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 20번 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 / inout 에 해당 port를 open 해줍니다.

3) "시작 > 관리도구 > 인터넷 정보 서비스 관리"를 엽니다.

Ч./							
🔲 IP 필터	목록						? ×
	IP 필터 목록은 여긴 IP 필터 하나로 결합	네 필터로 구성됩니다 압시킬 수 있습니다.	. 따라서, 복수 서브넛	!, IP 주소, 프로토콜	등을		
이름(<u>N</u>)							
in-out							~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
설명(<u>D</u>)							<u> </u>
				<u>^</u>			편집(<u>E</u>)
				-			제거(8)
IP 필터(<u>S</u>):					주 주	
미러됨	설명	프로토콜	원본 포트	대상 포트	원본 DNS 이름	원본 주소	원본 마스크 🔺
예		TCP	보누 모두	5002	〈내 IP 주소〉 〈내 IP 주소〉	〈내 IP 주소〉 〈내 IP 주소〉	255, 255, 255, 25
0 M		TCP	몸훈	5003	갧ස춫솟	/배 旧 춫솟〉	255, 255, 255, 25
예		TCP	모두	5004	<대 IP 주소>	<대 IP 주소>	255, 255, 255, 25
•							
						확인	취소

다.)

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 바랍니

🚡 로컬 보안 설정						
파일(<u>F</u>) 동작(<u>A</u>) 보기(<u>V</u>) 도움말(<u>H</u>)						
← → 🗈 📧 🗙 😭 🗟 😫 💷	🛅 🚠 🔟 🖉					
😥 보안 설정	이름 스	설명	정책 할당	•	마지막 수정한 .	시간
┃ 표~ 계성 성책 ┃ 표~ 로컬 정책	I Inext_filter I III in 차단	next_filter 등록 정보	Ł			2×301 7:59
□		규칙 일반				
┃		C.				
		그 다른 컴	!퓨터와 통신할 때 적용	할 보안 규칙을 지	정하십시오,	
		IP 보안 규칙(]):		1		
		IP 필터 목록	- 비필터 동작 enable	<u> </u>	<u> 터널 송섬</u> 없음	
		☑ in-out	enable	<없음>	없음	
		☑ all_blocking ☑ <ছঅ,১	disable 기보 응단	<없음> Kerberos	없음 <었음>	
			7E 88	10/beres		
		•			Þ	
		추가(<u>D</u>)	편집(<u>E</u>) 제기	l(<u>B</u>) マ 本:	가 마법사 사용())	>
			확인	취소	적용(<u>A</u>)	

🌘 인터넷 정보 서비스(IIS	S) 관리		
👣 파일(E) 동작(<u>A</u>) 보	.기(⊻) 창(₩) 도움말(표)		_ B ×
⇐ ⇒ 🔁 🖬 😭 📀	🖹 😫 🖬 💂 🕨 🗉 🗉		
🍋 인터넷 정보 서비스		상태	
이 모·종이 TEUD(로칠 컴퓨터) 고·승이 FTP 사이트	연결(<u>C</u>)	서비스가 실행 중입니다.	
	연결 끊기(<u>D</u>) 웹 페이지로 보기(<u>B</u>)	서비스가 중지되어 있습니다.	
Ē~) 응용 프로그램 (Ē~ <mark>ゐ</mark> 웹 사이트	새로 만들기(N)	- 중지됨	
▲ (▲) 웹 서비스 확장 	모든 작합(<u>N</u>) ·	-	
E-45 NE SMILE 215	보기(⊻) 여기에서 창 새로 만들기(<u>₩</u>)		
	새로 고침(E) 모르 미니미기(1)		
	폭독 대모대기(<u>L</u>)	_	
	속성(<u>R</u>)		
	도움말(<u>H</u>)		
		—	

4) 서버를 선택하고 속성을 누르면 다음과 같은 화면이 나옵니다.

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

TEDD(로컬 컴퓨터) 등록 정보 ? 🔉						
인터넷 정보 서비스						
✓ 메타베이스 직접 편집 허용(N) IIS가 실행 중일 때 IIS 메타베이스 구성 파일을 편집할 수 있도록 허용 합니다.						
UTF-8 로깅 IIS에서 로그 항목을 쓸 때 로컬 코드 페이지 대신 UTF-8 인코딩을 사용 할 수 있도록 합니다.						
MIME 형식 IIS는 MIME 형식 목록에 등록한 확장명 을 가진 파일만 지원합니다. 추가 파일 확 장명을 구성하려면 [MIME 형식]을 클릭 하십시오.						
<u>확인</u> 취소 적용(<u>A</u>) 도움말						

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

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

🚝 C:\WINDOWS\#system32\Winetsrv							
파일(E) 편집(E) 보기(⊻) 즐겨찾기(<u>A</u>) 도구(I) 도움말(∐)							
③ 뒤로 ▾ ④ ▾ 秒 🔎 검색 📂 폴더 │ ॑॑							
주소(D) 🛅 C:\WINDOWS\#system32\#inetsrv							
폴더	x 이름 ▲	크기 종류					
 ☐ Tours ☐ i-Defense ☐ IIS Temporary Compressed Files ☐ ime ☐ inf ☐ java ☐ Media ☐ msagent 	 logui, ocx lonsint, dll mailmsg, dll MBSchema, bin, 00000000h MBSchema, xml MetaBase, xml metadata, dll nextlink, dll nntpadm, dll nntpsnap, dll 	65KB ActiveX 컨트롤 13KB 응용 프로그램 확장 75KB 응용 프로그램 확장 795KB 00000000H 파일 258KB XML 문서 54KB XML 문서 228KB 응용 프로그램 확장 60KB 응용 프로그램 확장 182KB 응용 프로그램 확장 2,601KB 응용 프로그램 확장					

6) 찾기로 "LM/MSFTPSVC"를 입력하고 찾기를 누릅니다.

그런 다음 MaxConnectiions="100000" 아래에 다음과 같이

PassivePortRange="5001-5005" 을 입력을 합니다.

関 MetaBase, xml	- 메모장	
파일(<u>F</u>) 편집(<u>E</u>)	서식(<u>O</u>) 보기(<u>V</u>) 도움말(<u>H</u>)	
	.smx,audio/x-smd	_
	.mmf,application/x-smaf"	
//IcMimoMan>		
<iisftpservice< th=""><th>Location ="/LM/MSFTPSVC"</th><th></th></iisftpservice<>	Location ="/LM/MSFTPSVC"	
	AdminACL="49634462a0000005800000400000042d49e84ec8bd8d19e4 AllowAnonumous="TRUE"	8d62a1e0321a80c93b184e25{
	찾기 ? ×	
	찾을 내용(<u>N</u>): 기보께/MSHTPSVC 다음 찾기(E) 149e807ct	8910d5fe4e462a9e04a1ab9c\$
	▷ 명호 취소 □ 대/소문자 구분(C) ○ 위로(U) ○ 아래로(D)	_
	INDEXTELIEFIANS="INDEXTELLEDING I INDEXTELLEDING I INDEXTEL	ileMethod ooFxtFileUri
	LogFileDirectory="C:#WINDOWS#system32#LogFiles"	
	LogFilePeriod="1"	
	LogFileTruncateSize="20971520"	
	LogNonAnonymous- FALSE LogNonAnonymous- FALSE	
	LogOdbcPassword="4963446260000000120000004000000042d49e83cc8c	b0d41e4e1628ae0551a80c94i
	LogOdbcTableName="FTPLog"	
	LogOdbcUserName="InternetAdmin"	
	LogPluginClsid="{FF160663-DE82-11CF-BC0A-00AA006111E0}"	
	LogType="1" HSDASDiventation HTDHSH	
	MaxClientcMeccane=" "	
	MaxConnections="188888"	
	PassivePortRange="5001-5005"	
>		
<th></th> <th></th>		
<11sFtpServer	LOCATION ="/LM/MSFIPSVC/1"	_
•		Þ
		Ln 698, Col 17 🥢

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

🎭 서비스					
파일(<u>F</u>) 동작(<u>A</u>)	보기(⊻) 도움말(표)				
	〕 ₴ 😫 छ ▶ ■ ॥ ■>				
🎭 서비스(로컬)	이름 🔺	설명	상태	시작 유형	다음 사용자로 로그
	🖏 File Replication	여러		수동	Local System
	🐝 FileguriPoint Updater Service			수동	Local System
	FTP Publishing Service	0	시작됨	자동	Local System
	🖏 Help and Support	0	시작됨	자동	Local System
	HTTP SSL	HTT		수동	Local System
	🏽 🍇 Human Interface Device Access	키보		사용 안 함	Local System

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

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 특 정포트값을 설정해도 됩니다.

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