작성자 : 기술지원부 조 태 준 tedcho@nextline.net

FTP 서비스는 두개의 포트를 열어서 운영이 됩니다. 기본 FTP 의 경우 21 번포트로 접근을 해서 인증을 받은 후에 20 번 포트를 열어서 LIST 를 보여주고, 데이터를 전송을 합니다. 이것은 FTP 프로토콜이 가지는 서비스 특성입니다. 보안상의 문제등으로 기본 포트를 사용하지 않고 변경을 하게 됩니다.

이런경우 방화벽 안쪽에 있는 비 정규 포트의 FTP 서버의 접근은 돼나 디렉터리 List 가 보이지 않는 경우가 발생을 하게 됩니다. 이유는 많은 방화벽은 외부 인터페이스를 통해 새 연결을 받아 들이지 않습니다. 이러한 연결은 방화벽에 예기치 않은 연결 시도로 검색되므로 연결이 끊어집니다. 이러한 환경에서는 FTP 서버가 FTP 클라이언트에 새로운 연결 요청을 해야 하므로 표준 모드 FTP 클라이언트가 작동하지 않습니다.

FTP 서버가 모든 랜덤 포트 번호를 열 수 있으므로 방화벽에서는 이러한 구성을 하기 어렵습니다. . IIS 4.0 과 5.0 은 1024 – 5000 의 기본 임시 포트 범위를 사용하지만 IIS 6.0 을 비롯한 많은 FTP 서버가 1024 – 65535 의 임시 포트 범위를 사용하도록 구성됩니다. 이러한 세컨드리 포트에 대한 연결에도 모든 임시 포트에 대한 Any 액세스 권한을 부여하는 정책은 보안상 안전하지 않습니다.

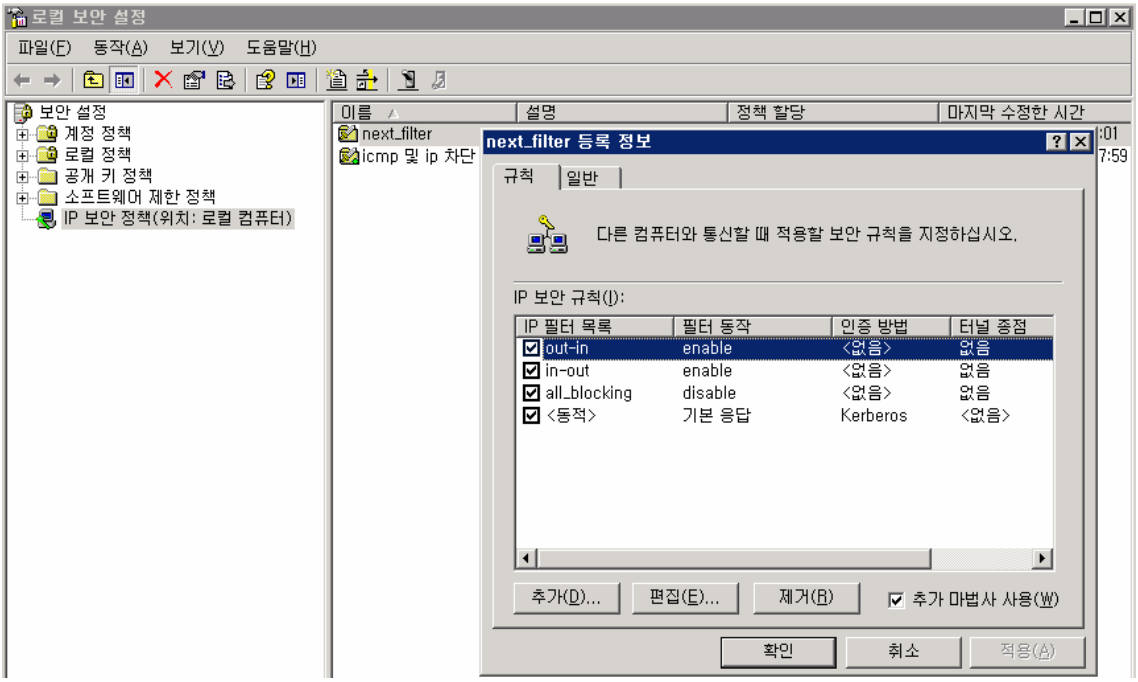
IIS 6.0 에서는 이러한 부분을 해결을 할 수 있게 해줍니다. windows 방화벽을 올린 상태 또는 일반 방화벽을 올린 상태에서 모두 동일하게 적용이 됩니다.

먼저 IIS 6.0 이 랜덤하게 포트를 열수 있는 포트 범위를 준비합니다.

5001-5005 번까지 5 개의 포트를 준비 하였습니다. 추가로 사용하지 않는 포트 구성이 가능합니다.

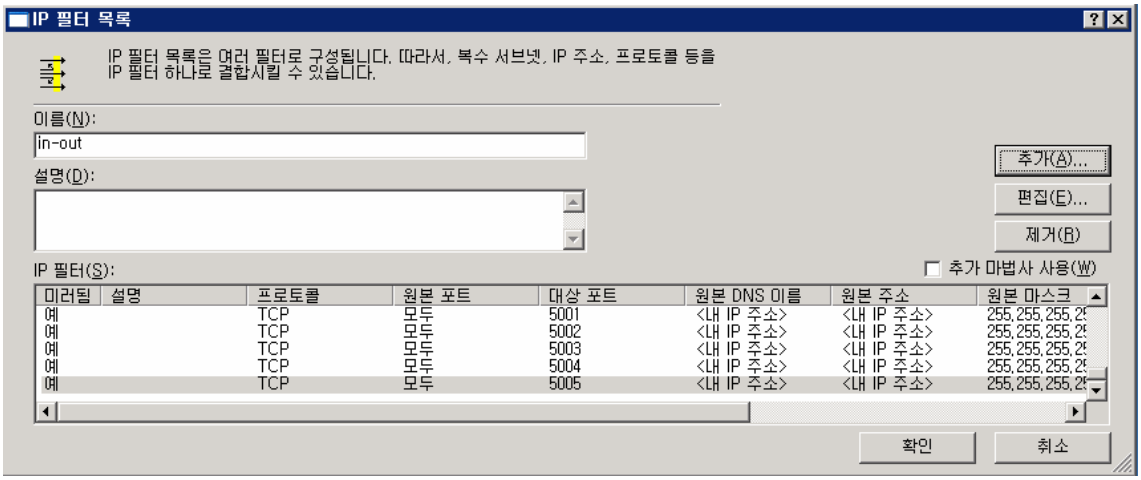
1. next_firewall 방화벽을 가지고 설명을 드리겠습니다.

1) 아래와 같이 “시작 > 관리도구 > 로컬보안정책 > next_filter” 를 오픈하여 out-in / in-out 에 해당 port를 open 해줍니다.

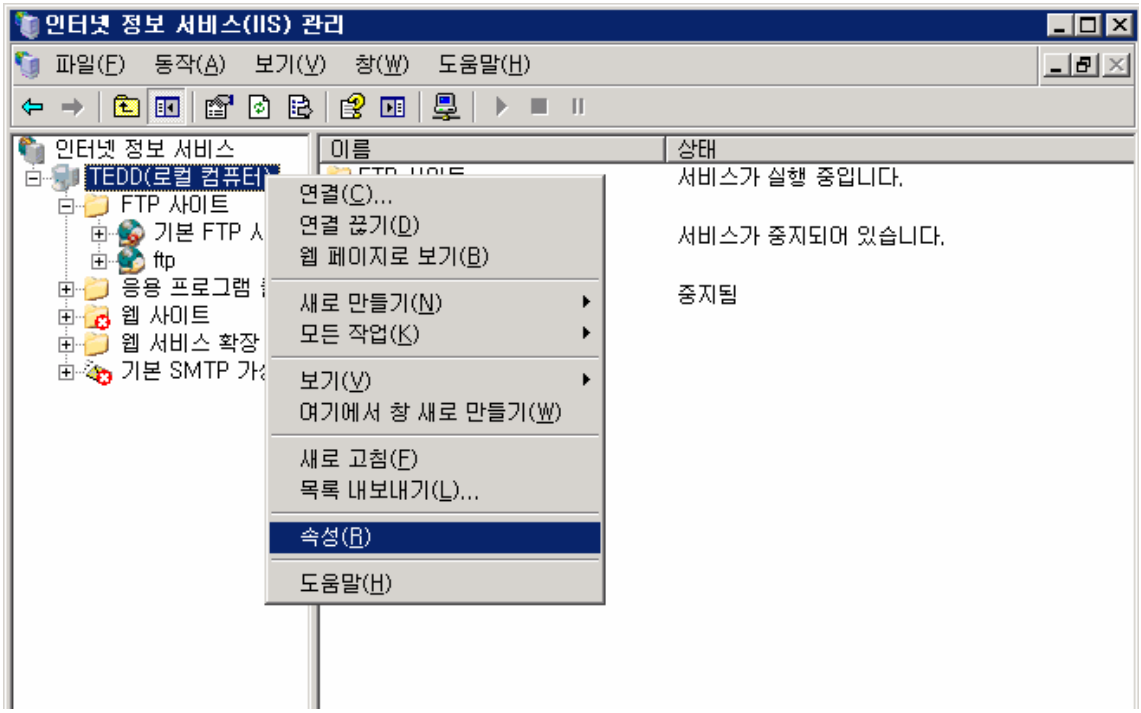


2)위와 같이 5개가 등록이 된것을 확인합니다.

(방화벽에서 사용하고자 하는 port를 오픈하는 작업 입니다. 자세한 nett_filter 설정 방법은 “넥스트라인 > 고객지원 > 기술문서 > 윈도우 보안지침 매뉴얼” 을 참고하시기 바랍니다.)

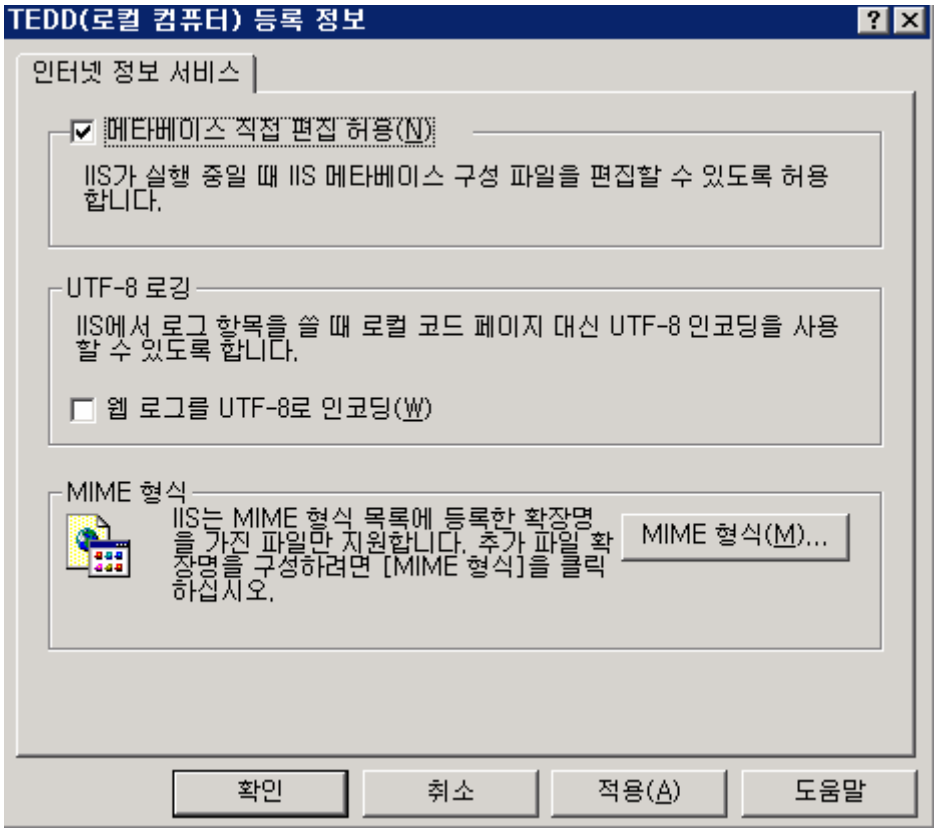


3) “시작 > 관리도구 > 인터넷 정보 서비스 관리” 를 엽니다.



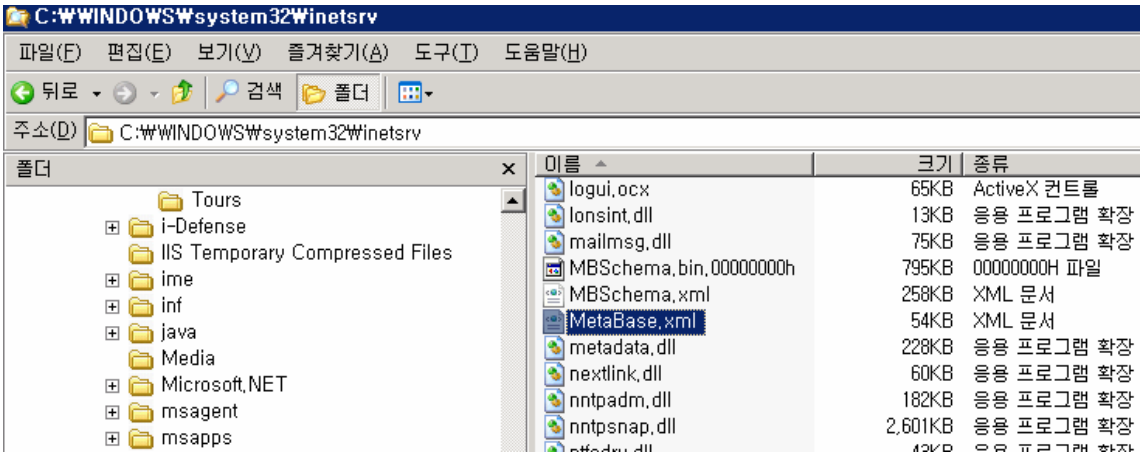
4) 서버를 선택하고 속성을 누르면 다음과 같은 화면이 나옵니다.

인터넷 정보 서비스 > 메타베이스 직접 편집 허용 에 체크를 해줍니다.



5) 아래 경로로 이동 후 Metabase.xml 파일을 메모장으로 오픈 합니다.

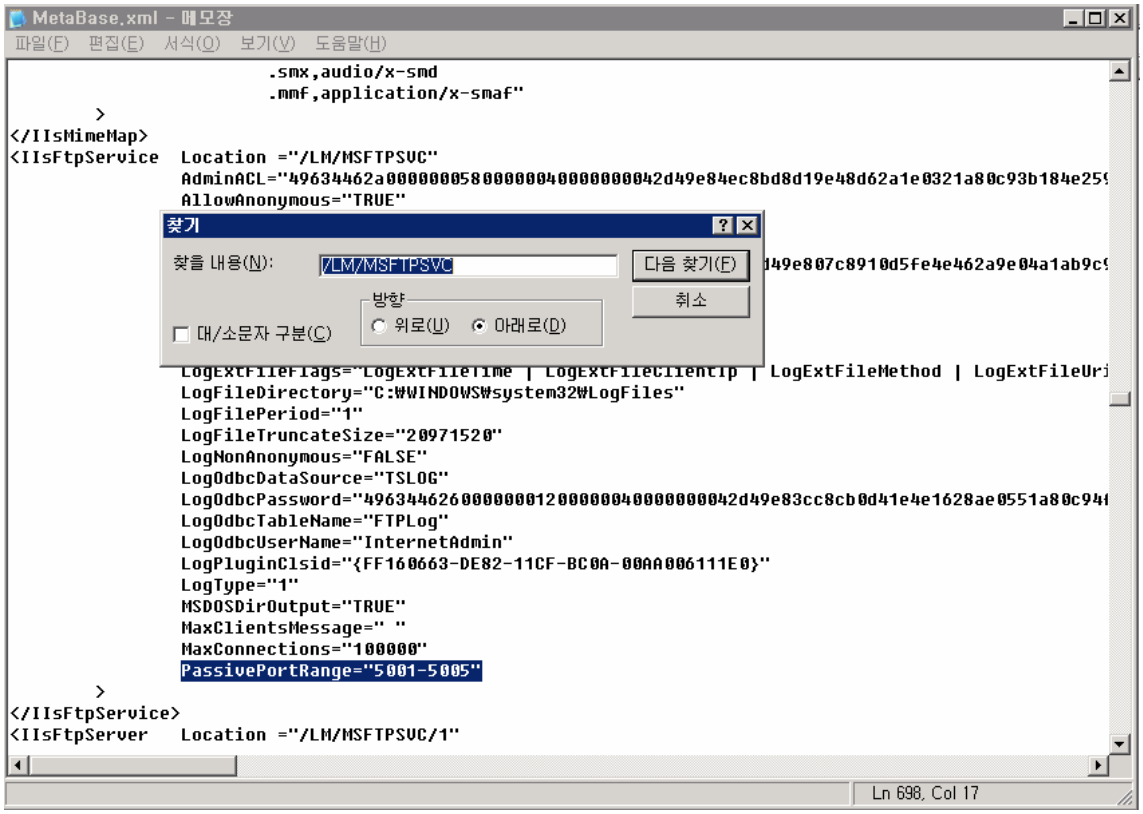
C:₩windows₩system32₩inetsrv₩Metabase.xml



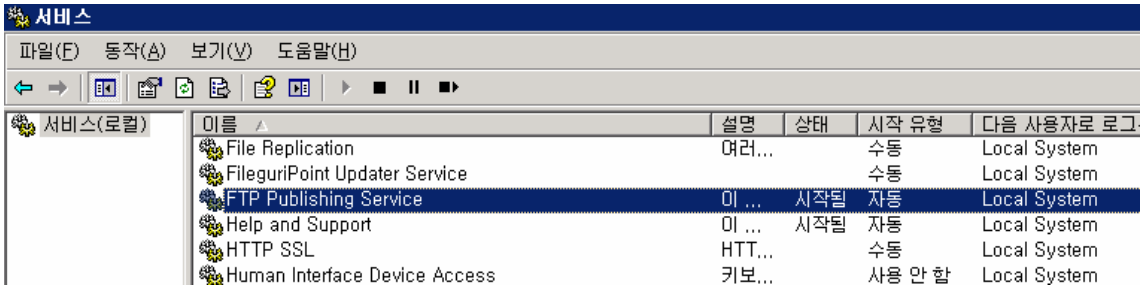
6) 찾기로 “LM/MSFTPSVC” 를 입력하고 찾기를 누릅니다.

그런 다음 MaxConnectiions="100000" 아래에 다음과 같이

PassivePortRange="5001-5005" 을 입력을 합니다.



7) 시작 > 관리도구 > 서비스 > FTP 서비스를 재시작을 누릅니다.



8) FTP 클라이언트로 접근해보시면 액티브 모드 와 패시브 모두 두개다 접근이 이루워 집니다.

IIS에서는 모두 1024 - 65535의 임시 포트 범위를 허용하도록 구성할 수 있습니다.
5000 이상의 TCP 포트에 연결하려는 경우 발생할 수 있는 문제에 대한 자세한 내용은 Microsoft 기술 자료의 다음 문서를 참조하시길 바랍니다.

http://support.microsoft.com/kb/323446/ko
http://support.microsoft.com/kb/309816/ko

2. 추가적으로 Windows Server 2003 의 경우 ADSUTIL을 이용하는 방법이 있습니다.
Adsutil.vbs set /MSFTPSVC/PassivePortRange "5001-5005"

3.Windows 2000 Server 의 경우는 레지스트리 값을 추가해야 합니다.
HKEY_LOCAL_MACHINE₩System₩CurrentControlSet₩Services₩Msftpsvc₩Parameters₩
에서 REG_SZ 타입의 PassivePortRange 값이름을 추가합니다.
값으로는, 5001-5005 을 설정합니다.

위 2가지 경우 모두 설정 후 FTP 서비스를 재시작 해야 적용되며, 위와 같이 범위 또는 특정포트값을 설정해도 됩니다.

서버에 방화벽을 운영하는 서버인데, 클라이언트가 액티브모드를 지원하지 않는경우에 적용하는 것이 좋은 해결책이 될 수 있습니다.