

Windows Server 2003

- Windows Firewall -

Copyright @ 2012 Good Internet

소 속	IDC실
이 름	정명구 매니저
E-mail	tech@tongkni.co.kr

통큰아이

INDEX

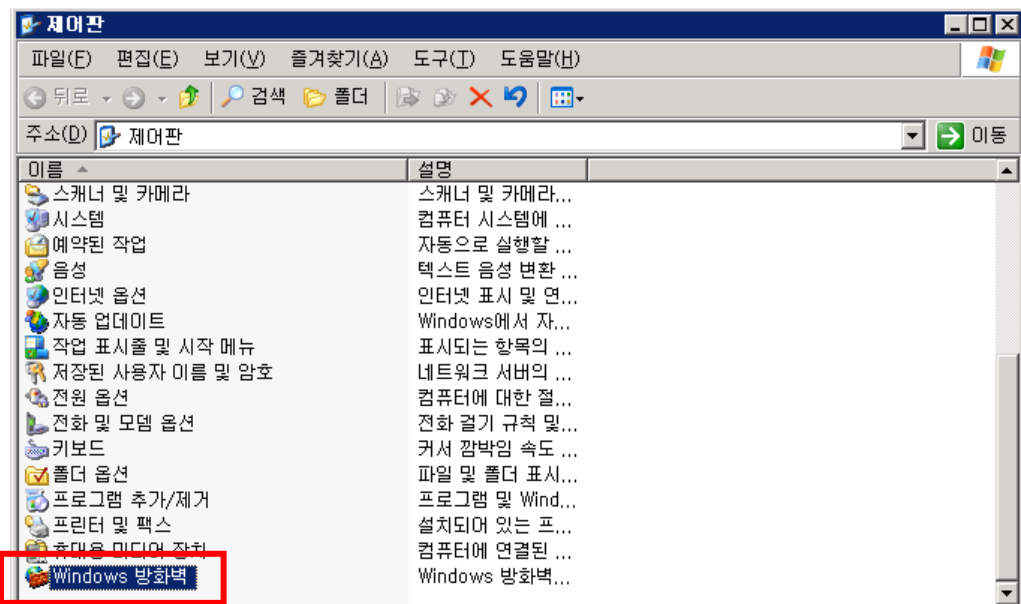
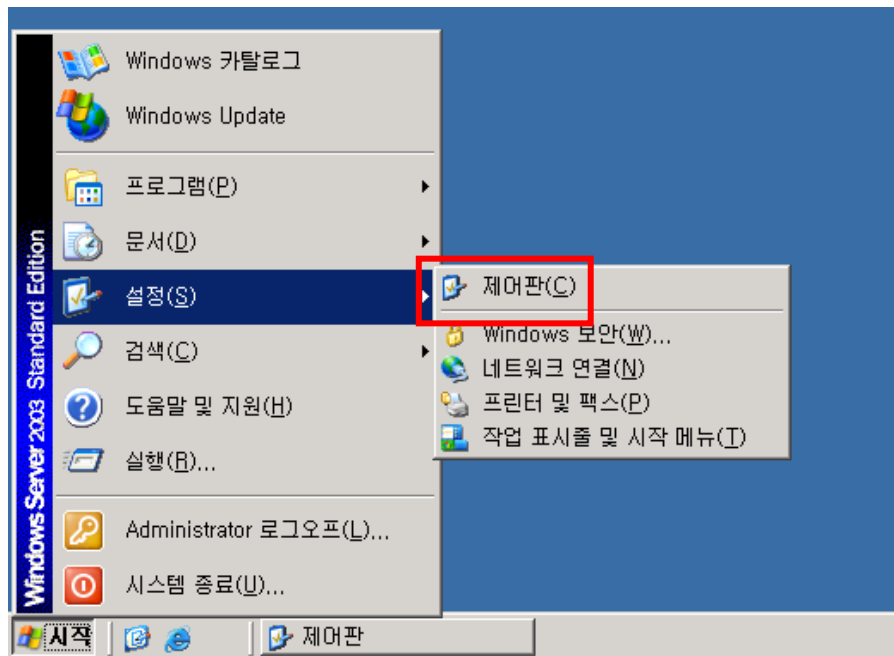
1. 개요	3
2. 방화벽 설정하기.	4
3. 활용하기.	7
3.1 일반적으로 사용하는 서비스 포트 허용하기.	7
3.2 ICMP(ping) 허용하기.	11
(참고) Well-Known 포트 번호 리스트.....	13

1. 개요.

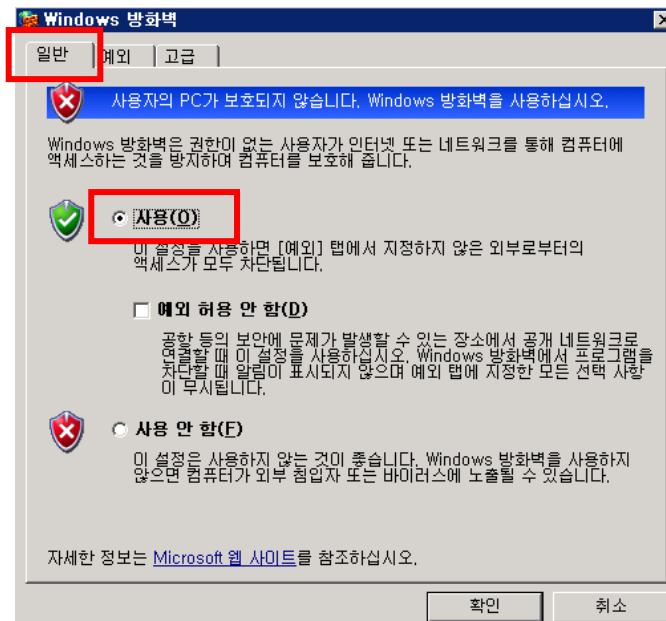
- 윈도우 서버에서 제공하는 기본 방화벽으로 간단한 조작법으로 서버의 포트를 관리 할 수 있는 보안 솔루션 입니다.
기본적인 보안 설정으로 반드시 설정할 수 있도록 합니다.
- 네트워크 구간에서의 방화벽 장비나 서버에서 별도의 보안 솔루션을 통해 보안성을 강화시킬 수 있지만 여기서는 윈도우에 내장된 기본 보안 기능인 방화벽을 이용하여 보안을 강화하고자 합니다.
- 윈도우 방화벽은 서버로 수신하는 포트번호를 제어할 수 있습니다.
- 아래는 방화벽을 구성하는 절차입니다.
 - ① 제어판에서 방화벽을 사용하도록 설정.
 - ② 허용할 예외 포트를 추가.
- 방화벽을 사용할 경우 기본적으로 모든 포트를 막고 예외로 추가한 포트만 통신이 가능합니다.
- ※ 주의 : 원격접속 포트를 예외로 추가하지 않은 채 방화벽을 사용하도록 설정하면 외부PC에서 서버로의 원격접속이 불가능해집니다.
또한 웹 서비스 등의 어떠한 서비스가 이미 운영되고 있는 서버의 경우에도 반드시 해당 서비스들의 포트를 허용하는 예외를 추가한 후에 방화벽을 설정하시기 바랍니다.
- 본 매뉴얼은 보안을 위한 방화벽 설정 방법에 대해 작성되었습니다.

2. 방화벽 설정하기.

① 시작 -> 제어판 -> Windows 방화벽 을 클릭합니다.

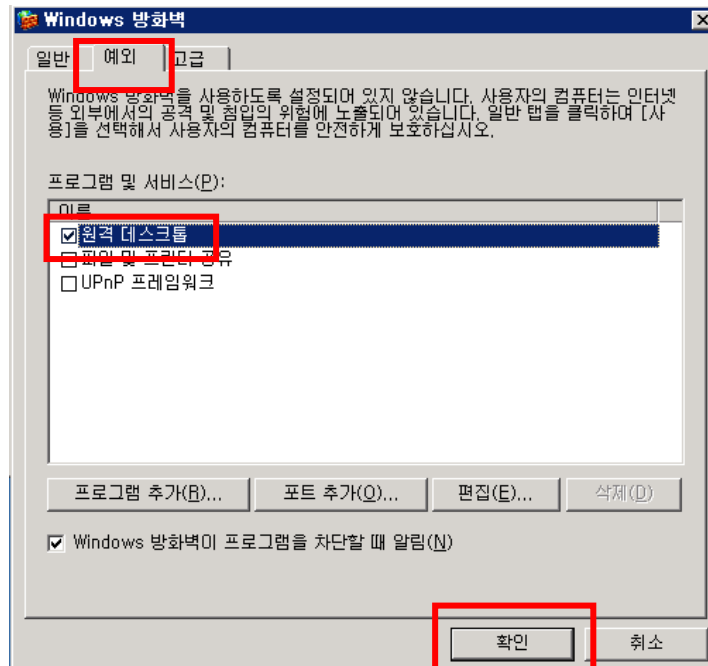


② 일반 탭에서 “사용”을 체크합니다.



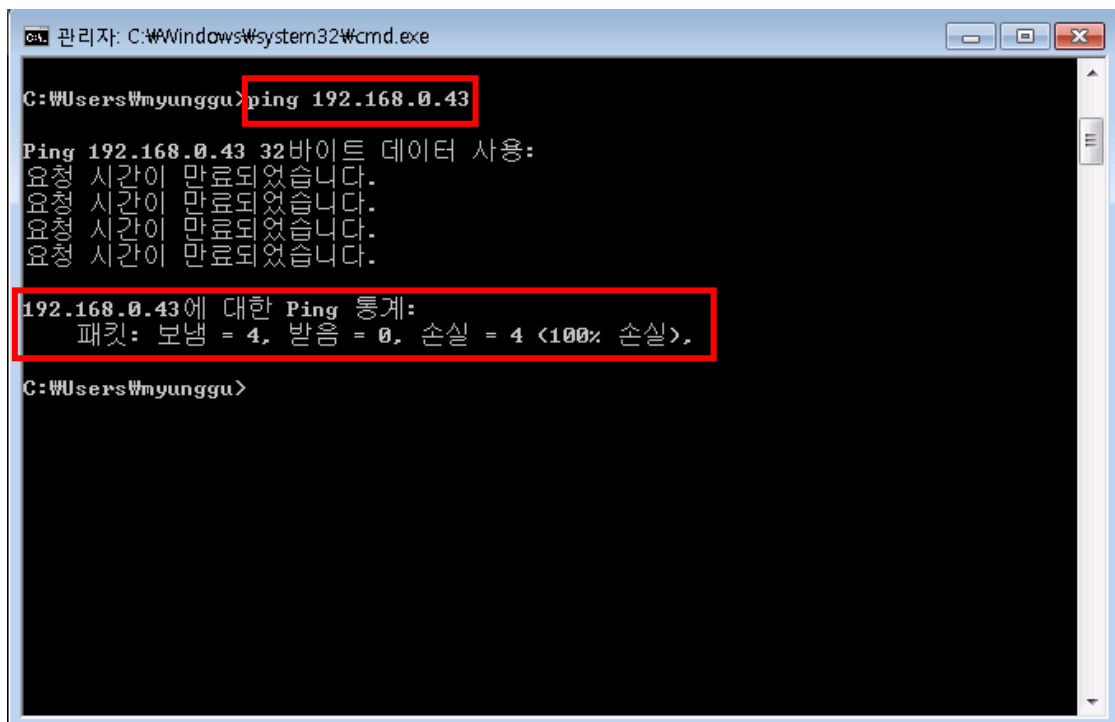
③ 예외 탭에서 “원격 데스크톱” 항목에 체크 후 확인을 누릅니다.

※ 항목이 없는 경우 챕터 3을 참고하여 추가하시기 바랍니다.



- ④ 외부 PC의 cmd 창에서 Ping 테스트 및 원격접속을 테스트하여 방화벽이 정상적으로 설정되었는지 확인합니다.

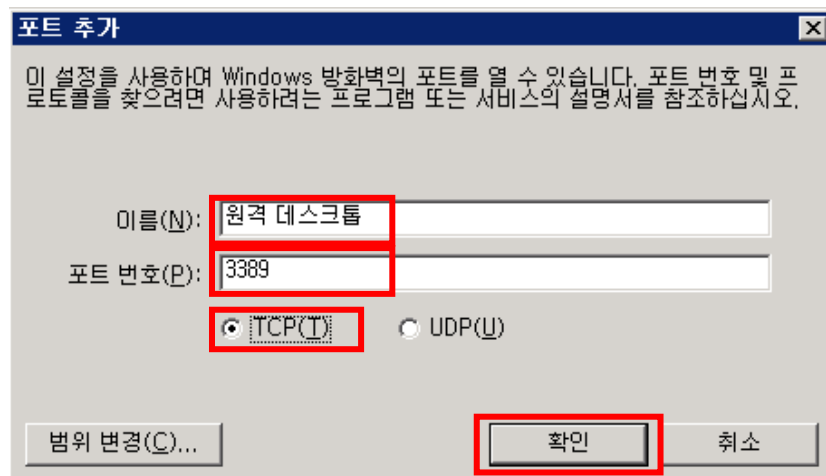
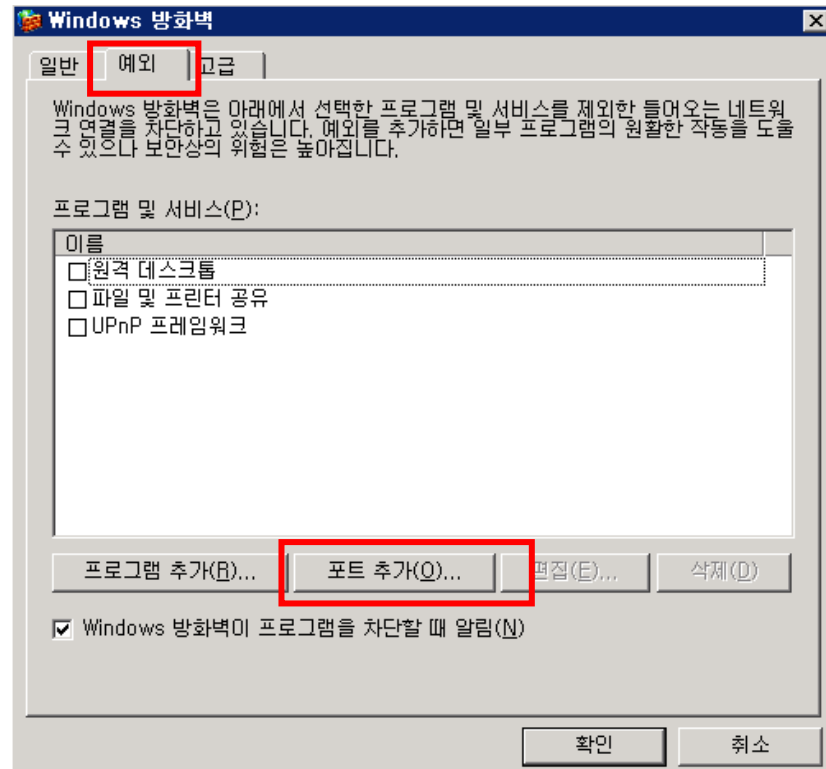
(Ping 응답이 없고, 원격접속이 잘 된다면 정상적으로 할당이 완료된 것 입니다.)



3. 활용하기

3.1 일반적으로 사용하는 서비스 포트 허용하기.

- ① 원격 데스크톱 포트를 허용하는 경우 - TCP 3389번 포트 허용.
방화벽 예외 탭에서 "포트 추가"버튼을 클릭한 후 항목에 아래와 같이 추가합니다.
(이미 존재하는 경우 따로 추가할 필요 없습니다.)



- ② 서버에서 웹 서비스를 운영하는 경우 - TCP 80번 포트 허용.
방화벽 예외 탭에서 "포트 추가"버튼을 클릭한 후 항목에 아래와 같이 추가합니다

이 설정을 사용하여 Windows 방화벽의 포트를 열 수 있습니다. 포트 번호 및 프로토콜을 찾으려면 사용하려는 프로그램 또는 서비스의 설명서를 참조하십시오.

이름(N): Web 서비스

포트 번호(P): 80

☒ TCP(T) ☐ UDP(U)

범위 변경(C)... **확인** 취소

③ FTP 서비스를 운영하는 경우 – TCP 20, 21번 포트 허용.

※ 같은 방식으로 TCP 21번포트도 추가합니다.

이 설정을 사용하여 Windows 방화벽의 포트를 열 수 있습니다. 포트 번호 및 프로토콜을 찾으려면 사용하려는 프로그램 또는 서비스의 설명서를 참조하십시오.

이름(N): FTP 서비스

포트 번호(P): 20

☒ TCP(T) ☐ UDP(U)

범위 변경(C)... **확인** 취소

④ DNS 서비스를 운영하는 경우 – TCP 53번, UDP 53번 포트 허용.

※ 같은 방식으로 TCP 53번 포트도 추가합니다.

이 설정을 사용하여 Windows 방화벽의 포트를 열 수 있습니다. 포트 번호 및 프로토콜을 찾으려면 사용하려는 프로그램 또는 서비스의 설명서를 참조하십시오.

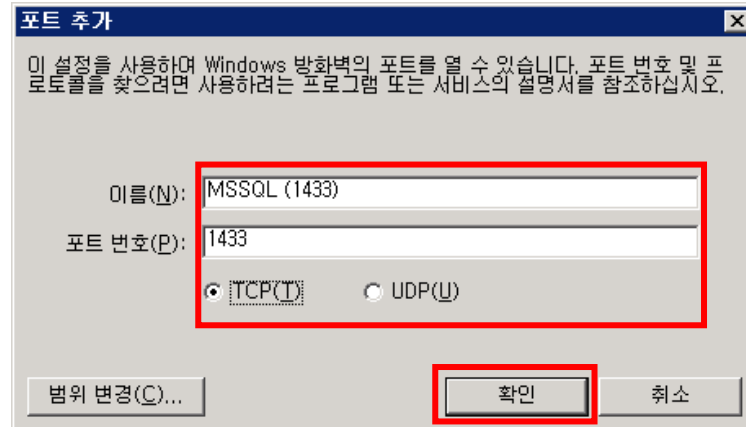
이름(N): DNS (UDP 53)

포트 번호(P): 53

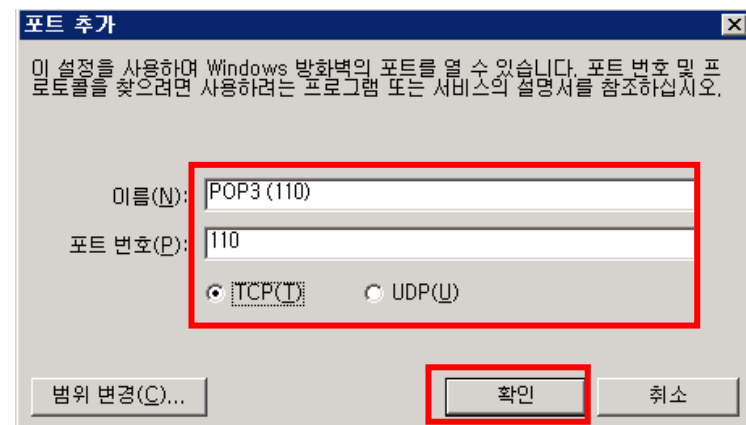
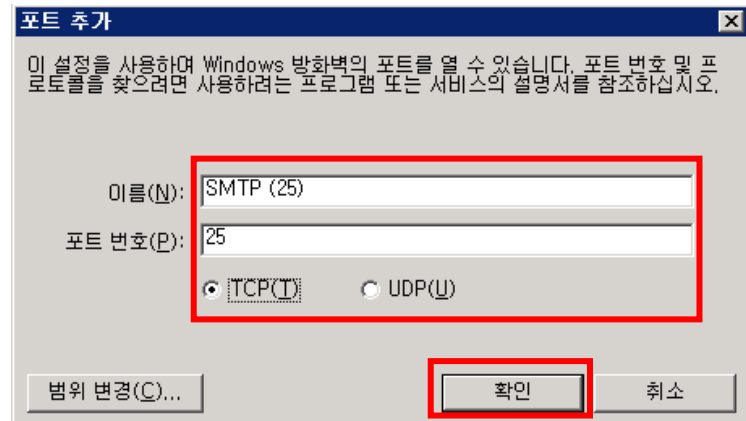
☐ TCP(T) ☒ UDP(U)

범위 변경(C)... **확인** 취소

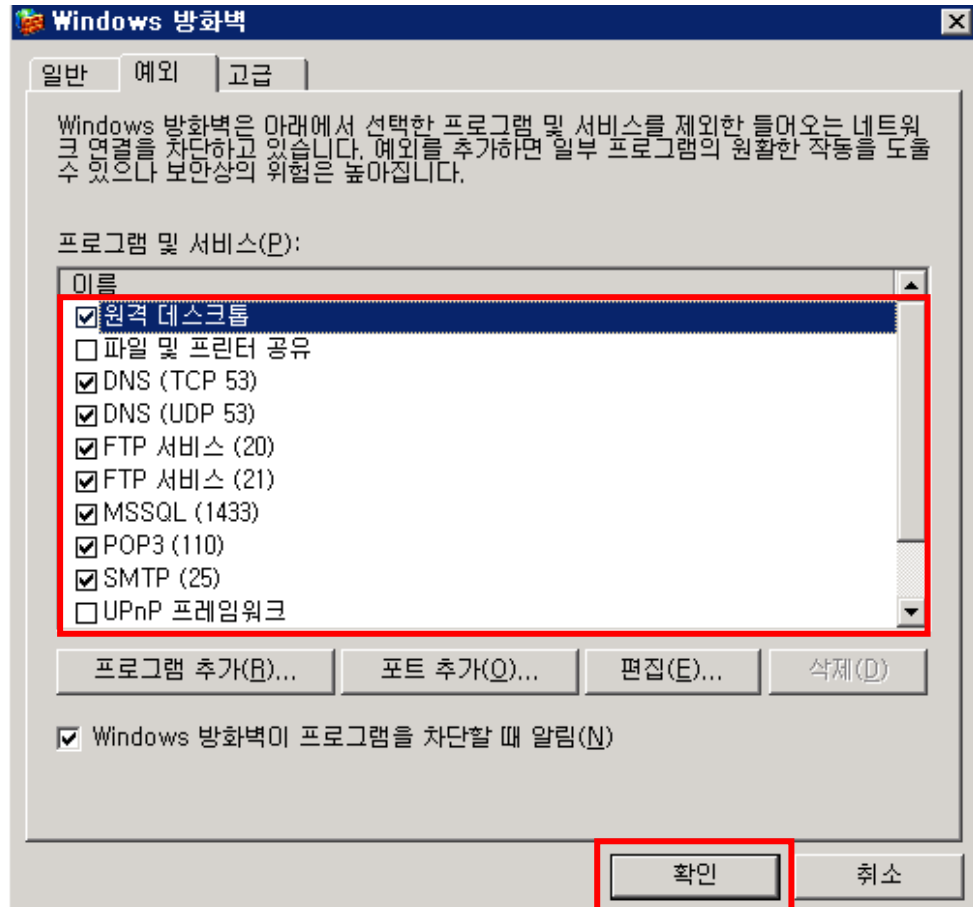
⑤ DB서버로 사용하기 위해 MS-SQL이 운영되고 있는 경우 – TCP 1433번 포트 허용.
(외부에서 DB서버에 접근할 경우가 없다면 허용하지 않아도 됩니다.)



⑥ 메일 서버로 운영하고 있는 경우 – TCP 25 (SMTP) , TCP 110 (POP3)번 포트 허용.



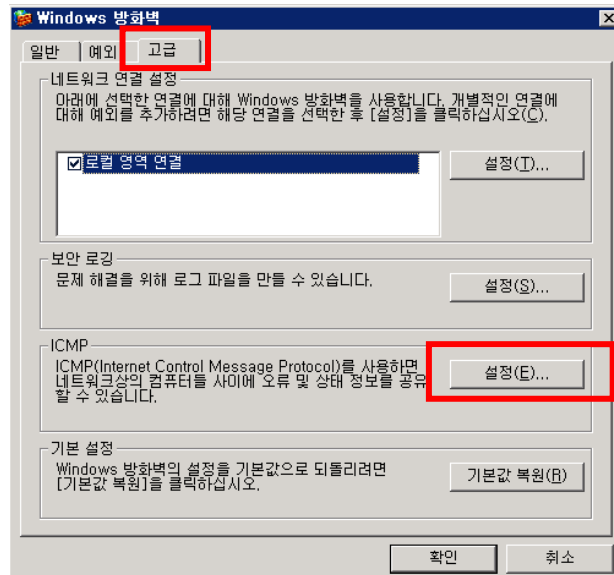
⑦ 아래 그림은 여러가지 예외 포트를 추가한 상태의 한 예시 입니다.



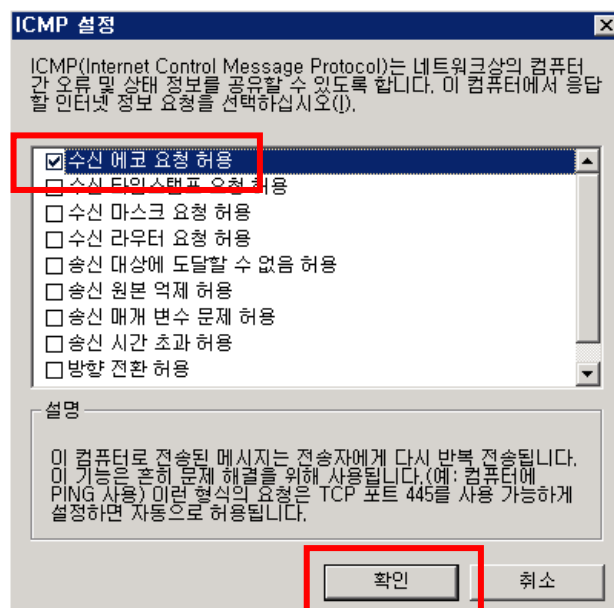
3.2 ICMP(ping) 허용하기

- ① ICMP(ping테스트)를 허용할 경우에는 포트가 아닌 프로토콜이기 때문에 설정 방법이 다

룹니다. 고급 탭에서 ICMP "설정" 버튼을 클릭하고 "수신 에코 요청 허용"을 체크합니다.



② "수신 에코 요청 허용" 항목을 체크합니다.



③ 외부 PC의 cmd 창에서 Ping 테스트하여 응답이 정상적으로 오는지 확인합니다.

```
관리자: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Wmyunggu>ping 192.168.0.43

Ping 192.168.0.43 32바이트 데이터 사용:
192.168.0.43의 응답: 바이트=32 시간<1ms TTL=128
192.168.0.43의 응답: 바이트=32 시간<1ms TTL=128
192.168.0.43의 응답: 바이트=32 시간<1ms TTL=128
192.168.0.43의 응답: 바이트=32 시간<1ms TTL=128

192.168.0.43에 대한 Ping 통계:
    패킷: 보낸 = 4, 받음 = 4, 손실 = 0 (0% 손실),
    왕복 시간<밀리초>:
        최소 = 0ms, 최대 = 0ms, 평균 = 0ms

C:\Users\Wmyunggu>
```

(참고) 아래는 Well-Known 포트 번호 리스트 입니다.

참고하셔서 서비스에 필요한 포트번호가 있다면 방화벽 허용정책에 추가하시기 바랍니다.

통큰아이

포트 프로토콜 응용 프로그램 프로토콜 시스템 서비스이름

7 TCP Echo 단순 TCP/IP 서비스
7 UDP Echo 단순 TCP/IP 서비스
9 TCP Discard 단순 TCP/IP 서비스
9 UDP Discard 단순 TCP/IP 서비스
13 TCP Daytime 단순 TCP/IP 서비스
13 UDP Daytime 단순 TCP/IP 서비스
17 TCP Quotd 단순 TCP/IP 서비스
17 UDP Quotd 단순 TCP/IP 서비스
19 TCP Chargen 단순 TCP/IP 서비스
19 UDP Chargen 단순 TCP/IP 서비스
20 TCP FTP 기본 데이터 FTP 게시 서비스
21 TCP FTP 제어 FTP 게시 서비스
21 TCP FTP 제어 응용 프로그램 계층 게이트웨이 서비스
23 TCP 텔넷 텔넷
25 TCP SMTP Simple Mail Transfer Protocol
25 TCP SMTP Exchange Server
42 TCP WINS 복제 Windows Internet Name Service
42 UDP WINS 복제 Windows Internet Name Service
53 TCP DNS DNS 서버
53 UDP DNS DNS 서버
53 TCP DNS 인터넷 연결 방화벽/인터넷 연결 공유
53 UDP DNS 인터넷 연결 방화벽/인터넷 연결 공유
67 UDP DHCP 서버 DHCP 서버
67 UDP DHCP 서버 인터넷 연결 방화벽/인터넷 연결 공유
69 UDP TFTP Trivial FTP 데몬 서비스
80 TCP HTTP Windows Media 서비스
80 TCP HTTP World Wide Web 게시 서비스
80 TCP HTTP SharePoint Portal Server
88 TCP Kerberos Kerberos 키 배포 센터
88 UDP Kerberos Kerberos 키 배포 센터
102 TCP X.400 Microsoft Exchange MTA 스택
110 TCP POP3 Microsoft POP3 서비스

110 TCP POP3 Exchange Server
119 TCP NNTP Network News Transfer Protocol
123 UDP NTP Windows 시간
123 UDP SNTP Windows 시간
135 TCP RPC 메시지 대기열
135 TCP RPC 원격 프로시저 호출
135 TCP RPC Exchange Server
135 TCP RPC 인증서 서비스
135 TCP RPC 클러스터 서비스
135 TCP RPC 분산 파일 시스템
135 TCP RPC 분산 링크 추적
135 TCP RPC Distributed Transaction Coordinator
135 TCP RPC 분산 파일 복제 서비스
135 TCP RPC 팩스 서비스
135 TCP RPC Microsoft Exchange Server
135 TCP RPC 파일 복제 서비스
135 TCP RPC 그룹 정책
135 TCP RPC 로컬 보안 기관
135 TCP RPC 원격 저장소 알림
135 TCP RPC 원격 저장소 서버
135 TCP RPC Systems Management Server 2.0
135 TCP RPC 터미널 서비스 라이선스
135 TCP RPC 터미널 서비스 세션 디렉터리
137 UDP NetBIOS 이름 확인 컴퓨터 브라우저
137 UDP NetBIOS 이름 확인 서버
137 UDP NetBIOS 이름 확인 Windows Internet Name Service
137 UDP NetBIOS 이름 확인 Net Logon
137 UDP NetBIOS 이름 확인 Systems Management Server 2.0
138 UDP NetBIOS 데이터그램 서비스 컴퓨터 브라우저
138 UDP NetBIOS 데이터그램 서비스 메신저
138 UDP NetBIOS 데이터그램 서비스 서버
138 UDP NetBIOS 데이터그램 서비스 Net Logon
138 UDP NetBIOS 데이터그램 서비스 분산 파일 시스템
138 UDP NetBIOS 데이터그램 서비스 Systems Management Server 2.0
138 UDP NetBIOS 데이터그램 서비스 라이선스 로깅 서비스

139 TCP NetBIOS 세션 서비스 컴퓨터 브라우저
139 TCP NetBIOS 세션 서비스 팩스 서비스
139 TCP NetBIOS 세션 서비스 성능 로그 및 경고
139 TCP NetBIOS 세션 서비스 인쇄 스펙터
139 TCP NetBIOS 세션 서비스 서버
139 TCP NetBIOS 세션 서비스 Net Logon
139 TCP NetBIOS 세션 서비스 원격 프로시저 호출 로케이터
139 TCP NetBIOS 세션 서비스 분산 파일 시스템
139 TCP NetBIOS 세션 서비스 Systems Management Server 2.0
139 TCP NetBIOS 세션 서비스 라이선스 로깅 서비스
143 TCP IMAP Exchange Server
161 UDP SNMP SNMP 서비스
162 UDP SNMP 트랩 아웃바운드 SNMP 트랩 서비스
389 TCP LDAP 서버 로컬 보안 기관
389 UDP LDAP 서버 로컬 보안 기관
389 TCP LDAP 서버 분산 파일 시스템
389 UDP LDAP 서버 분산 파일 시스템
443 TCP HTTPS HTTP SSL
443 TCP HTTPS World Wide Web 게시 서비스
443 TCP HTTPS SharePoint Portal Server
443 TCP RPC over HTTPS Exchange Server 2003
445 TCP SMB 팩스 서비스
445 TCP SMB 인쇄 스펙터
445 TCP SMB 서버
445 TCP SMB 원격 프로시저 호출 로케이터
445 TCP SMB 분산 파일 시스템
445 TCP SMB 라이선스 로깅 서비스
445 TCP SMB Net Logon
464 UDP Kerberos Password V5 Kerberos 키 배포 센터
464 TCP Kerberos Password V5 Kerberos 키 배포 센터
500 UDP IPsec ISAKMP 로컬 보안 기관
515 TCP LPD TCP/IP 인쇄 서버
548 TCP Macintosh용 파일 서버 Macintosh용 파일 서버
554 TCP RTSP Windows Media 서비스
563 TCP SSL을 통한 NNTP Network News Transfer Protocol

593 TCP RPC over HTTPS 끝점 매핑 원격 프로시저 호출
593 TCP RPC over HTTPS Exchange Server
636 TCP LDAP SSL 로컬 보안 기관
636 UDP LDAP SSL 로컬 보안 기관
993 TCP SSL을 통한 IMAP Exchange Server
995 TCP SSL을 통한 POP3 Exchange Server
1067 TCP 설치 부트스트랩 서비스 설치 부트스트랩 프로토콜 서버
1068 TCP 설치 부트스트랩 서비스 설치 부트스트랩 프로토콜 클라이언트
1270 TCP MOM-Encrypted Microsoft Operations Manager 2000
1433 TCP SQL over TCP Microsoft SQL Server
1433 TCP SQL over TCP MSSQL\$UDDI
1434 UDP SQL Probe Microsoft SQL Server
1434 UDP SQL Probe MSSQL\$UDDI
1645 UDP 레거시 RADIUS 인터넷 인증 서비스
1646 UDP 레거시 RADIUS 인터넷 인증 서비스
1701 UDP L2TP 라우팅 및 원격 액세스
1723 TCP PPTP 라우팅 및 원격 액세스
1755 TCP MMS Windows Media 서비스
1755 UDP MMS Windows Media 서비스
1801 TCP MSMQ 메시지 대기열
1801 UDP MSMQ 메시지 대기열
1812 UDP RADIUS 인증 인터넷 인증 서비스
1813 UDP RADIUS 계정 인터넷 인증 서비스
1900 UDP SSDP SSDP 검색 서비스
2101 TCP MSMQ-DC 메시지 대기열
2103 TCP MSMQ-RPC 메시지 대기열
2105 TCP MSMQ-RPC 메시지 대기열
2107 TCP MSMQ-Mgmt 메시지 대기열
2393 TCP OLAP Services 7.0 SQL Server: 하위 수준 OLAP 클라이언트 지원
2394 TCP OLAP Services 7.0 SQL Server: 하위 수준 OLAP 클라이언트 지원
2460 UDP MS Theater Windows Media 서비스
2535 UDP MADCAP DHCP 서버
2701 TCP SMS 원격 제어(제어) SMS 원격 제어 에이전트
2701 UDP SMS 원격 제어(제어) SMS 원격 제어 에이전트
2702 TCP SMS 원격 제어(데이터) SMS 원격 제어 에이전트

2702 UDP SMS 원격 제어(데이터) SMS 원격 제어 에이전트
2703 TCP SMS 원격 채팅 SMS 원격 제어 에이전트
2703 UDP SMS 원격 채팅 SMS 원격 제어 에이전트
2704 TCP SMS 원격 파일 전송 SMS 원격 제어 에이전트
2704 UDP SMS 원격 파일 전송 SMS 원격 제어 에이전트
2725 TCP SQL Analysis Services SQL Analysis Server
2869 TCP UPNP 범용 플러그 앤 플레이 장치 호스트
2869 TCP SSDP 이벤트 알림 SSDP 검색 서비스
3268 TCP 글로벌 카탈로그 서버 로컬 보안 기관
3269 TCP 글로벌 카탈로그 서버 로컬 보안 기관
3343 UDP 클러스터 서비스 클러스터 서비스
3389 TCP 터미널 서비스 NetMeeting 원격 데스크톱 공유
3389 TCP 터미널 서비스 터미널 서비스
3527 UDP MSMQ-Ping 메시지 대기열
4011 UDP BINL 원격 설치

감사합니다.