parameters' 키에 AutoShareServer와 AutoShareWks 값을 REG_DWORD로 만들고 '0'으로 설정한다.

[제어판] -> [관리도구] -> [컴퓨터관리] -> [공유폴더] -> [공유] -> 공유목록선택후 공유중지

[7] 파일시스템 관리

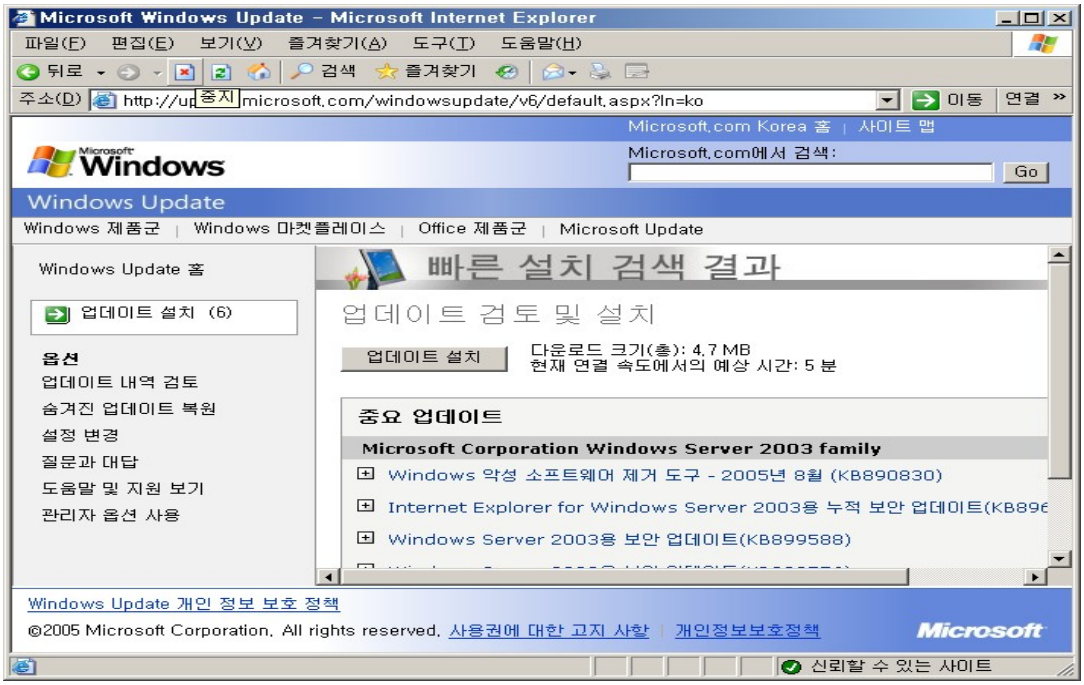
시스템의 중요 파일 및 디렉토리 내용의 변화 여부를 확인하는 파일 무결성검사를 실시한다.
Perl 이 설치된 시스템에서 사용가능하다.

Fcheck : http://www.geocities.com/fcheck2000/FCheck_2.07.59.zip

fcheck 수정 -> fcheck.cfg 수정 -> 무결성 DB 생성 -> 무결성 검사

[8]. 보안패치 및 서비스팩 설치

부언 설명할 필요가 없을 것이다. 시스템관리자라면 백업과 보안패치만은 반드시 하도록 하자.
Update Site : http://v4.windowsupdate.microsoft.com/ko/default.asp



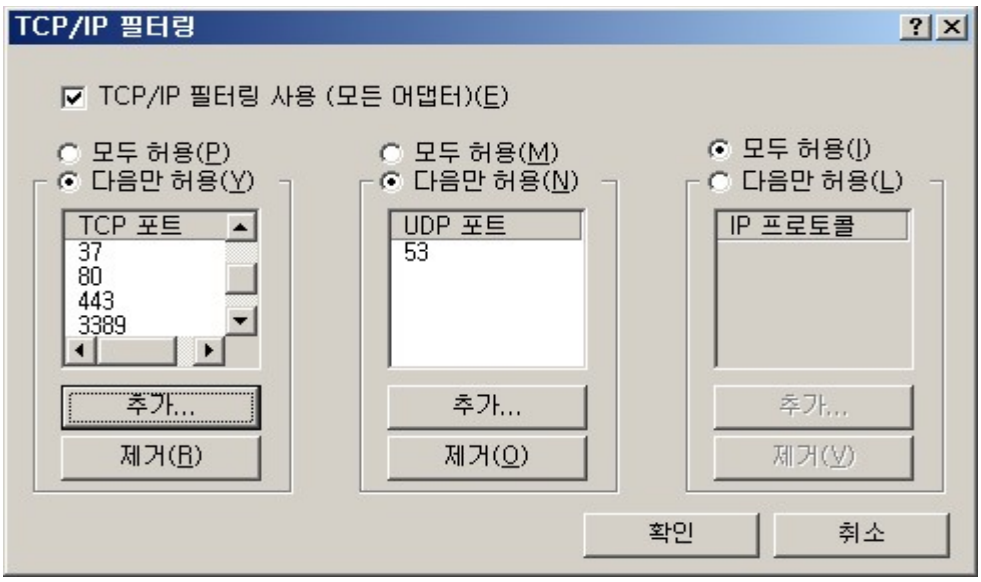
[9] 패킷 필터링

1. TCP/IP 필터링

TCP/IP Filtering은 InBound 되는 패킷만 제어가 가능하며, HTTP,FTP와 같은 특정 포트만을 오픈하여 서비스하는 시스템에 적합하다.

[내네트워크환경] -> [속성] -> [로컬영역연결] -> [속성] -> [일반]탭 -> [인터넷프로토콜(TCP/IP)] -> [속성] -> [고급] -> [옵션] -> [TCP/IP 필터링] -> [속성] -> TCP/IP 필터링 사용

C:₩WINDOWS₩system32₩drivers₩etc₩protocol
C:₩WINDOWS₩system32₩drivers₩etc₩services
위의 두 문서를 참조하여 해당 프로토콜에 대한 포트만을 허용하는 설정을 한다.
예 : TCP 포트 - 3389(터미널서비스), 80(HTTP), 21(FTP), 53(DNS-windows), 25(SMTP)
UDP 포트 - 53(DNS-unix)

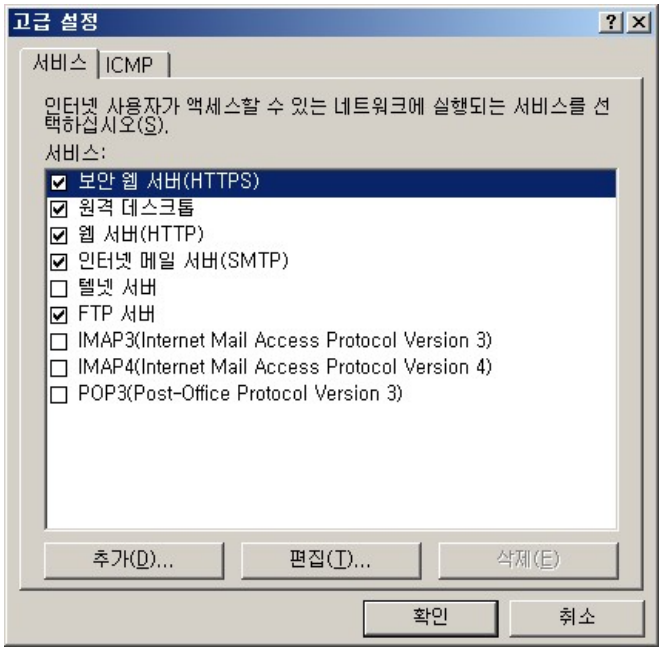


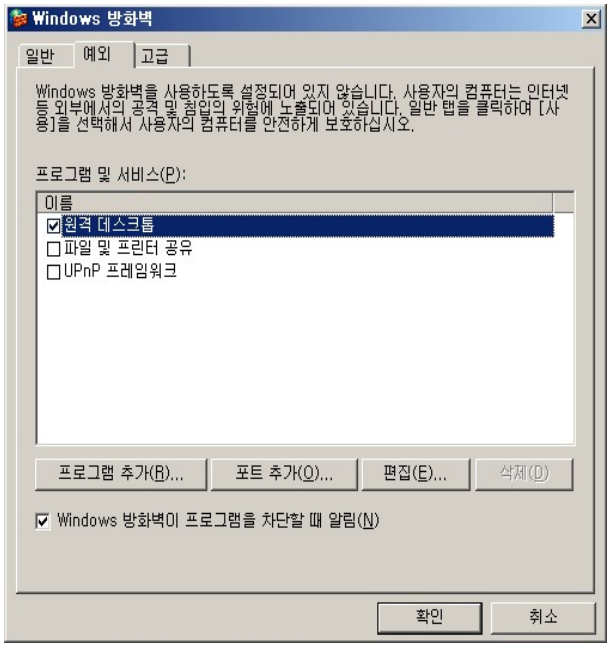
설정 변경후 적용하려면 시스템 리부팅이 필요하다.

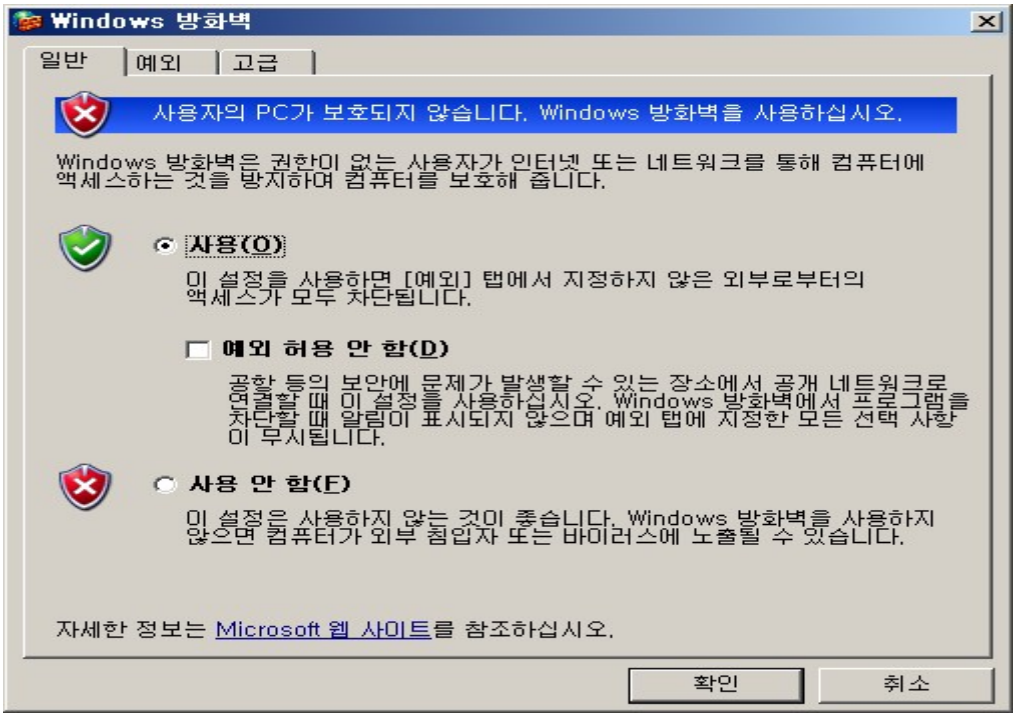
2. Windows 방화벽

Windows XP, 2003 에서 사용할 수 있는 자체 방화벽으로 외부로 나가는 트래픽은 필터링이 안되고 인바운드 트래픽만 필터링이 가능하다.
참고문서 : http://www.microsoft.com/korea/technet/prodtechnol/winxppro/Plan/icf.asp

[내네트워크환경] -> [속성] -> [로컬영역연결] -> [속성] -> [고급]탭 -> [설정] -> [고급]탭 -> [예외]탭 -> [일반]탭순으로 설정한다.
고급탭에는 서비스를 허용할 항목을 설정하는 네트워크연결설정부분과 보안로깅, ICMP, 기본값복원 설정으로 구성되어 있다. 고급탭의 네트워크연결설정에서 원격데스크톱, 웹서버, FTP서버 등의 서비스하려는 항목에 체크한다.
들어오는 패킷에 대한 기본정책이 차단하는 것이므로 원격에서 설정시 예외탭에 있는 원격데스크톱에 반드시 체크해 두는 것을 잊지 않도록 한다.



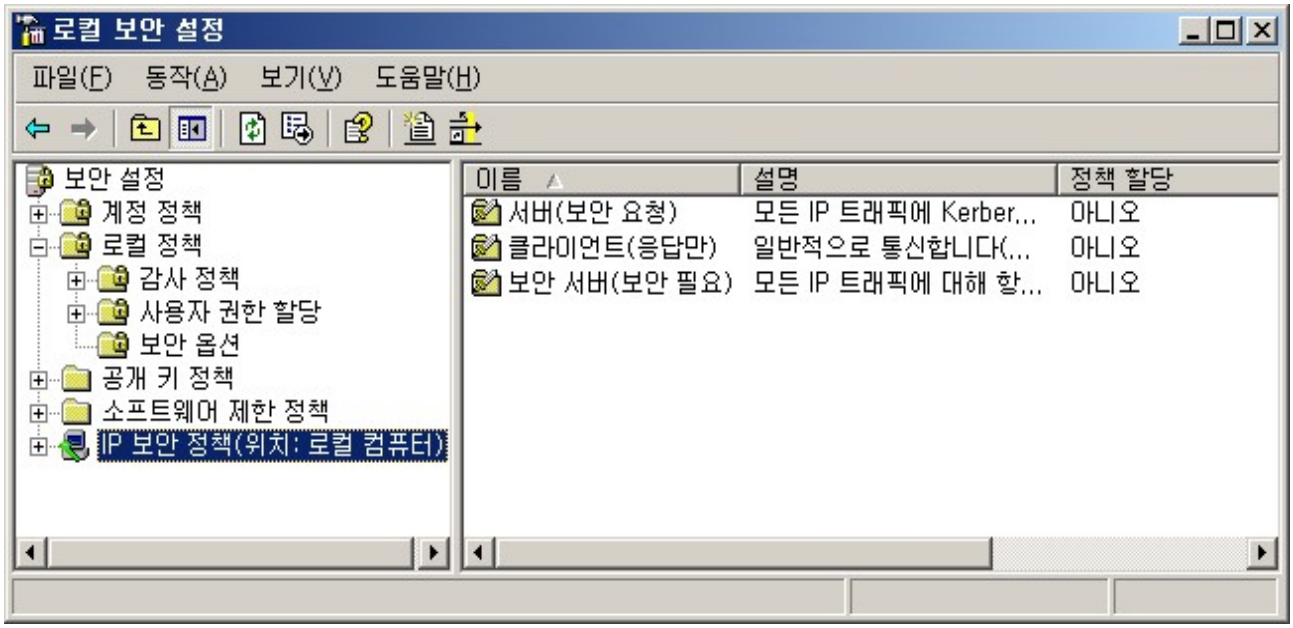




3. IPSEC

IPSEC(인터넷 프로토콜 보안)을 이용한 필터링은 InBound와 OutBound 되는 패킷 모두에 대해서 제어가 가능하므로, 서버관리자도 모르는 사이에 자신의 서버가 다른 서버를 공격하는데 이용되는 것을 방지할 수 있다.
액티브 디렉토리로 바꾼 사용자는 로컬 보안 정책(secpol.msc)및 도메인 보안정책(dompol.msc), 도메인 컨트롤러 보안정책 이 2가지가 추가로 생기게 되는데 특히 로컬 보안 정책보다 도메인 보안 정책이 우선 순위가 있어 액티브 디렉토리 사용자는 도메인 보안 정책에서 IPSec를 구성한다.

IPSEC 설정 : [시작] -> [제어판] -> [관리도구] -> [로컬보안설정] -> [IP 보안정책]



IPSEC 정책은 IP 필터, 필터의 동작, 이 필터들을 작동시킬 IP 보안정책 이 세가지로 요소로로 구성이 된다. 구성 순서는 관계가 없으나 IP 보안 정책부터 만들고 그 정책안에 필터을 만들고 필터의 동작을 정의 하는 방법이 효율성이 있다.

참고 : IIS Server IPSec Network Traffic Map

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
One point Client	ANY	ANY	ANY	ME	MOM Server	ALLOW	YES
Terminal Services	TCP	ANY	3389	ANY	ME	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller	ALLOW	YES
HTTP Server	TCP	ANY	80	ANY	ME	ALLOW	YES
HTTPS Server	TCP	ANY	443	ANY	ME	ALLOW	YES
All Inbound Traffic	ANY	ANY	ANY		ME	BLOCK	YES

예제 : 웹서버만을 운영하는 경우의 IPSEC 설정

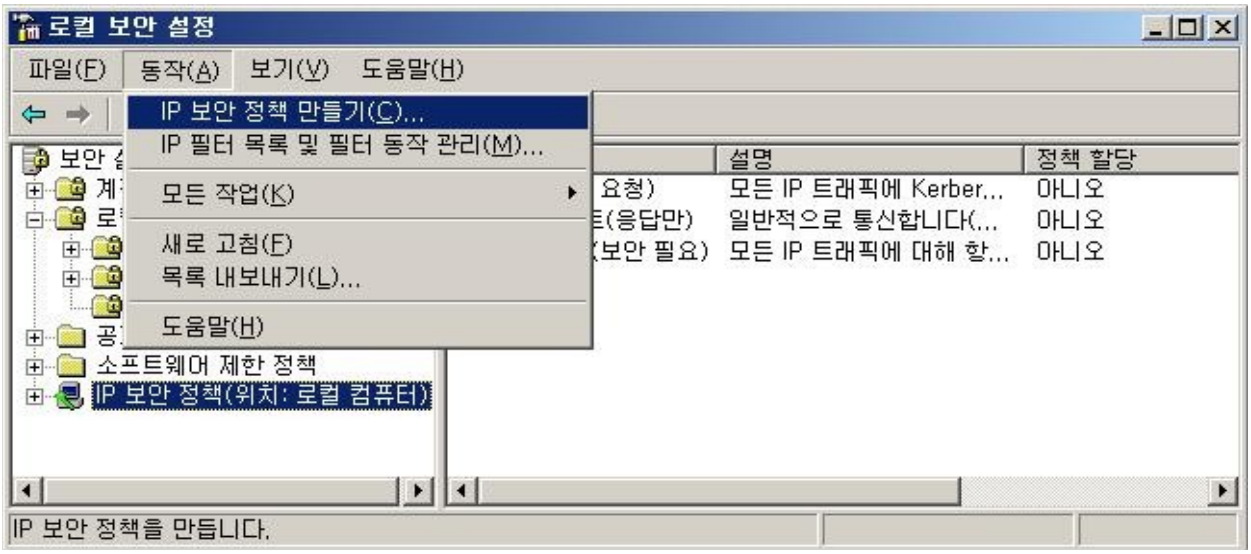
1. 웹서비스포트 80번은 어디에서나 접근 가능하게 한다.
2. 외부 DNS서버 UDP 53번 포트에 Client로서 접근 가능하게 한다.
3. 사무실 IP대역 (220.10.10.0/24)에서만 모든 접근 가능하게 한다.
4. 위의 1,2,3을 제외한 모든 접근을 차단한다.

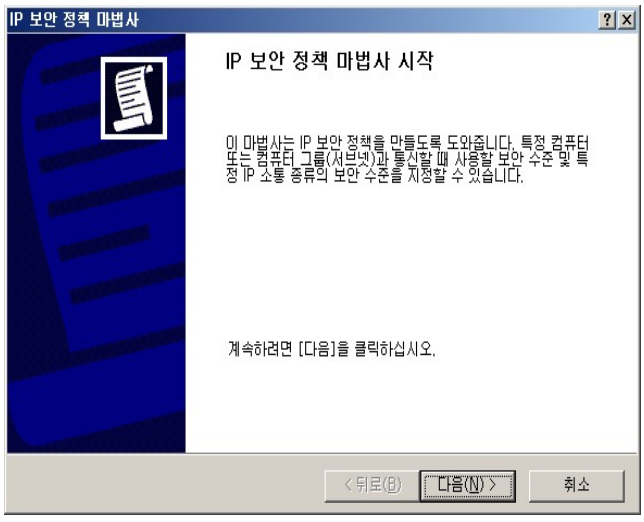
설정 순서는 각 항목에 대한 보안정책을 만들고, 적용할 IP 필터 목록을 작성한 다음, 해당 필터를 보안정책의 보안규칙에 등록한다.

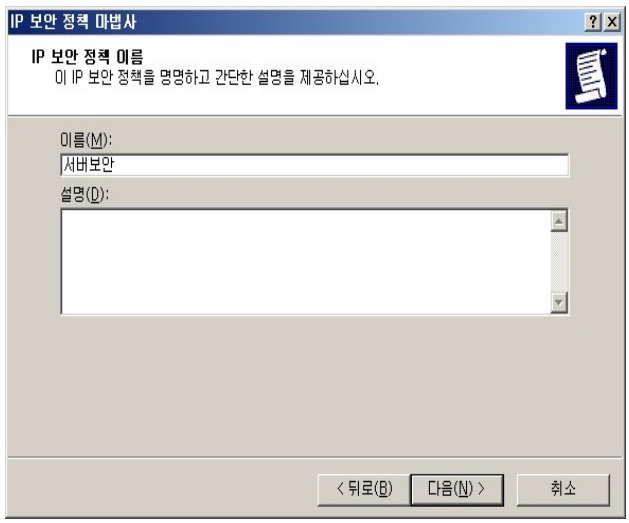
(1) IP 보안정책 만들기

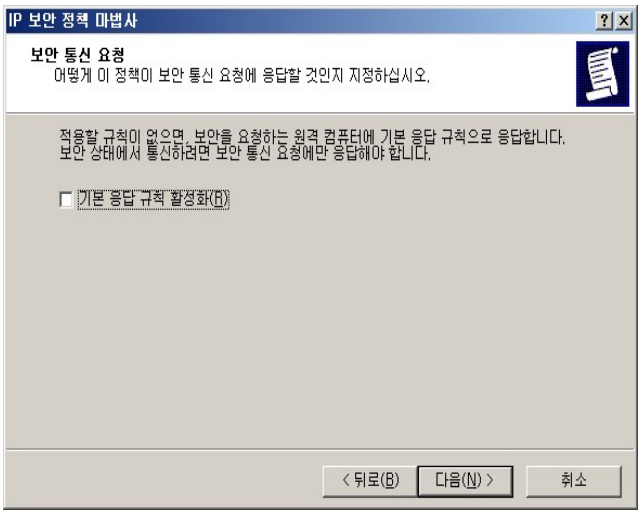
새 보안정책(이름:서버보안)을 만든다.

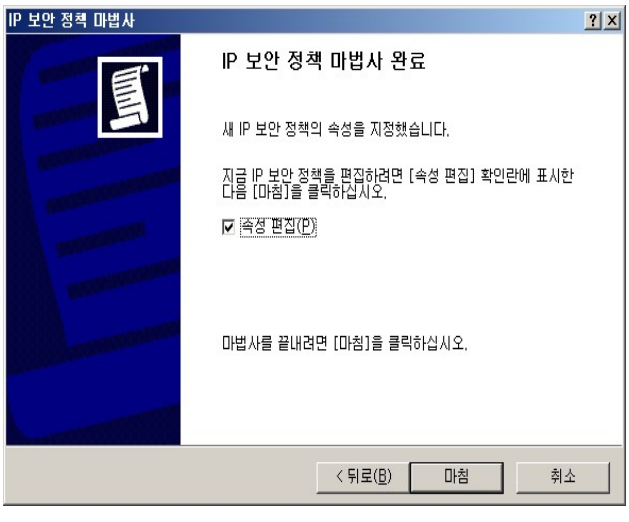
[동작] -> [IP 보안정책만들기] -> [IP 보안정책마법사시작] -> [다음] -> [IP 보안정책이름 : 서버보안] -> [다음] -> [기본응답규칙활성화] 체크 해제 -> [다음] -> [마침]





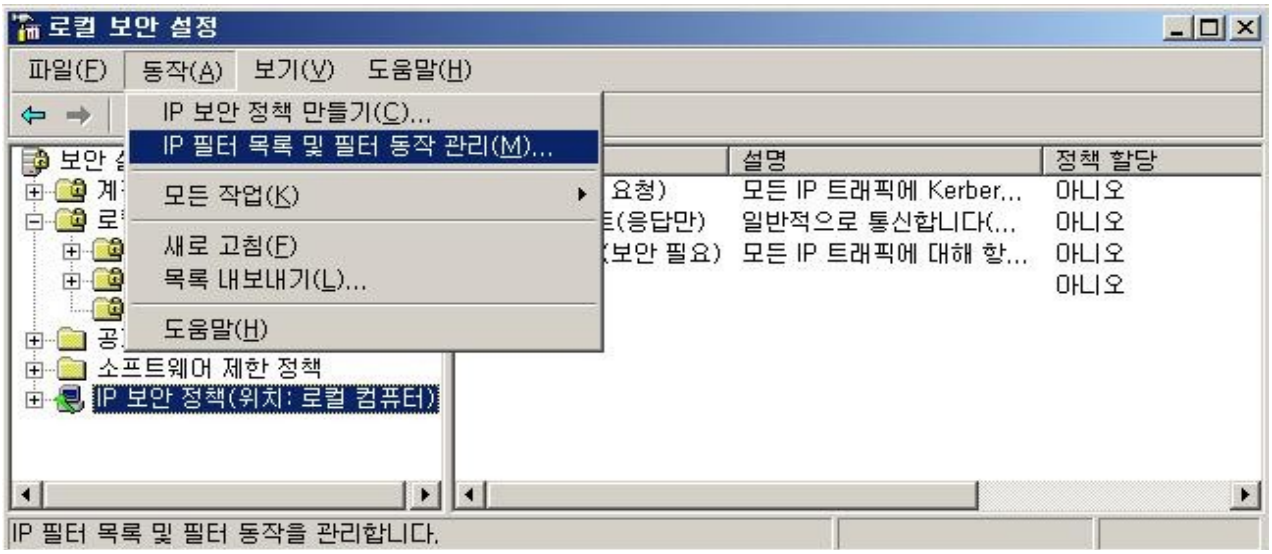


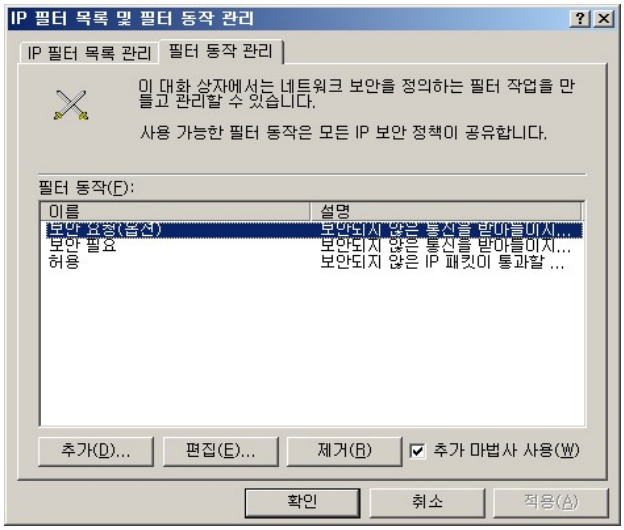


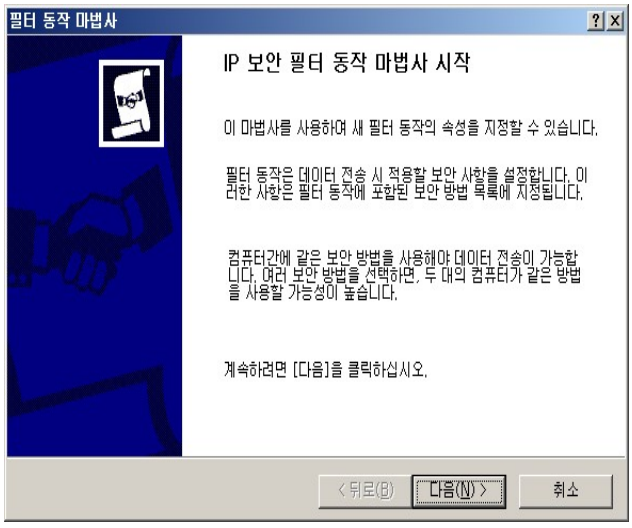


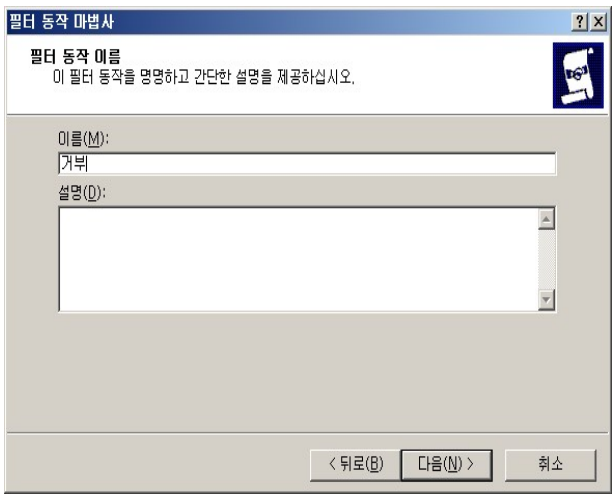
(2) 필터동작관리 중 거부 항목 추가하기

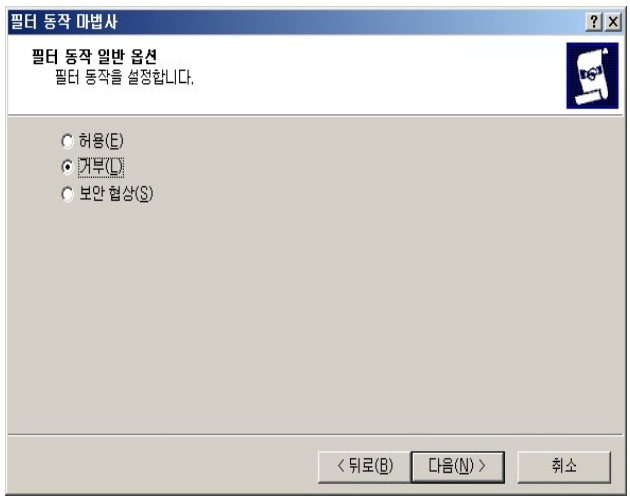
[동작] -> [Ip필터목록및필터동작관리창] -> [필터 동작 관리] -> [추가] -> [IP보안필터동작 마법사 시작] -> [다음] -> [필터동작이름] -> [거부] -> [다음] -> [필터동작일반옵션:거부] 선택 -> [다음] -> [마침]

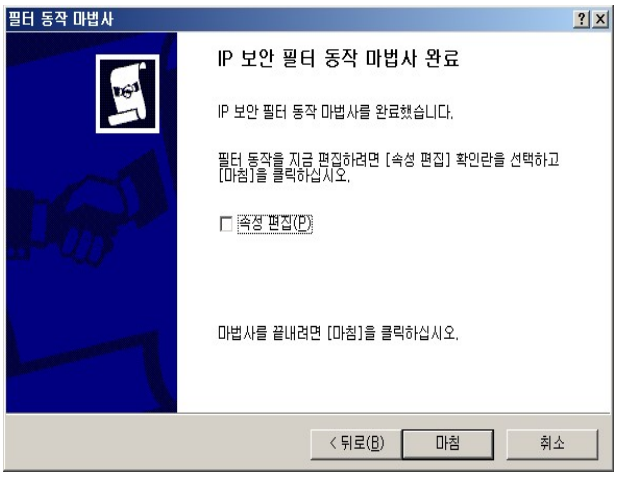


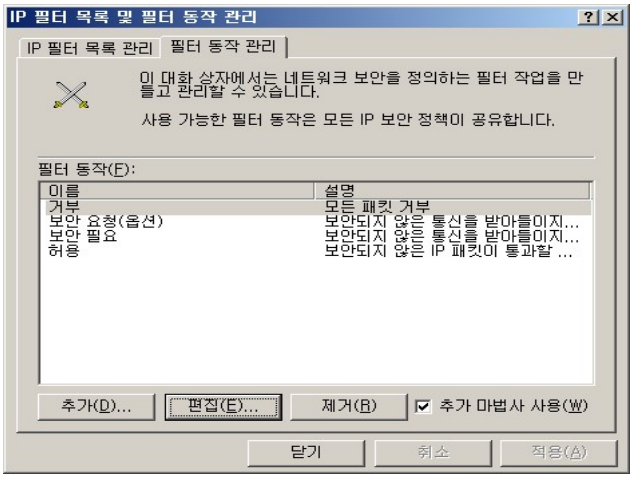








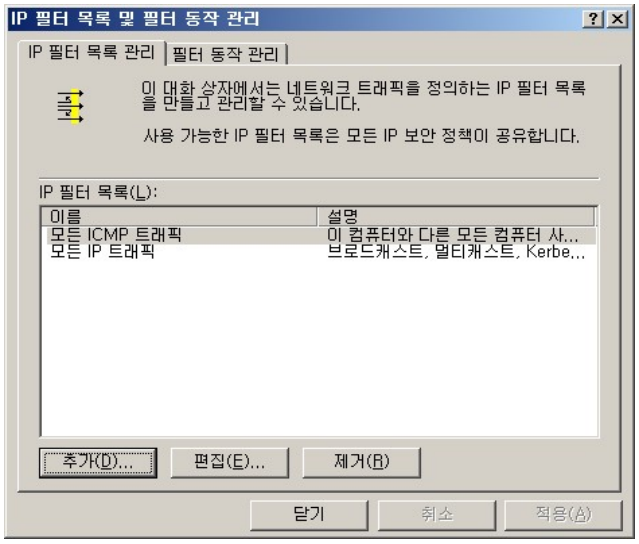


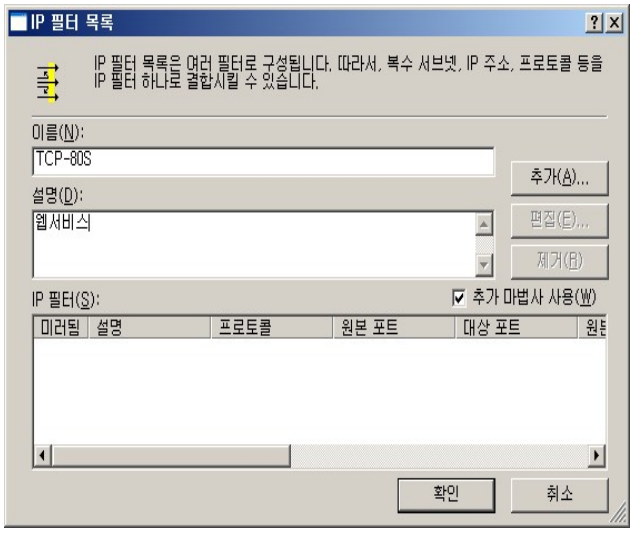


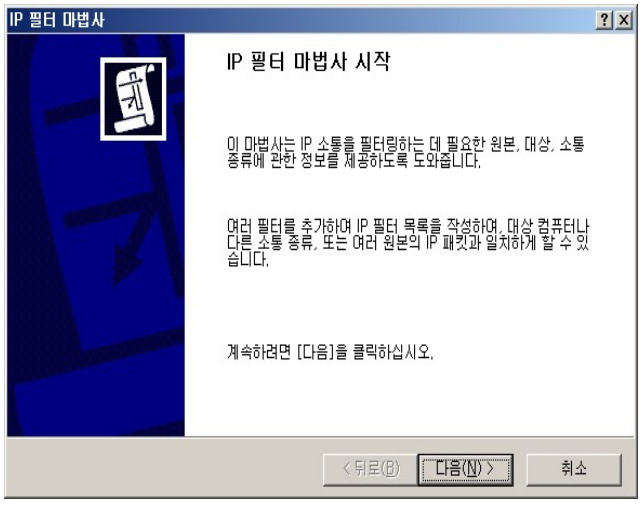
(3) IP 필터 목록 만들기

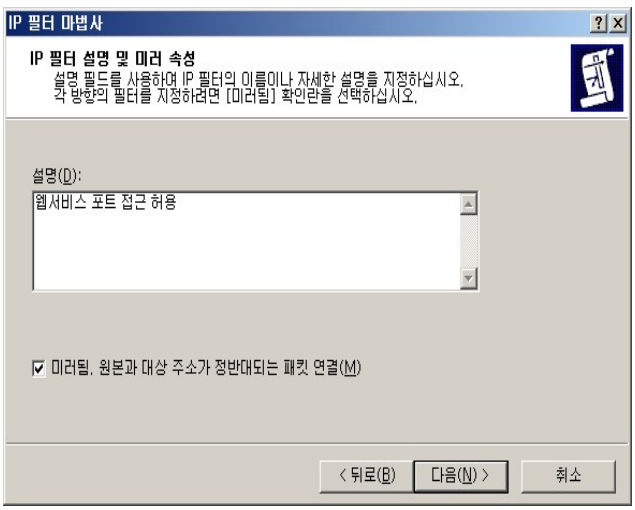
1) 웹서비스 : TCP-80S

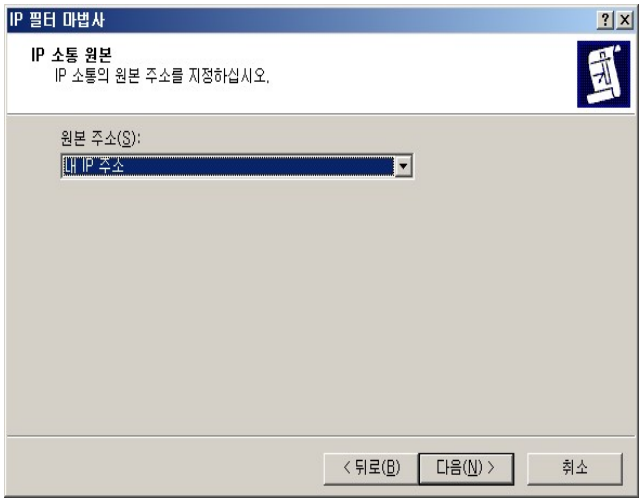
[IP 필터목록및필터동작관리창] -> [IP 필터목록관리]탭 -> [추가] -> [이름: TCP-80S] -> [추가] -> [IP 필터 마법사 시작] -> [다음] -> [설명 : 웹서버] -> [다음] -> [원본주소(목적지) : 내 IP 주소] -> [다음] -> [대상주소(송신자) : 모든 IP 주소] -> [다음] -> [프로토콜 종류선택 : TCP] -> [다음] -> [IP 프로토콜 포트 설정] -> [이 포트에서 : 80],[아무 포트로] -> [다음] -> [마침] -> [확인]

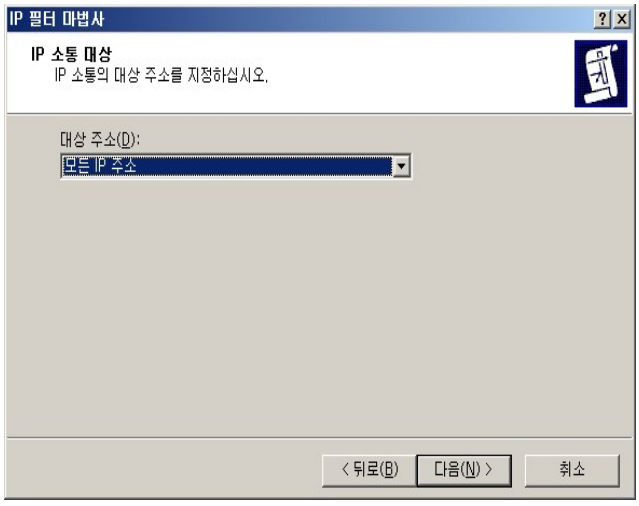


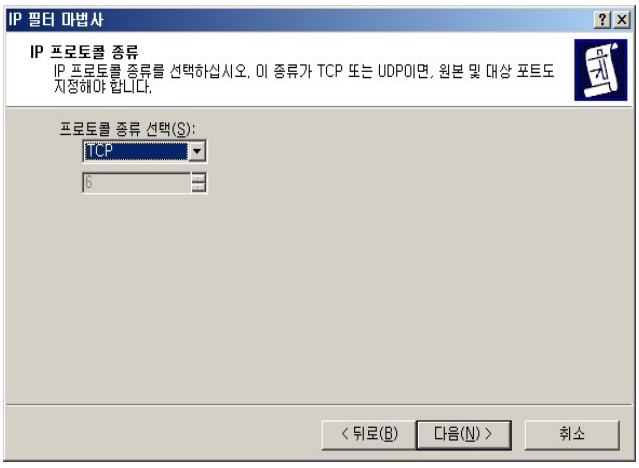


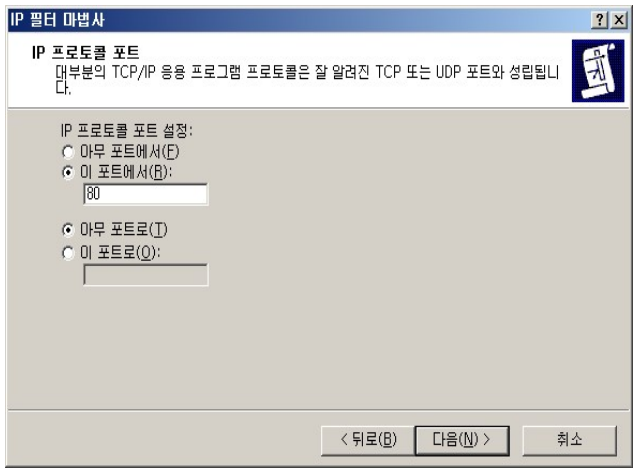


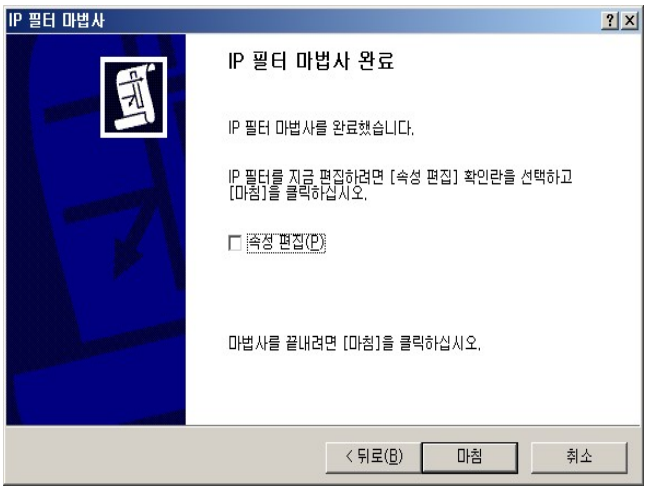










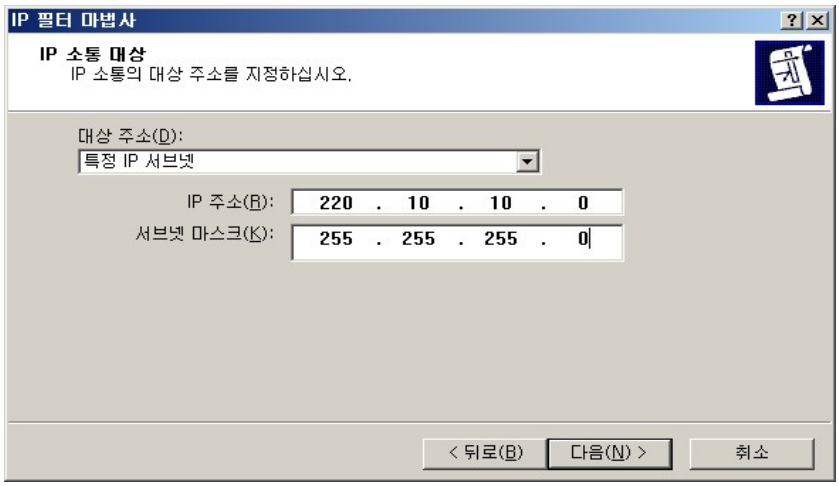


2) 외부의 리눅스 DNS 서버 : UDP-53C

-> [IP 필터 목록관리] -> [추가] -> [이름: UDP-53C] -> [추가] -> [IP 필터마법사 시작] -> [다음] -> [설명 : 외부 DNS서버 UDP 접근] -> [다음] ->[원본주소 : 내 IP 주소] -> [다음] -> [대상주소 : 모든 IP 주소] -> [다음] -> [프로토콜 종류선택 : UDP] -> [다음] -> [IP 프로토콜 포트 설정] -> [아무 포트에서],[이 포트로 : 53] -> [다음] -> [마침]-[확인]

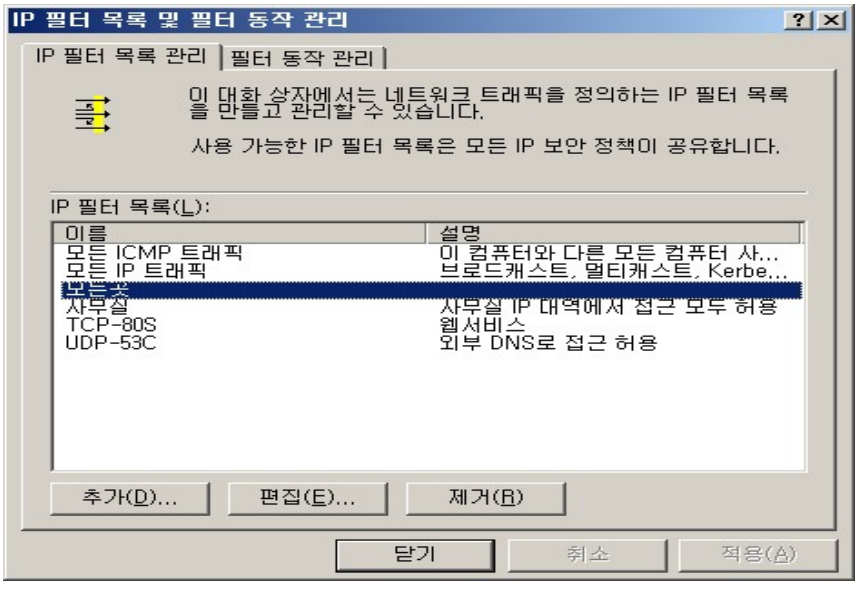
3) 사무실 IP 대역 : 사무실

-> [IP 필터 목록관리] -> [추가] -> [이름: 사무실] -> [추가] -> [IP 필터마법사 시작] -> [다음] -> [설명 : 사무실 IP 대역] -> [다음] -> [원본주소 : 내 IP 주소] -> [다음] -> [대상주소 : 특정 IP 서브넷] -> [IP 주소 :220.10.10.0 서브넷마스크:255.255.255.0] -> [다음] -> [프로토콜 종류선택 : 모두] -> [다음] -> [마침] -> [확인]



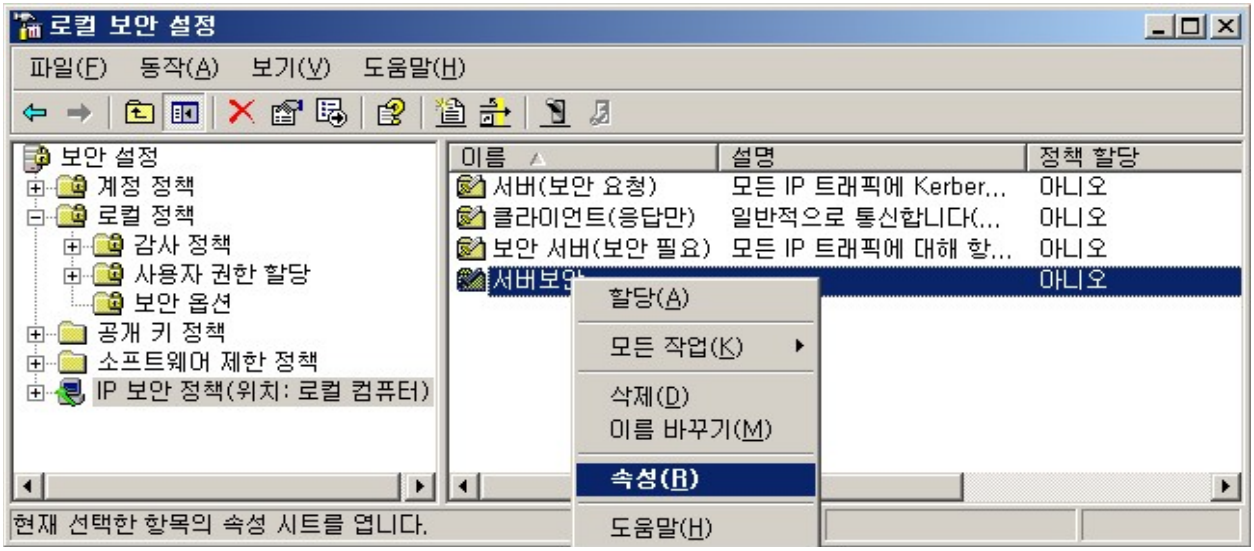
4) 모든 곳 : 모든곳

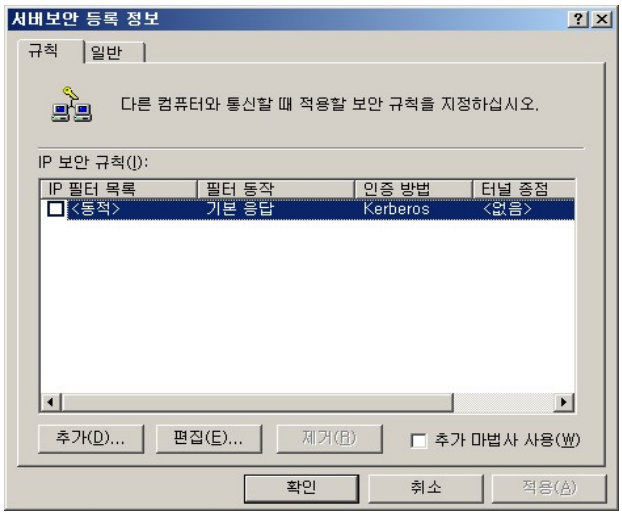
-> [IP 필터목록관리]탭 -> [추가] -> [이름: 모든곳] -> [추가] -> [IP 필터마법사 시작] -> [다음] -> [설명: 모든 곳] -> [다음] -> [원본주소 : 내 IP 주소] -> [다음] -> [대상주소 : 모든 IP 주소] -> [다음] -> [프로토콜 종류선택 : 모두] -> [다음] -> [마침] -> [확인] -> [닫기]

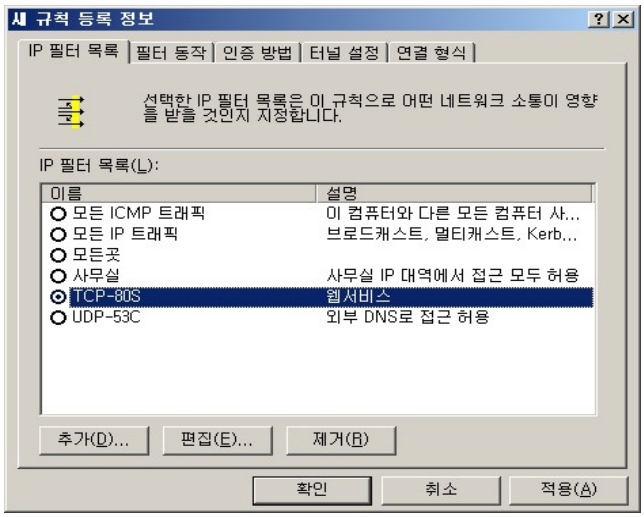


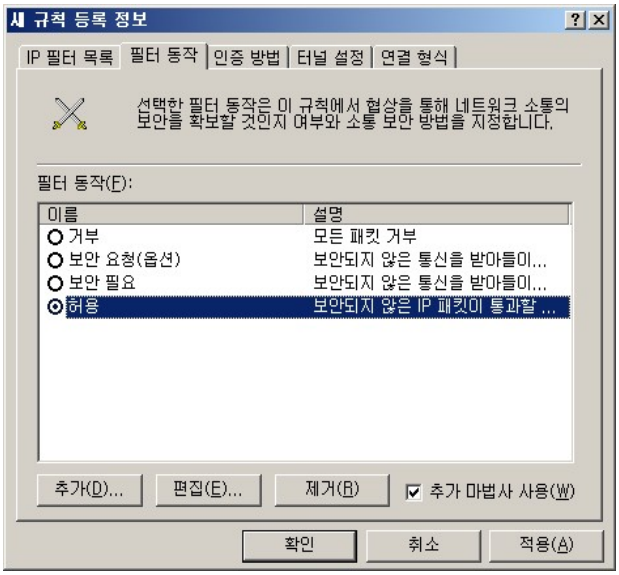
(4) 보안정책에 IP 보안 규칙 등록

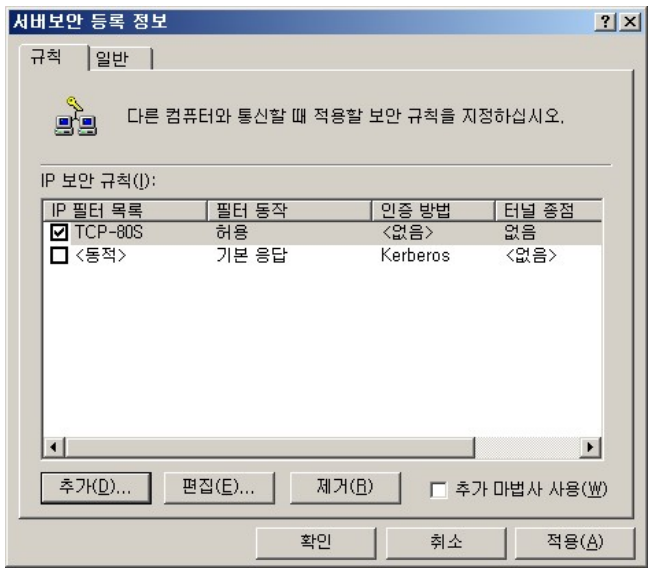
[서버보안 정책] -> [속성]
-> [IP 보안 규칙] -> [추가] -> [IP 필터목록]탭 -> [TCP-80S] 선택 -> [필터동작]탭 -> [허용] 선택 -> [확인]
-> [IP 보안 규칙] -> [추가] -> [IP 필터목록]탭 -> [UDP-53C] 선택 -> [필터동작]탭 -> [허용] 선택 -> [확인]
-> [IP 보안 규칙] -> [추가] -> [IP 필터목록]탭 -> [사무실] 선택 -> [필터동작]탭 -> [허용] 선택 -> [확인]
-> [IP 보안 규칙] -> [추가] -> [IP 필터목록]탭 -> [모든곳] 선택 -> [필터동작]탭 -> [거부] 선택 -> [확인]


로컬 보안 설정
파일(F) 동작(A) 보기(V) 도움말(H)
보안 설정
계정 정책
로컬 정책
감사 정책
사용자 권한 할당
보안 옵션
공개 키 정책
소프트웨어 제한 정책
IP 보안 정책(위치: 로컬 컴퓨터)
이름
설명
정책 할당
서버(보안 요청) 모든 IP 트래픽에 Kerber... 아니오
클라이언트(응답만) 일반적으로 통신합니다(... 아니오
보안 서버(보안 필요) 모든 IP 트래픽에 대해 항... 아니오
아니오
할당(A)
모든 작업(K)
삭제(D)
이름 바꾸기(M)
속성(R)
도움말(H)
현재 선택한 항목의 속성 시트를 엽니다.


서버보안 등록 정보
규칙 일반
다른 컴퓨터와 통신할 때 적용할 보안 규칙을 지정하십시오.
IP 보안 규칙(I):
IP 필터 목록 필터 동작 인증 방법 터널 종점
<동적> 기본 응답 Kerberos <없음>
추가(D)... 편집(E)... 제거(R) 추가 마법사 사용(W)
확인 취소 적용(A)

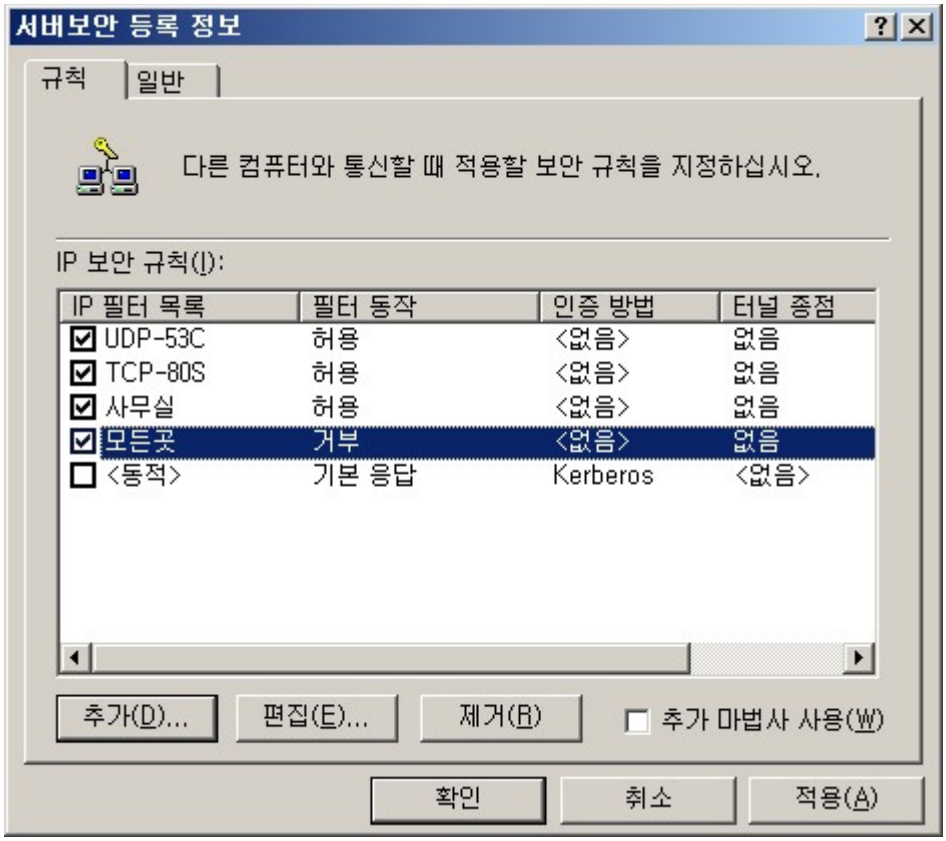

새 규칙 등록 정보
IP 필터 목록 필터 동작 인증 방법 터널 설정 연결 형식
선택한 IP 필터 목록은 이 규칙으로 어떤 네트워크 소통이 영향을 받을 것인지 지정합니다.
IP 필터 목록(L):
이름 설명
모든 ICMP 트래픽 이 컴퓨터와 다른 모든 컴퓨터 사...
모든 IP 트래픽 브로드캐스트, 멀티캐스트, Kerb...
모든곳
사무실 사무실 IP 대역에서 접근 모두 허용
TCP-80S 웹서비스
UDP-53C 외부 DNS로 접근 허용
추가(D)... 편집(E)... 제거(R)
확인 취소 적용(A)

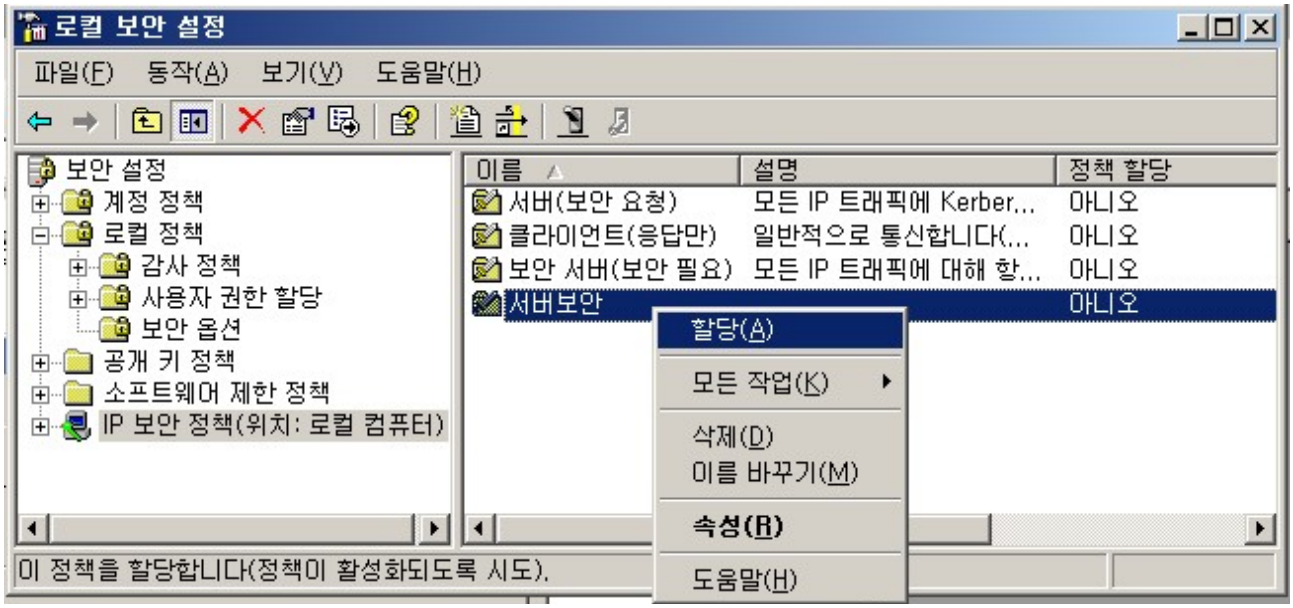

새 규칙 등록 정보
IP 필터 목록 필터 동작 인증 방법 터널 설정 연결 형식
선택한 필터 동작은 이 규칙에서 협상을 통해 네트워크 소통의 보안을 확보할 것인지 여부와 소통 보안 방법을 지정합니다.
필터 동작(F):
이름 설명
거부 모든 패킷 거부
보안 요청(옵션) 보안되지 않은 통신을 받아들이...
보안 필요 보안되지 않은 통신을 받아들이...
허용 보안되지 않은 IP 패킷이 통과할 ...
추가(D)... 편집(E)... 제거(R) 추가 마법사 사용(W)
확인 취소 적용(A)


서버보안 등록 정보
규칙 일반
다른 컴퓨터와 통신할 때 적용할 보안 규칙을 지정하십시오.
IP 보안 규칙(I):
IP 필터 목록 필터 동작 인증 방법 터널 종점
TCP-80S 허용 <없음> 없음
<동적> 기본 응답 Kerberos <없음>
추가(D)... 편집(E)... 제거(R) 추가 마법사 사용(W)
확인 취소 적용(A)

(5) 정책 적용

만들어진 정책을 적용하려면, 새로 만들어진 [서버보안] 정책항목에 마우스 오른쪽 버튼 클릭 -> [할당] 클릭
위의 설정 내용은 사무실에서만 FTP나 터미널서비스, PING 등의 접근이 허용되며, 웹서비스를 제외하고는 모든 곳에서 서버로의 접근이 거부된다. 또한, 서버내에서도 사무실로의 네트워킹을 제외하고는 외부로의 모든 접근이 차단된다. 예를 들어, 서버에서 웹브라우저로 윈도우 업데이트를 위해 microsoft.com에 접근하려면 위의 (3)-2) 항목처럼 클라이언트로 사용하기 위한 설정을 해야 한다.





추가 예제 : 서버에서 웹서핑을 하고자 한다.(외부 웹서버 80번 포트로의 접근 허용)

1) 필터 등록

[IP 필터목록및필터동작관리창] -> [IP 필터목록관리]탭 -> [IP 필터 목록] -> -> [추가] -> [이름 : 웹서핑] -> [추가] -> [IP 필터마법사 시작] -> [다음] -> [설명 : 서버에서 웹서핑] -> [다음] ->[원본주소 : 내 IP 주소] -> [다음] -> [대상주소 : 모든 IP 주소] -> [다음] -> [프로토콜 종류선택 : TCP] -> [다음] -> [IP 프로토콜 포트 설정] -> [아무 포트에서],[이 포트로 : 80] -> [다음] -> [마침] -> [확인] -> [닫기]

2) 정책에 필터 추가 등록

[서버보안 정책] -> [속성] -> [IP 보안 규칙] -> [추가] -> [IP 필터목록]탭 -> [서버에서웹서핑] 선택 -> [필터동작]탭 -> [허용] 선택 -> [확인] - [적용] -> [확인]

또 하나의 예제 : 특정한 IP (220.11.11.11) 에서만 서버의 터미널서비스 접속을 하고자 한다면?

1) 필터 등록

[IP 필터목록및필터동작관리창] -> [IP 필터목록관리]탭 -> [IP 필터 목록] -> [추가] -> [이름 : 우리집] -> [추가] -> [IP 필터마법사 시작] -> [다음] -> [설명 : 우리집 IP] -> [다음] ->[원본주소 : 내 IP 주소] -> [다음] -> [대상주소 : 특정 IP 주소 : 220.11.11.11] -> [다음] -> [프로토콜 종류선택 : TCP] -> [다음] -> [IP 프로토콜 포트 설정] -> [이 포트에서 : 3389],[아무 포트로] -> [다음] -> [마침] -> [확인] -> [닫기]

2) 정책에 필터 추가 등록

[서버보안 정책] -> [속성] -> [IP 보안 규칙] -> [추가] -> [IP 필터목록]탭 -> [서버에서웹서핑] 선택 -> [필터동작]탭 -> [허용] 선택 -> [확인] - [적용] -> [확인]

위의 3가지 필터링 방법중 IPSEC을 이용한 필터링을 적극 권장한다.

포트별 서비스 정리(윈도우 2000 기준)

<서비스명>	<포트>/<프로토콜>	[별칭]	[#<주석>]
echo	7/tcp		
echo	7/udp		
discard	9/tcp	sink null	
discard	9/udp	sink null	
systat	11/tcp	users	#Active users
systat	11/tcp	users	#Active users
daytime	13/tcp		
daytime	13/udp		
qotd	17/tcp	quote	#Quote of the day
qotd	17/udp	quote	#Quote of the day
chargen	19/tcp	ttytst source	#Character generator
chargen	19/udp	ttytst source	#Character generator
ftp-data	20/tcp	data	#FTP
ftp	21/tcp	control	#FTP

telnet	23/tcp		
smtp	25/tcp	mail	#Simple Mail Transfer Protocol
time	37/tcp	timserver	
time	37/udp	timserver	
rlp	39/udp	resource	#Resource Location Protocol
nameserver	42/tcp	name	#Host Name Server
nameserver	42/udp	name	#Host Name Server
nicname	43/tcp	whois	
domain	53/tcp		#Domain Name Server
domain	53/udp		#Domain Name Server
bootps	67/udp	dhcps	#Bootstrap Protocol Server
bootpc	68/udp	dhcpc	#Bootstrap Protocol Client
tftp	69/udp		#Trivial File Transfer
gopher	70/tcp		
finger	79/tcp		
http	80/tcp	www www-http	#World Wide Web
kerberos	88/tcp	krb5 kerberos-sec	#Kerberos
kerberos	88/udp	krb5 kerberos-sec	#Kerberos
hostname	101/tcp	hostnames	#NIC Host Name Server
iso-tsap	102/tcp		#ISO-TSAP Class 0
rtelnet	107/tcp		#Remote Telnet Service
pop2	109/tcp	postoffice	#Post Office Protocol - Version 2
pop3	110/tcp		#Post Office Protocol - Version 3
sunrpc	111/tcp	rpcbind portmap	#SUN Remote Procedure Call
sunrpc	111/udp	rpcbind portmap	#SUN Remote Procedure Call
auth	113/tcp	ident tap	#Identification Protocol
uucp-path	117/tcp		
nntp	119/tcp	usenet	#Network News Transfer Protocol
ntp	123/udp		#Network Time Protoco
epmap	135/tcp	loc-srv	#DCE endpoint resolution
epmap	135/udp	loc-srv	#DCE endpoint resolution
netbios-ns	137/tcp	nbname	#NETBIOS Name Service
netbios-ns	137/udp	nbname	#NETBIOS Name Service
netbios-dgm	138/udp	nbdatagram	#NETBIOS Datagram Service
netbios-ssn	139/tcp	nbsession	#NETBIOS Session Service
imap	143/tcp	imap4	#Internet Message Access Protocol
pcmail-srv	158/tcp		#PCMail Server
snmp	161/udp		#SNMP
snmptrap	162/udp	snmp-trap	#SNMP trap
print-srv	170/tcp		#Network PostScript
bgp	179/tcp		#Border Gateway Protocol
irc	194/tcp		#Internet Relay Chat Protocol
ipx	213/udp		#IPX over IP
ldap	389/tcp		#Lightweight Directory Access Protocol
https	443/tcp		MCom
https	443/udp		MCom
microsoft-ds	445/tcp		
microsoft-ds	445/udp		
kpasswd	464/tcp		# Kerberos (v5)
kpasswd	464/udp		# Kerberos (v5)

isakmp	500/udp	ike	#Internet Key Exchange
exec	512/tcp		#Remote Process Execution
biff	512/udp	comsat	
login	513/tcp		#Remote Login
who	513/udp	whod	shell
cmd	514/tcp		
syslog	514/udp		
printer	515/tcp		spooler
talk	517/udp		
ntalk	518/udp		
efs	520/tcp		#Extended File Name Server
router	520/udp	route routed	
timed	525/udp	timeserver	
tempo	526/tcp	newdate	
courier	530/tcp	rpc	
conference	531/tcp	chat	
netnews	532/tcp	readnews	
netwall	533/udp		#For emergency broadcasts
uucp	540/tcp	uucpd	
klogin	543/tcp		#Kerberos login
kshell	544/tcp	krcmd	#Kerberos remote shell
new-rwho	550/udp	new-who	
remotefs	556/tcp	rfs rfs_server	
rmonitor	560/udp	rmonitord	
monitor	561/udp		
ldaps	636/tcp	sldap	#LDAP over TLS/SSL
doom	666/tcp		#Doom Id Software
doom	666/udp		#Doom Id Software
kerberos-adm	749/tcp		#Kerberos administration
kerberos-adm	749/udp		#Kerberos administration
kerberos-iv	750/udp		#Kerberos version IV
kpop	1109/tcp		#Kerberos POP
phone	1167/udp		#Conference calling
ms-sql-s	1433/tcp		#Microsoft-SQL-Server
ms-sql-s	1433/udp		#Microsoft-SQL-Server
ms-sql-m	1434/tcp		#Microsoft-SQL-Monitor
ms-sql-m	1434/udp		#Microsoft-SQL-Monitor
wins	1512/tcp		#Microsoft Windows Internet Name Service
wins	1512/udp		#Microsoft Windows Internet Name Service
ingreslock	1524/tcp	ingres	
l2tp	1701/udp		#Layer Two Tunneling Protocol
pptp	1723/tcp		#Point-to-point tunnelling protocol
radius	1812/udp		#RADIUS authentication protocol
radacct	1813/udp		#RADIUS accounting protocol
nfsd	2049/udp	nfs	#NFS server
knetd	2053/tcp		#Kerberos de-multiplexor
man	9535/tcp		#Remote Man Server

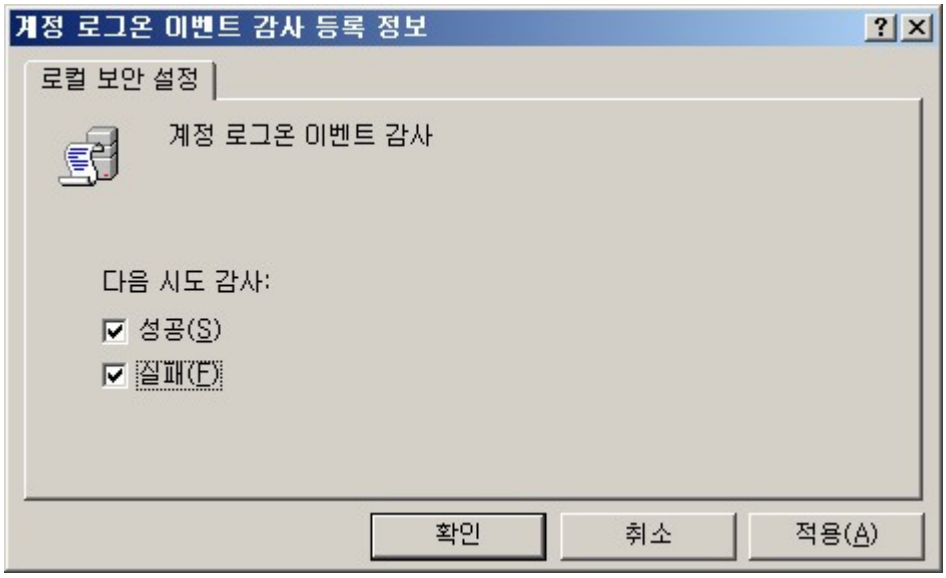
[10] 감사 관리

감사는 시스템 공격을 막지는 못하지만 진행중인 공격이나 침입자를 인식하고 공격의 흔적을 추적하는데 많은 도움을 준다. 웹 서버의 감사정책 수준을 높이고 NTFS 권한으로 로그 파일을 보호함으로써 공격자가 로그파일을 지우거나 변조하는 것을 방지하는 것도 필요하다.

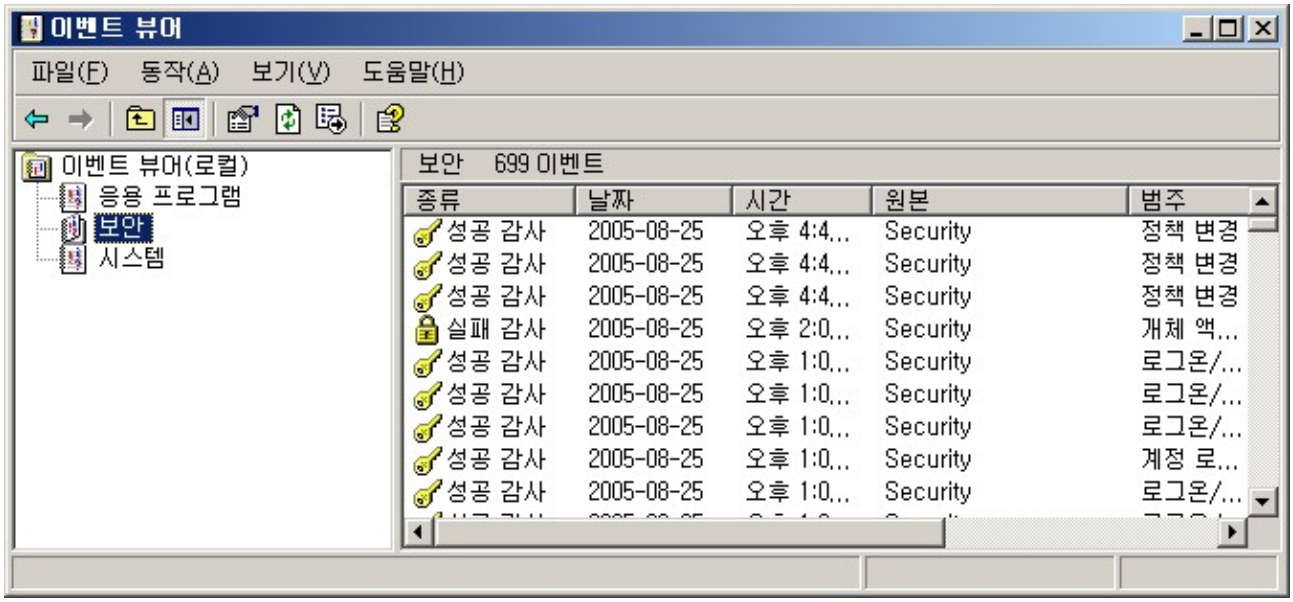
1. 로그인 실패 로그 기록

시스템에 로그인하는데 실패한 이벤트에 대해서는 반드시 로그를 기록해야 한다. 로그를 통해서 암호에 대한 무차별 대입 공격이나 사전 공격의 흔적을 찾을 수 있으며 공격자가 어떠한 계정으로 접근을 시도했는지도 알 수 있다.

[관리도구] -> [로컬 보안 설정] -> [로컬 정책] -> [감사 정책] -> [계정 로그온 이벤트 감사] -> [속성] -> [실패] 항목에 체크



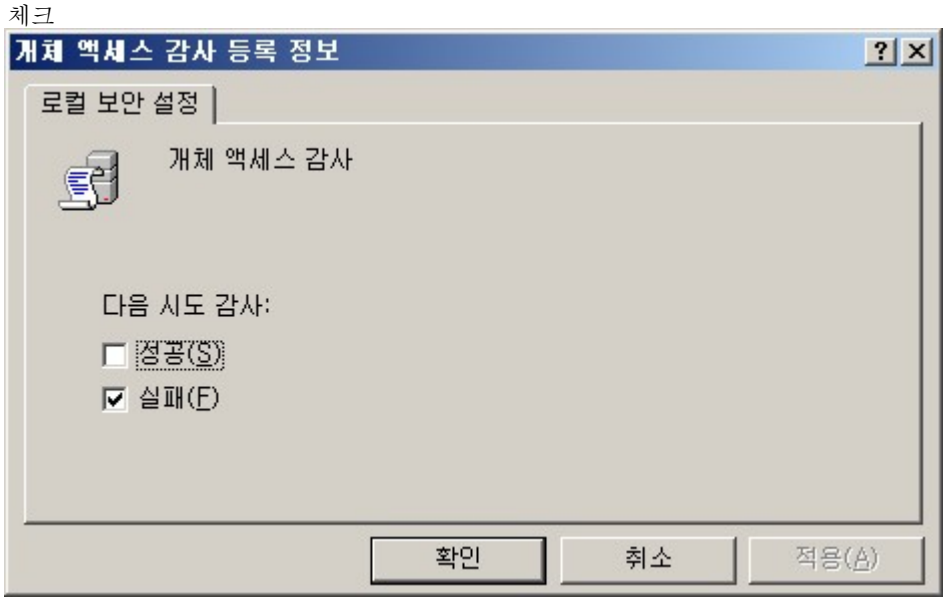
이후에 발생하는 로그인 실패 이벤트에 대한 내역을 [관리도구] -> [이벤트 뷰어] -> [보안] 로그 목록에서 확인한다.



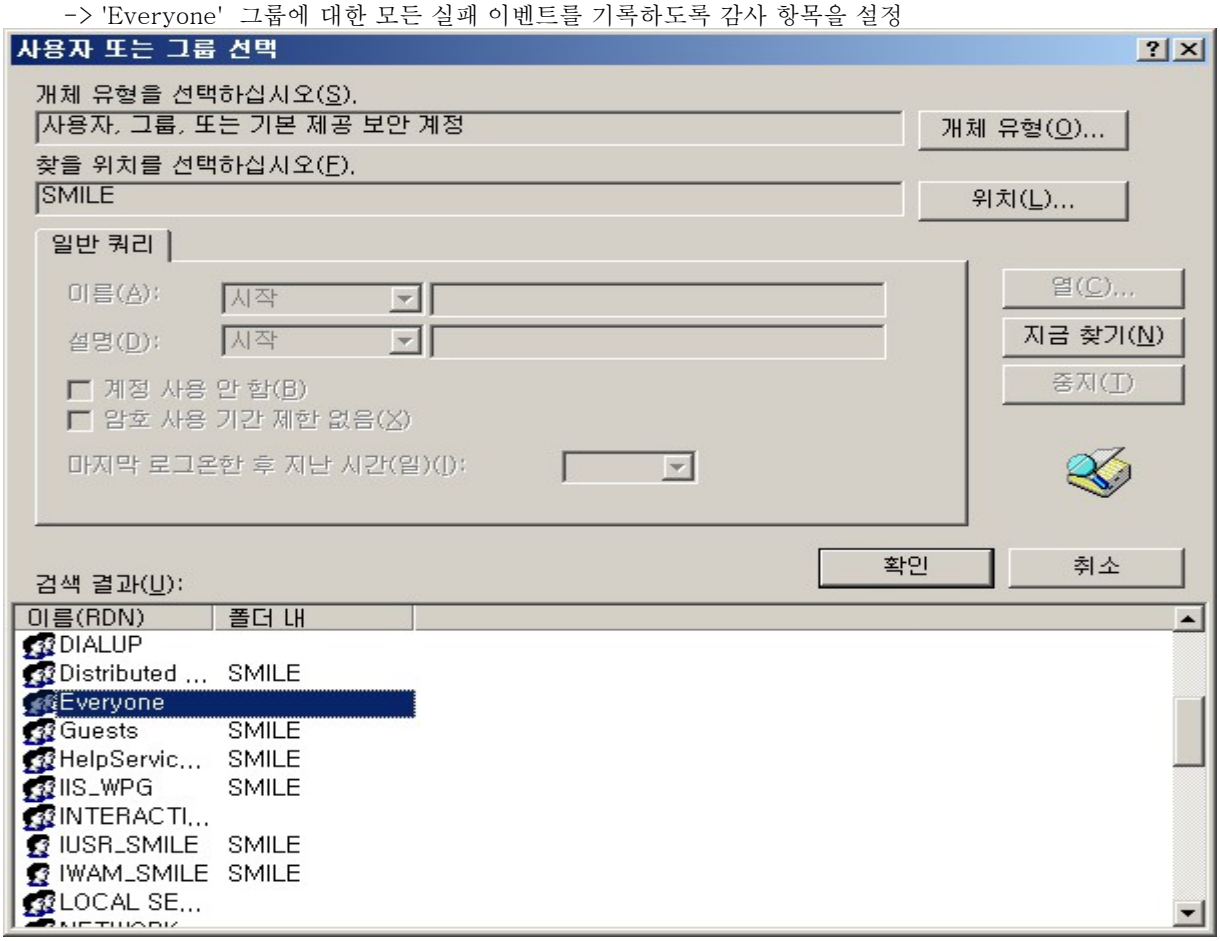
2. 개체 접근 실패 로그 기록

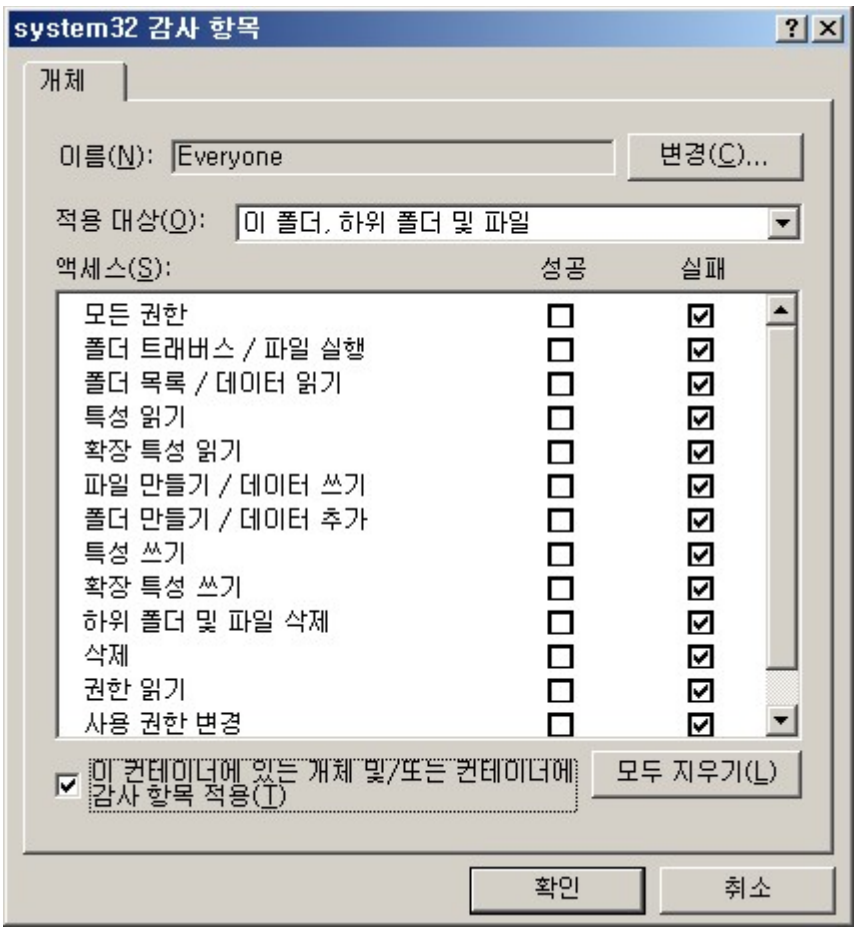
파일이나 폴더 등의 개체에 대한 악의적인 접근 시도에 대하여 감사기록을 한다. 개체 액세스에 대한 감사기능은 해당 디스크 볼륨이 NTFS 파티션일 경우에만 사용할 수 있다. NTFS 파일시스템은 FAT과 비교했을 때 파일 및 폴더 단위의 권한 부여 및 관리가 용이하므로 웹 서버의 자원이 저장되는 파티션은 NTFS를 사용하는 것이 좋다.

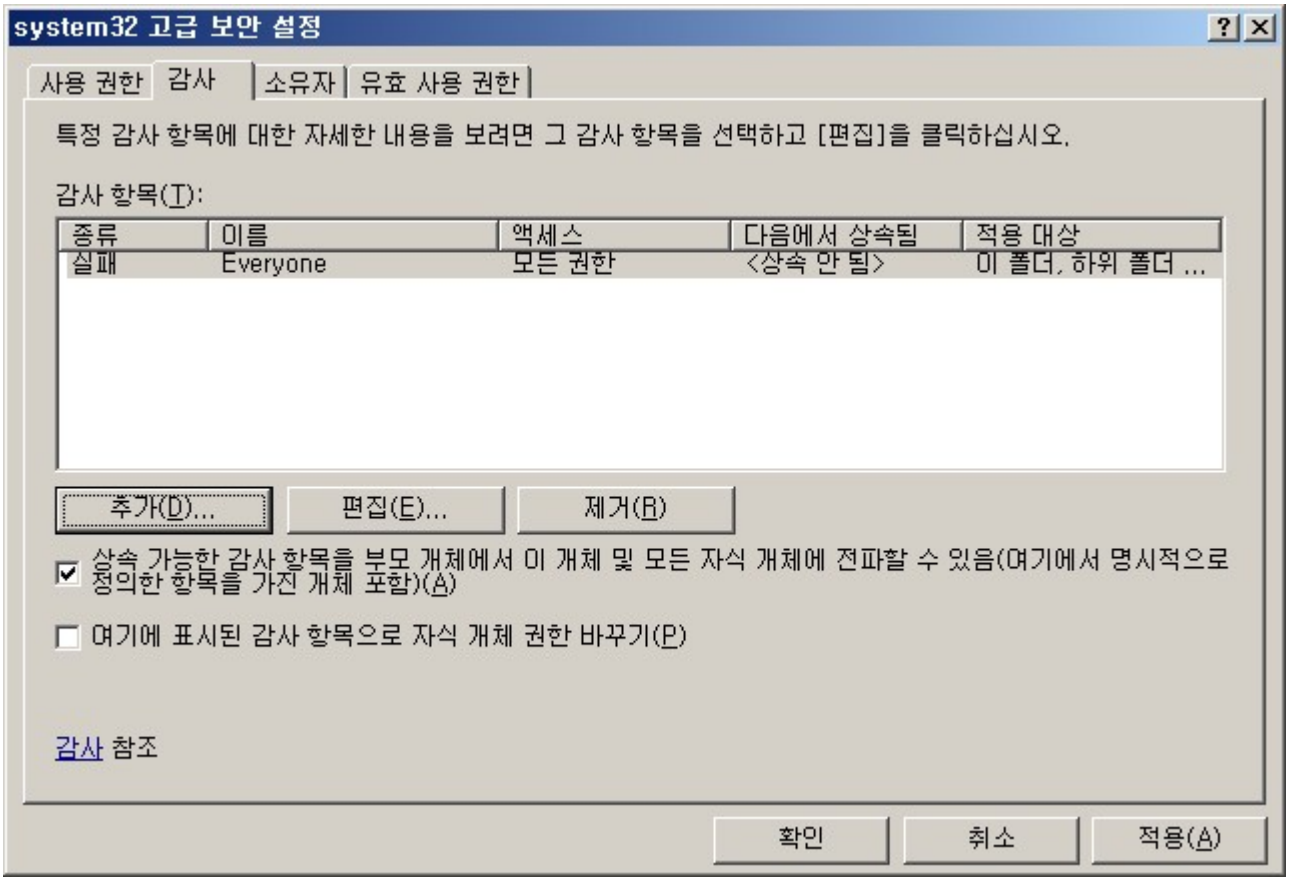
1) [관리도구] -> [로컬 보안 설정] -> [로컬 정책] -> [감사 정책] -> [개체 액세스 감사] -> [속성] -> [실패] 항목에 체크



2) 감사하려는 대상 폴더나 파일을 탐색기에서 선택 -> [속성] -> [보안]탭 -> [고급] -> [감사]탭 -> [추가] -> 'Everyone' 그룹에 대한 모든 실패 이벤트를 기록하도록 감사 항목을 설정




system32 감사 항목
개체
이름(N): Everyone
변경(C)...
적용 대상(O): 이 폴더, 하위 폴더 및 파일
액세스(S):
성공
실패
모든 권한
폴더 트래버스 / 파일 실행
폴더 목록 / 데이터 읽기
특성 읽기
확장 특성 읽기
파일 만들기 / 데이터 쓰기
폴더 만들기 / 데이터 추가
특성 쓰기
확장 특성 쓰기
하위 폴더 및 파일 삭제
삭제
권한 읽기
사용 권한 변경
이 컨테이너에 있는 개체 및/또는 컨테이너에 감사 항목 적용(T)
모두 지우기(L)
확인
취소


system32 고급 보안 설정
사용 권한
감사
소유자
유효 사용 권한
특정 감사 항목에 대한 자세한 내용을 보려면 그 감사 항목을 선택하고 [편집]을 클릭하십시오.
감사 항목(T):
종류
이름
액세스
다음에서 상속됨
적용 대상
실패
Everyone
모든 권한
<상속 안 됨>
이 폴더, 하위 폴더 ...
추가(D)...
편집(E)...
제거(R)
상속 가능한 감사 항목을 부모 개체에서 이 개체 및 모든 자식 개체에 전파할 수 있음(여기에서 명시적으로 정의한 항목을 가진 개체 포함)(A)
여기에 표시된 감사 항목으로 자식 개체 권한 바꾸기(P)
감사 참조
확인
취소
적용(A)

3. IIS 로그파일 위치 변경 및 NTFS 권한 적용

기본적으로 IIS 로그파일은 '%systemroot%₩system32₩LogFiles'에 사이트별로 저장되는데 이를 다른 폴더에 저장하거나 이름을 변경함으로써 공격자가 로그 파일을 변경하거나 삭제하는 것을 어느 정도 막을 수 있다. 가능하면 이 로그 파일이 저장되는 디렉토리를 웹 사이트가 위치한 디스크와 다른 볼륨을 사용하고 NTFS 권한을 Administrator(모든 권한), System(모든 권한)로 지정하여 다른 계정에서 로그 파일에 접근하는 것을 막는 것이 좋다.

[인터넷정보서비스관리] -> 각 웹사이트 -> [속성] -> [웹사이트]탭 -> 로깅사용 [속성] -> 로그파일디렉토리 변경

[11] IIS 보안

1. IIS 버전 비교

구분	IIS 5.0	IIS 6.0
Platform	Windows 2000	Windows Server 2003
Architecture	32 bit	32bit and 64bit
Metabase configuration	Binary	XML
Security	Windows 인증, SSL, Kerberos	Windows 인증, SSL, Kerberos Security wizard, Passport support
원격관리	HTMLA, Terminal Services	HTMLA, Remote Desktop
Cluster support	IIS clustering	Windows support
메일지원	SMTP	SMTP & POP3
IPv6 지원	IPv4	IPv4 and IPv6

IIS 6.0 설치시 기본구성 요소인 WWW 서비스만 설치되므로, ASP,SMTP,FTP 등은 추가 선택하여 설치하여야 한다.

2. 기본 구성 요소

항목	설명
서비스	웹과 FTP 관리를 위한 IIS 관리 서비스 World Wide Web 서버 서비스 FTP 서비스 메일발송을 위한 SMTP 서비스 뉴스그룹을 위한 NNTP 서비스
계정 및 그룹	IUSR_MACHINENAME(인터넷 게스트 계정) IWAM_MACHINENAME(IIS 프로세스 시작 계정) ASPNET(ASP.NET 컴퓨터 계정) IIS_WPG(IIS 작업자 프로세스 그룹)
폴더	Windir₩system32₩inetserv (IIS 프로그램) Windir₩system32₩inetserv₩iisadmin (IIS 관리 프로그램) Windir₩help₩iishelp (IIS 도움말 파일) Systemdrive₩inetpub (웹,FTP,SMTP 루트 폴더)
웹사이트	기본웹사이트(80번 포트) : Systemdrive₩inetpub₩wwwroot 관리웹사이트(3693번 포트) : Windir₩system32₩inetserv₩iisadmin

3. IIS 보안 점검 항목

1) 가상 디렉토리에 대한 적절한 ACL 설정
2) IIS 로그 파일에 대한 ACL 설정
3) 로깅 사용
4) 사용하지 않는 예제 프로그램 삭제
5) 가상 디렉토리 삭제
6) 사용하지 않는 스크립트 매핑 삭제

4. 불필요한 폴더 제거

1) IIS 예제 : iissamples
2) IIS 설명서 : iishelp
3) 데이터 엑세스 : MSDAC

5. 파일권한

CGI (.exe , .dll , .cmd , .pl), 스크립트파일 (.asp , .aspx), Include 파일 (.inc , .shm , .shtml) 등의 파일에는 Everyone에게 권한을 주지 않는다.
일반 파일 (.txt , .gif , .jpg , .html) 에는 Everyone 에게 읽기 권한을 부여한다.
파일 종류에 따른 파일권한을 설정할 수 있도록 각각 종류에 디렉토리를 생성하여 관리한다.

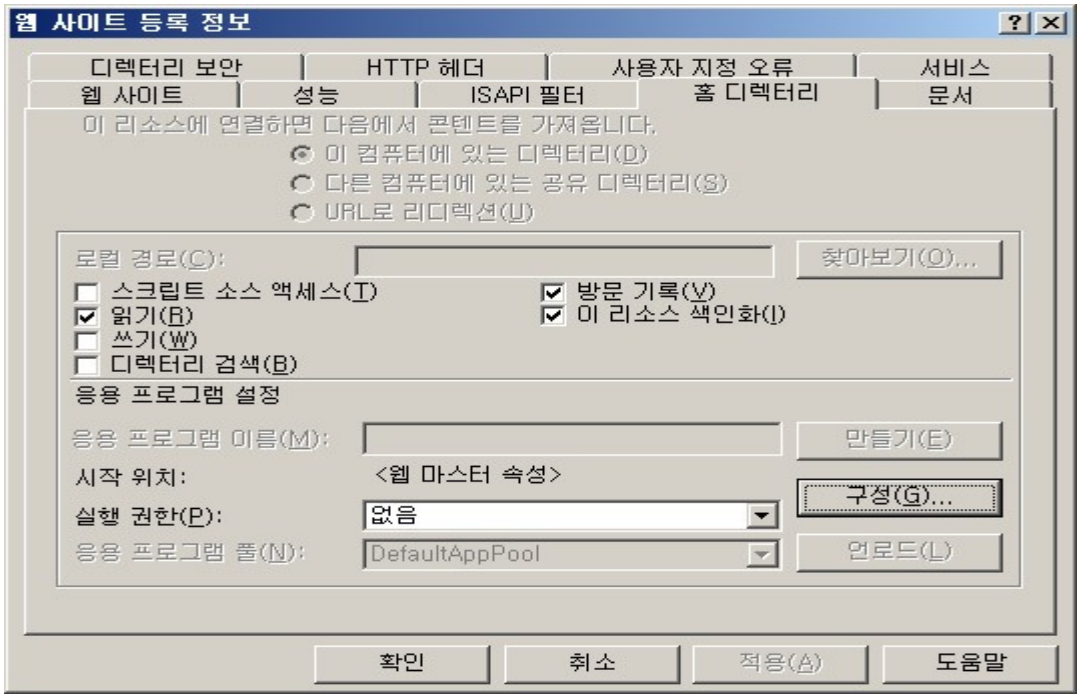
6. 불필요한 매핑 제거

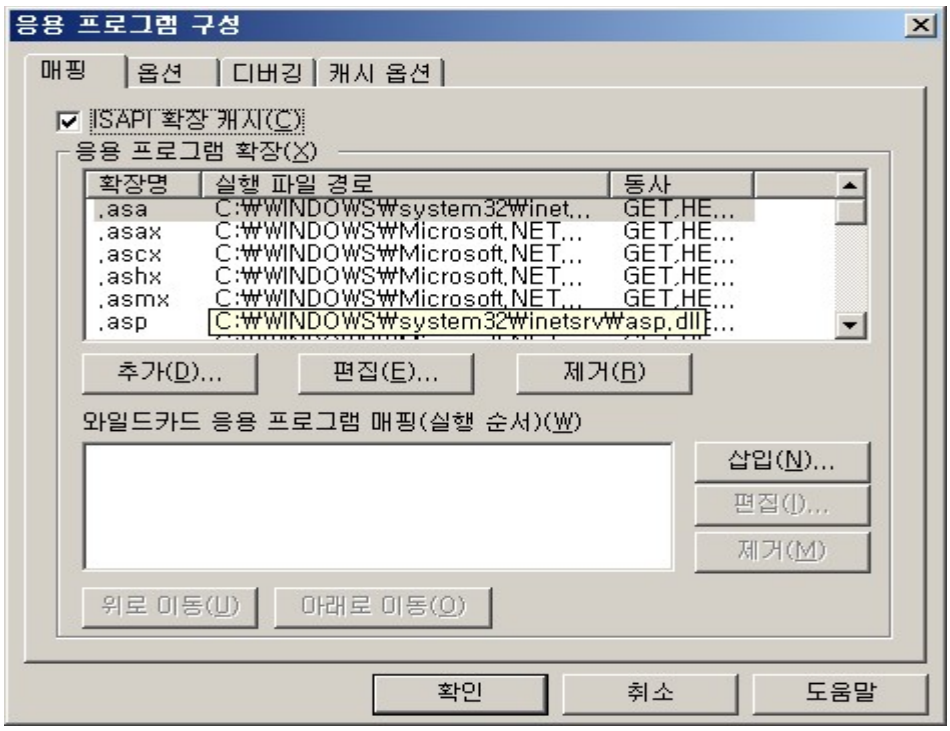
전체 웹사이트에 적용시 : [인터넷정보서비스관리[-> [웹사이트] -> [속성] -> [홈디렉토리]탭 -> [구성] -> [매핑]탭
개별 적용시에는 각 사이트의 매핑탭에서 설정한다.

매핑탭을 보면 많은 수의 파일매핑이 되어 있는데 실제로 웹서버에서 사용하는 .asp , .asa를 제외하고는 모두 제거하는 것이 좋다. 적용 대상서버가 웹서버가 아닌 파일 서버 및 DB 전용의 서버라면 모든 매핑파일 자체가 필요가 없다.

* 제거 권고 매핑

1) 웹기반 암호 재설정 : .htr
2) IIS 커넥터 : .idc
3) Server Side Includes : .stm, .shtm, .shtml
4) 인쇄 : .printer
5) 인덱스 서버 : .htw, .ida, .idq

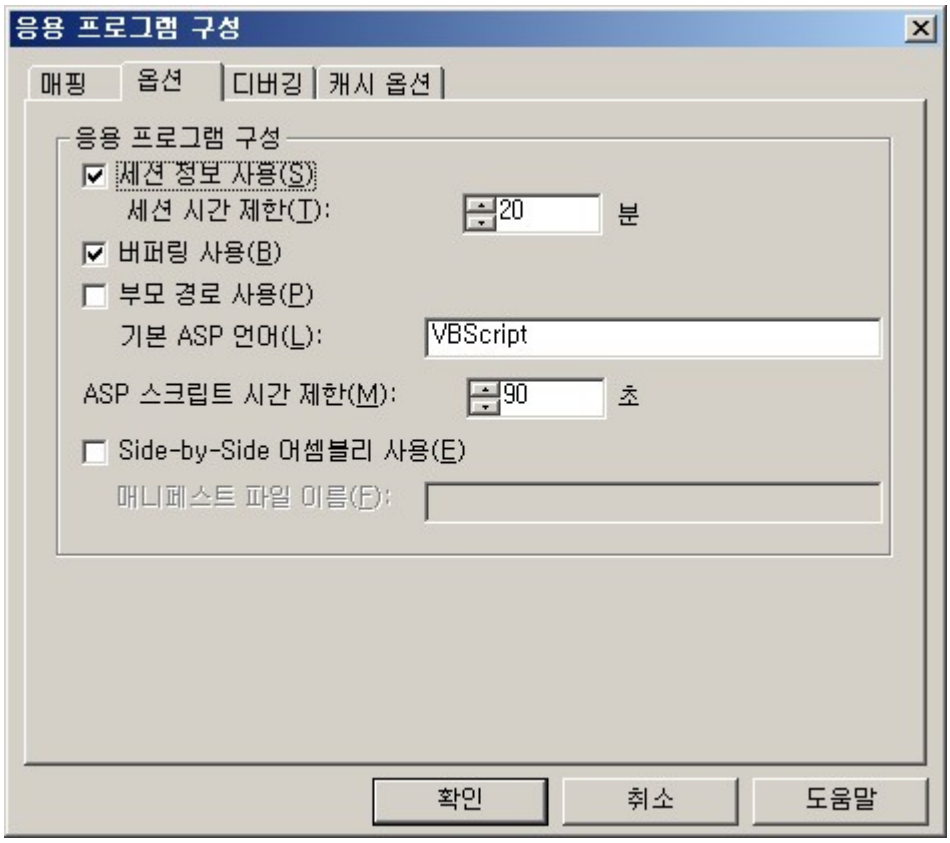




7. 상위 경로 접근 제거

시스템 파일 및 명령어를 삽입하기 위해 ../../../ 등의 패턴 입력을 제한한다.

[인터넷정보서비스관리] -> [웹사이트] -> [속성] -> [홈디렉토리탭] -> [구성] -> [옵션]탭 -> [부모경로사용] 체크 해제



8. 컨텐츠 디렉토리 권한

[인터넷정보서비스관리] -> [웹사이트] -> [속성] -> [홈디렉토리]탭 -> 읽기, 방문기록,이리소스색인화 외에는 체크하지 않는다. 즉, 읽기 정도의 권한만 할당

9. #exec 명령쉘 호출 중지

명령어가 웹서버에서 임의의 명령을 호출하도록 사용될 수도 있다. IIS는 디폴트로 이것이 중지되어 있으며 이를 가능하게 하는 레지스트리 키가 '0'로 셋팅되어 있는지 확인한다.

HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩W3SVC₩Parameters₩SSIEnableCmdDirective

10. WebDAV 비활성화

WebDAV(Web Distributed and Versioning)는 웹서버 상에 존재하는 파일들을 공동으로 편집·관리하기 위한 도구로서 HTTP와 같은 웹 운영프로토콜의 확장된 형태이며, 버퍼오버플로우 취약점이 있다.
또한, Windows 2000 서버에서 IIS 설치시 기본으로 설치되며, 설치후 계속 사용가능하도록 설정되어 있고,
WebDAV 라이브러리 파일의 속성 및 홈페이지 디렉토리에 쓰기 권한이 모두 허용되어 있는 경우에 해커가 WebDAV 도구를 사용하여 원격에서 홈페이지 디렉토리에 임의의 파일을 삽입하여 웹페이지를 변조할 수 있다.

조치방법 :
WebDAV 기능중지 : 시작메뉴 -> 실행 클릭 -> regedit 입력후 확인 -> 레지스트리편집기 창에서
HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩W3SVC₩Parameters로 이동
-> 디렉토리안에서 마우스 오른쪽 버튼 클릭 -> 새로만들기 -> DWORD 값(D) -> 새 값#1 을
DisableWebDAV 로 변경 -> DisableWebDAV 선택후 마우스 오른쪽버튼 클릭 -> 수정(M) ->
값 데이터(V) 항목에 1 입력 -> 확인 -> IIS를 재시작 또는 윈도우 시스템 리부팅

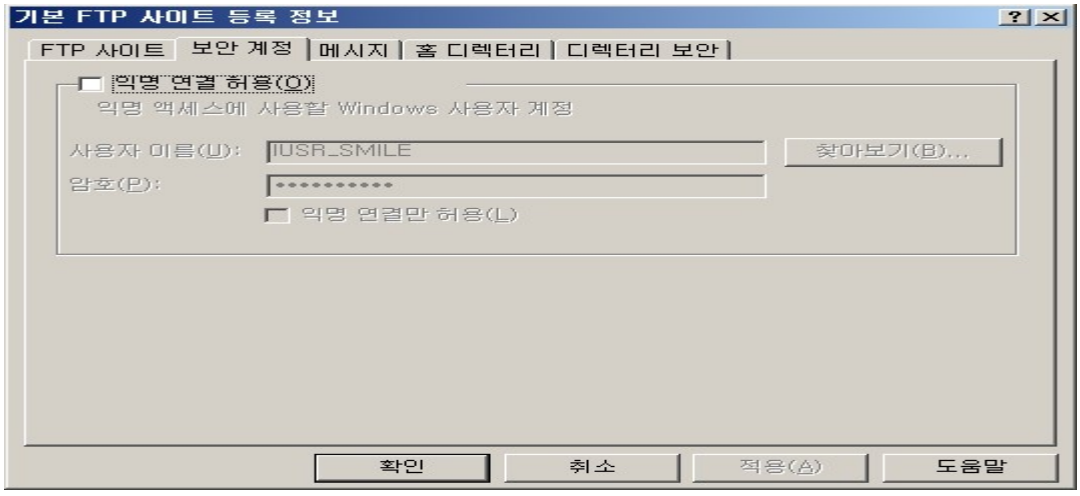
httpext.dll 파일의 Everyone 권한 삭제 : C:₩WINNT₩system32₩inetsrv₩httpext.dll 마우스 오른쪽버튼 클릭
-> 등록정보 -> 보안 -> Everyone 선택 -> 제거 버튼 클릭 -> 확인

홈디렉토리 메뉴의 쓰기 권한 삭제 : 제어판 -> 관리도구 -> 인터넷서비스관리자 -> 서비스중인 웹사이트의
마우스 오른쪽버튼 클릭 -> 등록정보 -> 홈디렉토리 -> 로컬경로 항목중 쓰기 부분의 체크 해지
-> 적용 -> 확인

[12] FTP 익명 접속 거부

FTP 서비스에 익명접속을 허용하지 않도록 설정한다.(매우 중요)

[인터넷정보서비스관리] -> [해당FTP 사이트] -> [속성] -> [보안계정] -> [익명연결허용] 체크 해지 -> [적용] -> [확인]



[13] MS-SQL 서비스팩 설치

지난 2003년 1월 25일에 Slammer Worm으로 일어났던 인터넷 대란을 기억할 것이다.
MS-SQL 2000 서비스팩3을 설치했더라면 문제는 전혀 없었을 것이다.
(MS에서 그 이전에 패치가 나온 상태였는데도 불구하고...)
시스템 관리자는 다시 한 번 보안패치에 대하여 관심을 기울여야 할 것이다.

설치 :
MS-SQL Server 2000 서비스팩4를 아래 사이트에서 해당 설치된 언어에 따라 선택후 다운로드 받는다.
다운로드 받은 파일을 실행하면 압축이 풀린다.
패치전에 반드시 DB 백업을 한다.
MS-SQL 동작을 정지시킨다.
압축을 푼 폴더에 setup.bat 파일을 실행하면 패치가 진행 된다.
패치후 엔터프라이즈관리자에서 제품버전이 8.00760 이상임을 반드시 확인후 MS-SQL을 시작한다.

다운로드 : http://www.microsoft.com/downloads/details.aspx?displaylang=ko&FamilyID=8e2dfc8d-c20e-4446-99a9-b7f0213f8bc5

한국어 버전 :
http://www.microsoft.com/downloads/info.aspx?na=46&p=6&SrcDisplayLang=ko&SrcCategoryId=&SrcFamilyId=8e2dfc8d-c20e-4446-99a9-b7f0213f8bc5&u=http%3a%2f%2fdownload.microsoft.com%2fdownload%2fc%2f6%2f1%2fc61fbaf2-2030-418f-844b-9548776014c7%2fSQL2000-KB884525-SP4-x86-KOR.EXE

영문 32bit 버전 :
http://www.microsoft.com/downloads/info.aspx?na=46&p=8&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=8e2dfc8d-c20e-4446-99a9-b7f0213f8bc5&u=http%3a%2f%2fdownload.microsoft.com%2fdownload%2f1%2fb%2fd%2f1bdf5b78-584e-4de0-b36f-c44e06b0d2a3%2fSQL2000-KB884525-SP4-x86-ENU.EXE

[14] 윈도우 보안도구

운영체제의 서비스 팩과 보안 패치를 최신 버전으로 유지하는 것은 보안 사고를 예방하기 위한 기본적인 과제이다. 과거 큰 피해를 입었던 보안 사고들은 주기적인 보안 패치를 통해서 미연에 막을 수 있는 것이 대부분이었다. 이러한 권장 패치에 대한 알림과 자동 업데이트 기능이 운영체제 차원에서 제공되므로 이를 적극 이용한다.
또한, 마이크로소프트에서 제공하고 있는 보안도구의 활용도 필요하다.

1. MBSA

MBSA(Microsoft Baseline Security Analyzer)라는 툴을 이용하면 중요한 보안 패치의 적용 여부 뿐만 아니라 운영체제나 인터넷 익스플로어, SQL 서버, MDAC 등의 구성요소를 분석하여 보안상 취약한 부분을 손쉽게 확인할 수 있다.

다운로드 : http://www.microsoft.com/technet/security/tools/mbsahome.mspx

2. IIS Lockdown

IIS Lockdown 툴은 사용 목적에 따라 권장되는 IIS 웹 서버의 설정을 구성해주는 도구이다. 즉, 사용 목적에 따라 필요한 구성요소만 활성화시키고 그외의 구성요소는 비활성 상태로 만든다. IIS 6.0의 경우는 이미 적용된 사항으로 하위 버전을 사용하는 경우에만 설치한다.
IIS Lockdown 툴은 실행과 동시에 IIS 웹 서버의 하위 서비스나 그 환경설정 내용이 변경되어 적용되므로 주의가 필요하다. 적용 후에 일부 서비스가 정상 동작하지 않을 수 있으며 이를 수정하는 과정이 필요할 수 있기 때문이다. 따라서 실제 사용중인 웹 서버에 바로 적용하기 전에 테스트 서버로 동일한 환경을 구성한 뒤에 정상적으로 서비스가 되는지 테스트한 후에 사용하는 것이 좋다.
IIS Lockdown 툴은 설치 프로그램이 아니라 단독 실행파일이다. 웹 서버가 사용되는 목적에 따라 활성화되는 구성요소와 IIS의 메타베이스 정보가 다르게 설정되므로 올바른 템플릿을 선택하는 것이 중요하다. 각 템플릿 별 세부 설정사항에 대한 내용은 아래 링크페이지를 참고한다.

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q325864

다운로드 : http://www.microsoft.com/technet/security/tools/locktool.mspx

3. URLScan

URLScan은 ISAPI 필터로 특정 HTTP 요청을 블록킹함으로써 IIS 서버를 보호하는 역할을 담당한다. 명령 프롬프트에서 'iislockd.exe /q /c'라고 입력함으로써 IISLockdown을 실행하지 않고 URLScan 필터만 설치할 수도 있다. 설치된 URLScan을 삭제하려면 제어판 -> 프로그램 추가/제거 에서 UrlScan 을 찾아 삭제하면 된다.

URLScan 필터는 'C:₩WINDOWS₩system32₩inetsrv₩urlscan' 에 설치된다. 이 디렉토리에는 URLScan의 실행에 필요한 바이너리 파일과 환경설정 파일이 있으며 로그파일이 저장된다. 이 디렉토리에서 urlscan.ini 파일이 있는데 바로 URLScan 필터의 동작을 설정하는 환경설정 파일이다.

UrlScan.ini 파일에는 필터링 하는데 사용되는 여러 섹션과 설정 항목이 존재한다. 어떠한 메소드를 허용하고 거부할 것인가는 AllowVerbs와 DenyVerbs를 이용하면 되고, 어떠한 확장자를 허용하고 거부할 것인가는 AllowExtensions와 DenyExtensions 섹션을 이용하면 된다. 서버의 경로 탐색에 대한 거부는 DenyUrlSequences 섹션을, 그리고 전반적인 설정에 사용되는 options 섹션이 있다.

ISAPI 필터는 IIS 웹 서버가 요청을 받기 전에 해당 요청을 가로채서 먼저 처리하므로 UrlScan 필터에 의해서 거부된 요청은 IIS 웹 서버로 전달되지 않는다. 초기 설정 후에는 로그 파일을 잘 분석하여 어떠한 요청이 거부되는지, 만약 정상적인 요청이 거부되고 있다면 UrlScan.ini 설정파일을 수정하는 과정이 필요하다.

다운로드 : http://www.microsoft.com/downloads/details.aspx?familyid=23D18937-DD7E-4613-9928-7F94EF1C902A&displaylang=en

[15] 네트워크 보안

1. NetBIOS 비활성화

NetBIOS는 별개의 컴퓨터 상에 있는 애플리케이션들이 근거리통신망 내에서 서로 통신할 수 있게 해주는 프로토콜로서 Windows에 의해 채택되어 있다. 만약 웹 서버에서 네트워크를 통한 다른 컴퓨터와의 공유가 필요없다면 NetBIOS를 제거함으로써 DDos(Distributed Denial of Service) 공격이나 호스트 열거(host enumeration)에 대한 위험 요소를 줄일 수 있다. NetBIOS는 다음과 같은 포트를 사용한다

TCP/UDP 137번 (NetBIOS name service)
TCP/UDP 138번 (NetBIOS datagram service)
TCP/UDP 139번 (NetBIOS session service)

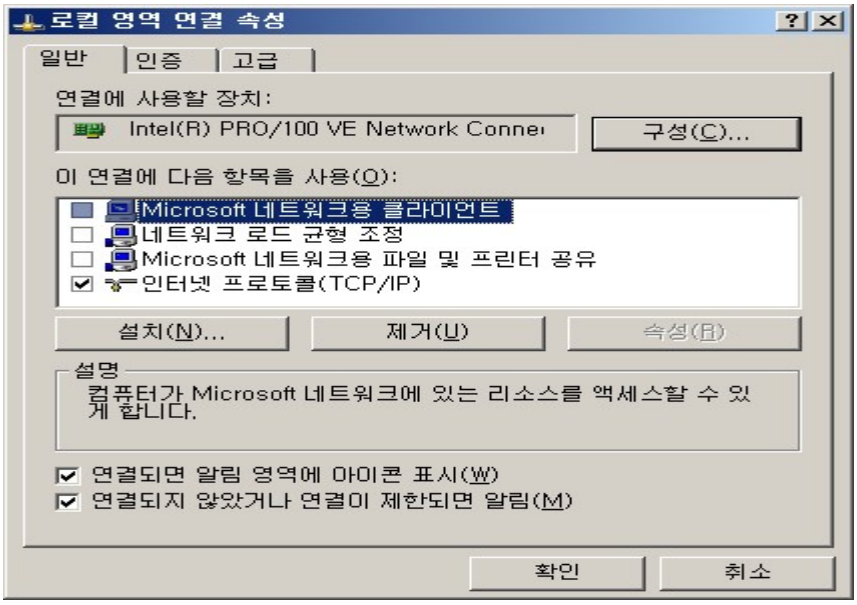
TCP/IP에서 NetBIOS를 비활성화하는 방법은 다음과 같다.
[내 컴퓨터] -> [속성] -> [하드웨어]탭 -> [장치관리자] -> [보기] 메뉴 -> [숨김장치표시] -> [비 플러그 앤 플레이 드라이버] -> [NetBios over Tcpip] -> [제거]

2. SMB 비활성화

SMB(Session Message Block) 프로토콜은 Windows에서 디스크와 프린터를 네트워크 상에서 공유하는데 사용된다. SMB는 다음과 같은 포트를 사용한다.
TCP 139번 포트
TCP 445번 포트

SMB를 비활성화하려면 다음과 같은 방법으로 TCP/IP에서 SMB를 언바인드 시킨다.

[내네트워크 환경] -> 속성 -> [로컬영역연결] -> 속성 -> [Microsoft 네트워크용 클라이언트] 와 [Microsoft 네트워크용 파일 및 프린터 공유] 항목의 체크 해제 -> 확인



3. TCP Stack 강화하기

레지스트리로 제공되는 TCP/IP와 관련된 매개변수의 설정을 변경함으로써 SYN Floods, ICMP, SNMP 공격과 같은 네트워크 레벨에서의 DoS(서비스 거부) 공격을 막을 수 있다.

아래에서 설명되는 레지스트리키의 기준값은 아래 참고사이트를 참조 바란다.
참고사이트 : http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod109.asp

1) SYN Floods 공격 방어

SYN 공격은 TCP/IP에서 연결을 맺는 메카니즘의 취약점을 대상으로 하며, 공격자는 TCP의 SYN 요청을 의도적으로 발생시키는 프로그램을 이용해서 서버상의 커넥션 큐를 넘치게 만든다. SYN Floods 공격으로부터 웹 서버를 보호하려면 레지스트리 편집기를 이용해서

HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩Tcpip₩Parameters 키에 다음과 같은 항목에 대한 값을 지정하면 된다.

항목	권장	범위	설명
SynAttackProtect	2	0-2(활성)	SYN 공격에 대한 보호 기능을 활성화시킨다. SYN-ACKS의 재전송을 적게 조절함으로써 SYN 공격을 막는다. TcpMaxHalfOpen나 TcpMaxHalfOpenRetried 설정과 함께 사용되어야 한다.
TcpMaxPortsExhausted	5	0-65535	SYN Floods 공격이 발생했음을 판단하는데 기준이 되는 TCP 연결의 최대값
TcpMaxHalfOpen	500	100-65535	SYN 공격이 동작하기 전에 SYN_RCVD 상태에서 연결을 허용할 최대값. 이를 적용하려면 먼저 SynAttackProtect가 활성화되어 있어야 한다.
TcpMaxHalfOpenRetried	400	80-65535	SYN 공격이 동작하기 전에 SYN_RCVD 상태에서 연결을 허용할 최대값. SYN_RCVD는 SYN 공격에 대한 방어가 동작하기 전에 적어도 한번의 SYN 플래그를 재전송한다. 이를 적용하려면 먼저 SynAttackProtect가 활성화되어 있어야 함.

2) AFD.SYS 설정

FTP 서버 및 웹 서버와 같은 Windows 소켓 응용 프로그램에서는 연결 시도를 Afd.sys에서 처리한다. Afd.sys도 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩AFD₩Parameters 키에 대하여 다음 항목을 적용한다.

항목	권장	범위	설명
EnableDynamicBacklog	1	0(사용안함) 1(사용)	많은 양의 SYN_RCVD 연결에 대해서 능동적으로 대처할 것인지에 대한 AFD.SYS 기능의 활성화 여부를 지정한다.
MinimumDynamicBacklog	20	0-4294967295	Listening endpoint에서 허용하는 접속의 최소 수를 지정한다. 접속수가 설정된 값 이하가 되면 새로운 스레드에서 추가 연결을 생성한다.
MaximumDynamicBacklog	20000	0-4294967295	Listening endpoint에서 허용하는 'Quansi-free' 연결의 최대 수를 지정한다. 'Quansi-free' 는 SYN_RCVD 상태의 연결과 free connections를 더한 값이다.
DynamicBacklogGrowthDelta	10	0-4294967295	추가적인 연결이 필요할 때 생성되는 free connections의 수를 지정한다.

3) ICMP 공격 방어

ICMP(Internet Control Message Protocol)는 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고 에러를 알려주는 프로토콜이다. 대표적인 예로 ping 명령어는 인터넷 접속을 테스트하기 위해 ICMP를 사용한다. HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩AFD₩Parameters 키에서 다음 항목을 설정한다.

항목	권장	범위	설명
EnableICMPRedirect	0	0(사용안함) 1(사용)	이 값을 0으로 설정함으로써 ICMP 리디렉트 패킷을 수신했을 때 호스트 경로를 생성하지 않게 하여 부하를 줄일 수 있다.

4) SNMP 공격방어

SNMP(Simple Network Management Protocol)는 네트워크를 관리하기 위한 프로토콜로서 망 관리를 위해 SNMP manager와 agent가 서로 통신하는데 사용된다. 그러나 SNMP을 악용하면 네트워크 연결 장비를 무력화시킬 수 있을 뿐만 아니라 장비를 직접 조작하거나 서비스 거부 공격으로 웹사이트를 마비시킬 수 있다. HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩Tcpip₩Parameters 키에 다음과 같은 항목에 대한 값을 지정한다.

항목	권장	범위	설명
EnableDeadGWDetect	0	0(사용안함) 1(사용)	공격자가 2차 게이트웨이로 스위칭하는 것을 막는다. 이 값을 1로 설정하면 TCP는 dead-gateway 탐지를 수행한다.

[16] 홈페이지 보안 관리

1. 관리자페이지 접근통제 취약점

문제점 :
웹서비스의 사용자나 데이터, 컨텐츠를 손쉽게 관리하기 위한 목적으로 다양한 기능과 권한을 갖고 있는 홈페이지의 관리자페이지는 일반적으로 추측하기 쉬운 URL(예: /admin, /manager)을 사용하고 있어 ID/패스워드에 대한 크랙 또는 접근 허가 정책의 부재로 웹관리자의 권한이 노출되어 홈페이지의 변조뿐만 아니라 웹서버의 권한까지도 노출 위험성이 있다.

조치방법 :
관리자로그인페이지는 유추하기 어려운 디렉토리명이나 파일명을 사용한다.
별도의 IP 레벨로 접근권한을 설정.
웹인터페이스는 SSL과 같은 암호화를 적용.

IIS : 제어판 -> 관리도구 -> 인터넷서비스관리자 -> 해당 관리자 페이지 폴더에 마우스 오른쪽 버튼 클릭 -> 등록정보 -> 디렉토리 보안 -> IP 주소 및 도메인 이름 제한 편집 -> 액세스 거부 선택 -> 추가 -> 관리자 호스트 IP 또는 서브넷을 등록

2. 디렉토리 리스팅 취약점

문제점 :
인터넷 사용자에게 모든 디렉토리 및 파일 목록이 보여지게 됨으로 인한 비공개자료 및 서버 접근 정보 유출

조치방법 :
제어판 -> 관리도구 -> 인터넷서비스관리자 -> 서비스중인 웹사이트의 마우스 오른쪽버튼 클릭 -> 등록정보 -> 홈디렉토리 -> 디렉토리검색(B) 체크 해지 -> 적용 -> 확인

3. 파일 다운로드 취약점

문제점 :
다운로드 대상파일의 위치 지정에 제한 조건을 부여하지 않은 다운로드스크립트의 경우, 웹브라우저의 주소창에 '../' 등의 문자열을 입력하여 시스템디렉토리에 비공개 자료들이 유출

조치방법 :
게시판 등에 파일 다운로드 기능이 있는지 점검.
파일 다운로드 스크립트 이용 여부 확인.
다운로드 스크립트내에서 다운로드 허용파일명에 '..', '/', '₩' 와 같은 문자열이 존해하면 필터링할 수 있도록 수정하여, 특정 디렉토리하의 파일만 다운로드 받을 수 있도록 함.

4. 크로스 사이트 스크립트 취약점

문제점 :
글쓰기 기능이 있는 게시판 등에서 입력내용에 대해 실행코드인 스크립트의 태그를 적절히 필터링하지 않을 경우, 악의적인 스크립트가 포함된 게시물을 등록할 수 있어 해당 게시물을 열람하는 일반사용자의 PC로부터 개정정보인 쿠키를 유출할 수 있는 등의 피해 초래

조치방법 :
글쓰기가 가능한 게시판에서 사용자들이 올리는 글에 대해서 script를 모두 필터링할 수 있도록 관련 웹소스코드를 수정, script 문장에 존재하는 메타캐릭터를 아래의 예와 같이 변환시킨다.
< -> &lt > -> &gt (-> &#40) -> &#41 # -> &#35 & -> &#38

5. 파일 업로드 취약점

문제점 :
첨부파일 업로드를 허용하는 게시판에서 .asp , .pl 등의 확장자를 가진 스크립트 파일의 업로드를 허용할 경우, 해커가 악성 실행 프로그램을 업로드한 후에 웹브라우저를 이용하여 원격에서 서버의 시스템명령어를 실행시킬 수 있다. 보통 백도어 프로세스 실행으로 백도어포트 오픈됨.

조치방법 :
업로드되는 파일의 확장자가 실행가능한 확장자명(php, asp, jsp, cgi, pl 등)일 경우 필터링하여 업로드되지 않도록 관련 웹소스코드 수정, 2중 확장자 형태도 필터링

인터넷서비스관리자 -> 업로드폴더에 마우스 오른쪽 버튼 클릭 -> 등록정보 -> 디렉토리 -> 실행권한 없음 선택 -> 적용 -> 확인

6. SQL Injection 취약점

문제점 :
웹브라우저 주소창 또는 사용자 ID 및 패스워드 입력화면 등에서 DB SQL문에 사용되는 문자기호(',")의 입력을 필터링 하지 않은 경우에 인증절차 없이 DB에 접근하여 자료 유출 및 변조 가능

조치방법 :
DB와 연결하는 웹소스코드에서 ID 및 패스워드 입력란에 특수문자(' " / ₩ ; : -- + 공백 등)는 필터링하도록 수정한다. SQL 서버의 에러메세지를 외부에 보여주지 않도록 설정한다.

[17] 터미널서비스 포트변경하기

윈도우 서버에 설치된 터미널서비스의 포트번호를 변경하여 사용한다.
변경후엔 IPSEC 등에 변경된 포트정보를 수정한다. 꼭!!

1. 포트 번호 변경

1) 시작 -> 실행 -> regedit 입력 -> 확인을 눌러 레지스트리 편집기를 실행한다.

2)HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩TerminalServer₩Wds₩rdpwd₩Tds₩tcp 로 이동한다.

3) PortNumber REG_DWORD 0x00000d3d(3389) 수정모드에서 10진수를 선택하고 원하는 포트번호를 입력

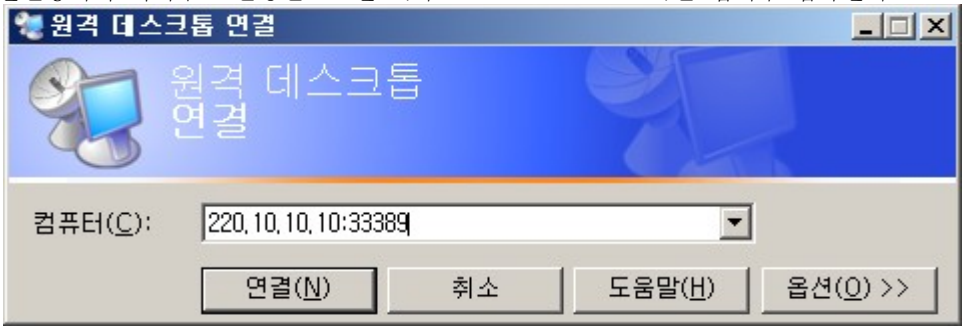
4) HKEY_LOCAL_MACHINE₩System₩CurrentControlSet₩Control₩TerminalServer₩WinStations₩RDP-Tcp 로 이동

5) PortNumber REG_DWORD 0x00000d3d(3389) 수정모드에서 10진수를 선택하고 원하는 포트번호를 입력

6) 편집기 창을 닫고 리부팅한다.

2. 클라이언트에서 서버 접속하기

원격데스크탑 연결창에서 서버주소:변경된포트번호(예: 10.10.10.10:33389)를 입력후 접속한다.



[18] 후기

지금까지의 내용이 다소 부족한 감이 있으나, 위의 항목 하나하나를 따라서 적용해 보길 권장한다.
또한, 후임 시스템관리자를 위해서 보안설정을 적용한 사항들은 반드시 메모해 두길 바란다.

보안설정 내용에서 중요한 것은 다음과 같다.

1. 보안패치를 꼭 한다.
2. IPSEC을 반드시 적용한다.
3. 바이러스 방역 솔루션을 설치한다.
4. 데이타 백업을 철저히 한다.

보안패치를 함으로써 시스템의 보안버그로 인한 시스템의 침해사고를 예방할 수 있으며,
IPSEC에서 서비스에 필요한 포트 예를 들어 웹서비스만을 한다면 80 번 포트외에는 외부의 접속을 거부해 둠으로써, 크래킹 시도로 인한 백도어포트가 열리더라도 크래커의 접근을 차단할 수 있다.
웹서비스 80번 포트로 들어오는 웜이나 바이러스의 침투는 바이러스 방역 솔루션으로 차단한다면, 시스템의 침해사고는 거의 발생하지 않을 것이다.
위의 4가지 항목을 준수한다면 안전한 시스템관리에 만전을 기할 수 있으리라 믿는다.

참고문서 :

http://www.microsoft.com/korea/technet/security/default.asp
http://www.microsoft.com/korea/technet/security/tools/w2ksvrcl.asp#165332g
http://download.microsoft.com/download/1/B/D/1BDF5B78-584E-4DE0-B36F-C44E06B0D2A3/ReadmeSql2k32sp4.htm