랜섬웨어 조치방법

㈜컴퓨터메이트

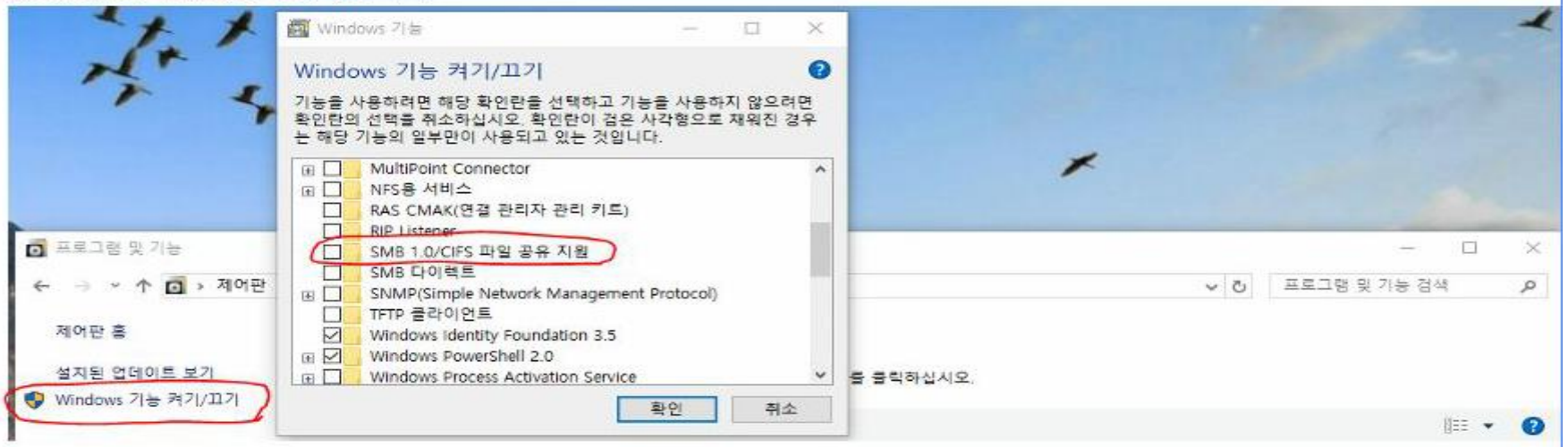
1. 보안에 취약한 OS 목록

OS
Windows Vista
Windows Server 2008
Windows 7
Windows Server 2008 R2
Windows 8.1
Windows Server 2012 and Windows Server 2012 R2
Windows RT 8.1
Windows 10
Windows Server 2016
Windows Server Core installation option

2. 윈도우 기능 사용안함 설정

랜섬웨어 - 워너크라이 예방

2017년 5월 14일 일요일
오후 8:10

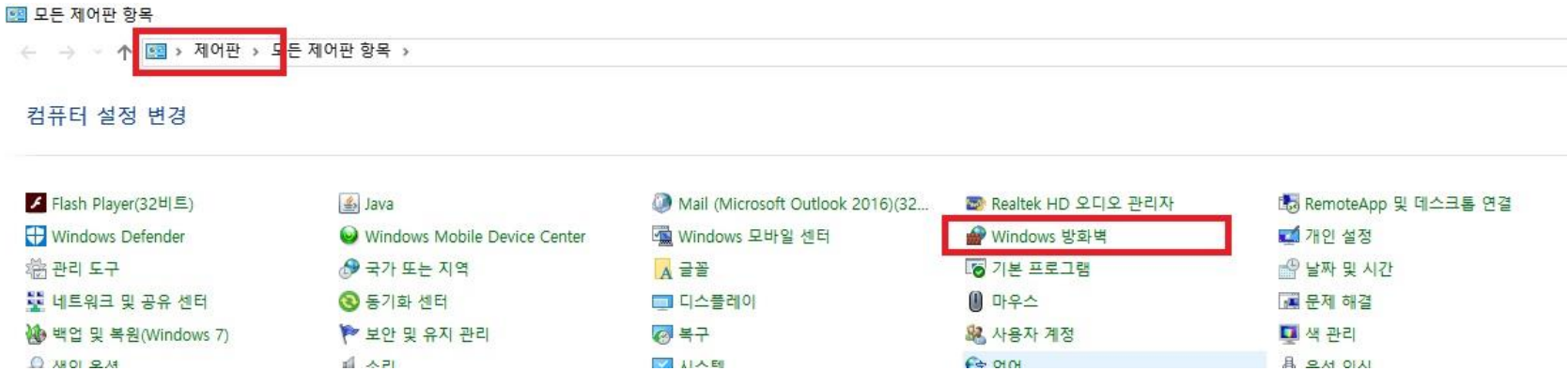
1. 제어판 > 프로그램 추가/제거 > Windows 기능 켜기/끄기
2. SMB 1.0/CIFS 파일 공유지원 체크 해제
3. 

+@. SMB 관련포트
1) UDP 137, 138
2) TCP 139, 445

+@. 관련 보안 패치(지원 중단된 윈도우 XP 등)
http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

3. 포트차단설정

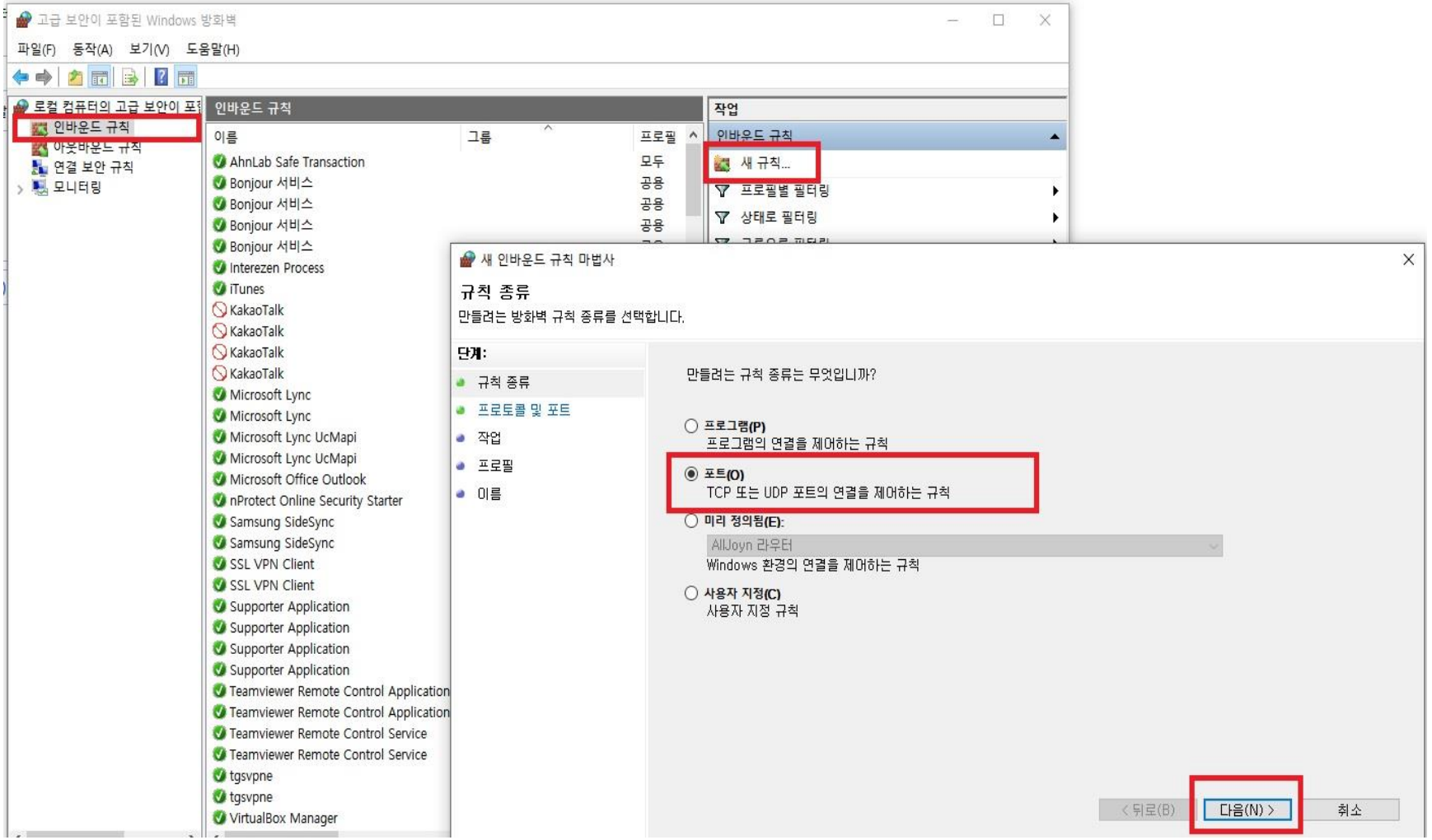
1. [제어판] - [Windows 방화벽] 선택



2. [고급설정]선택

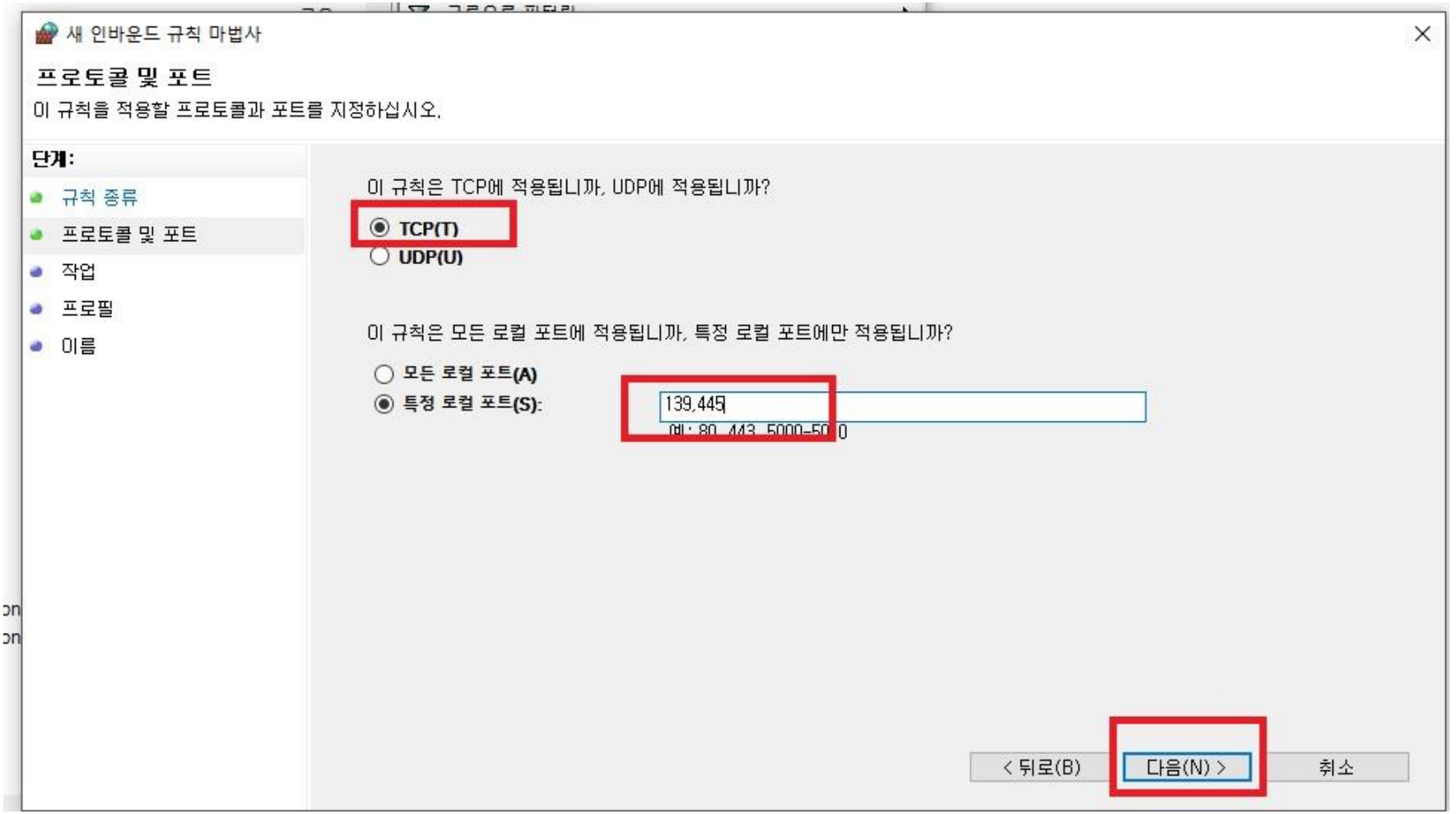
3. 포트차단설정

3. [인바운드규칙] - [새규칙] 선택, 규칙마법사가 뜨면 [포트]선택하고 [다음]버튼 선택



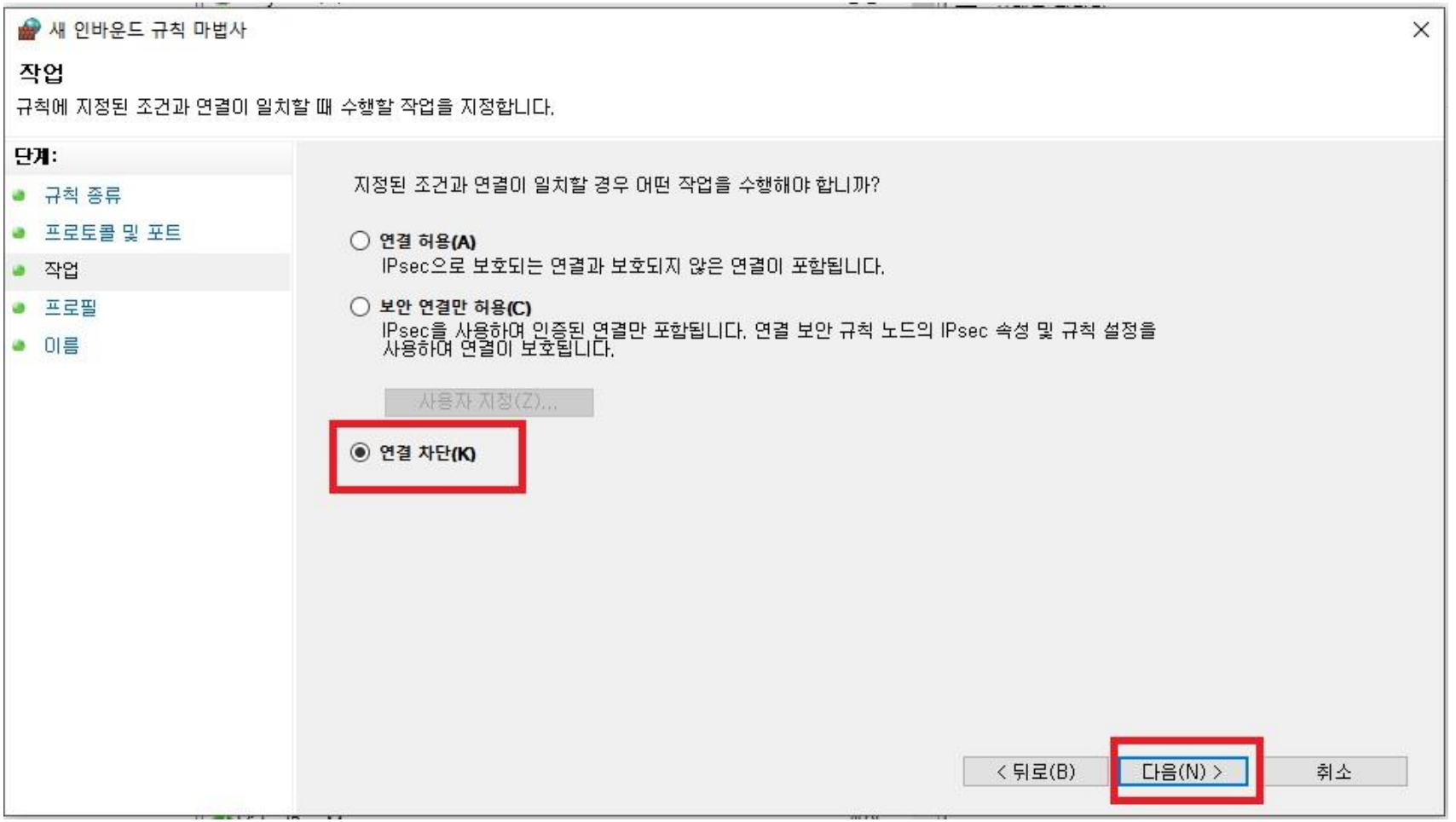
3. 포트차단설정

4. [TCP(T)] 선택, 아래에 특정로컬포트(S)에 139, 445를 입력한 후 [다음]버튼선택



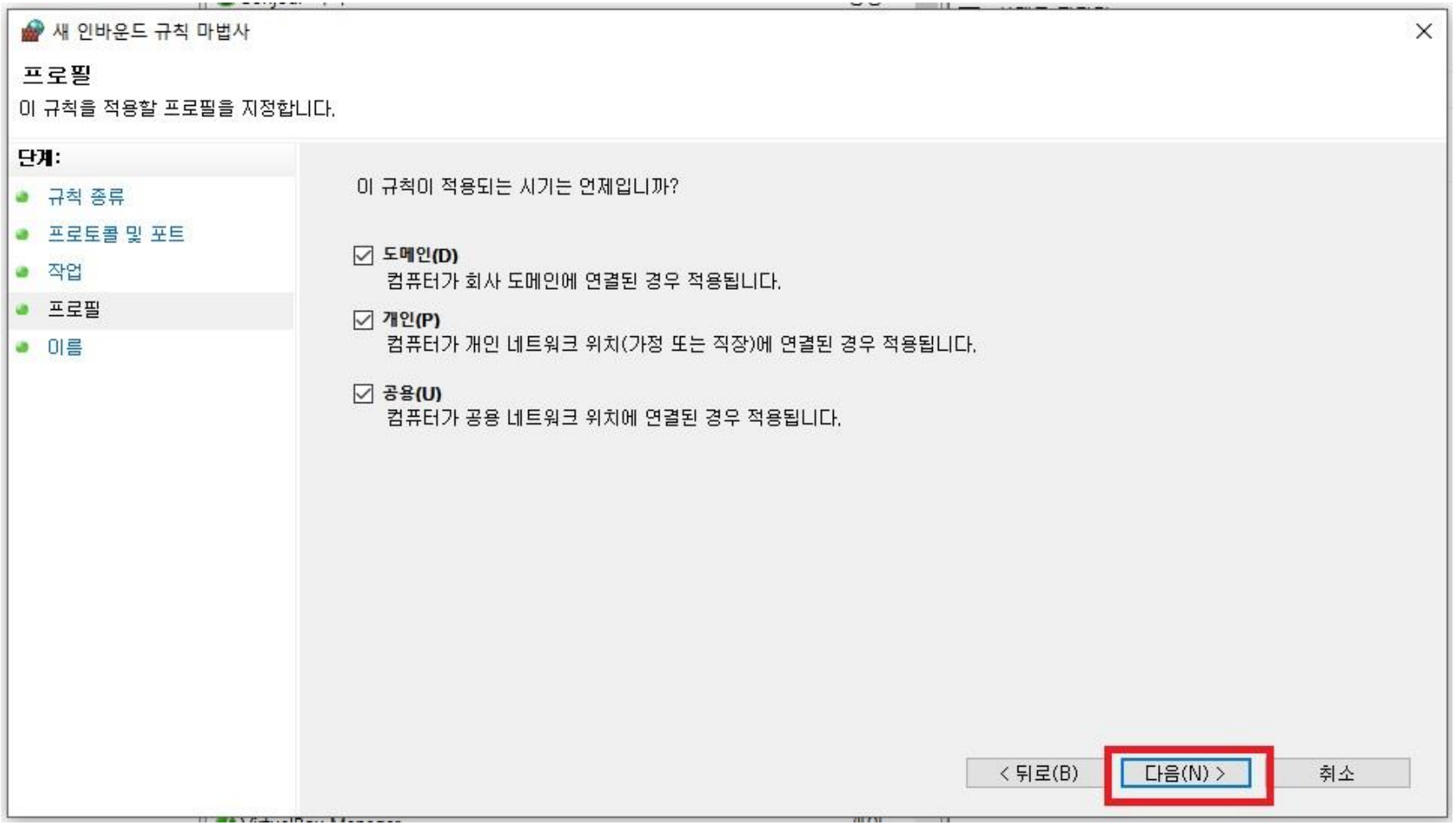
3. 포트차단설정

5. [연결차단]을 선택



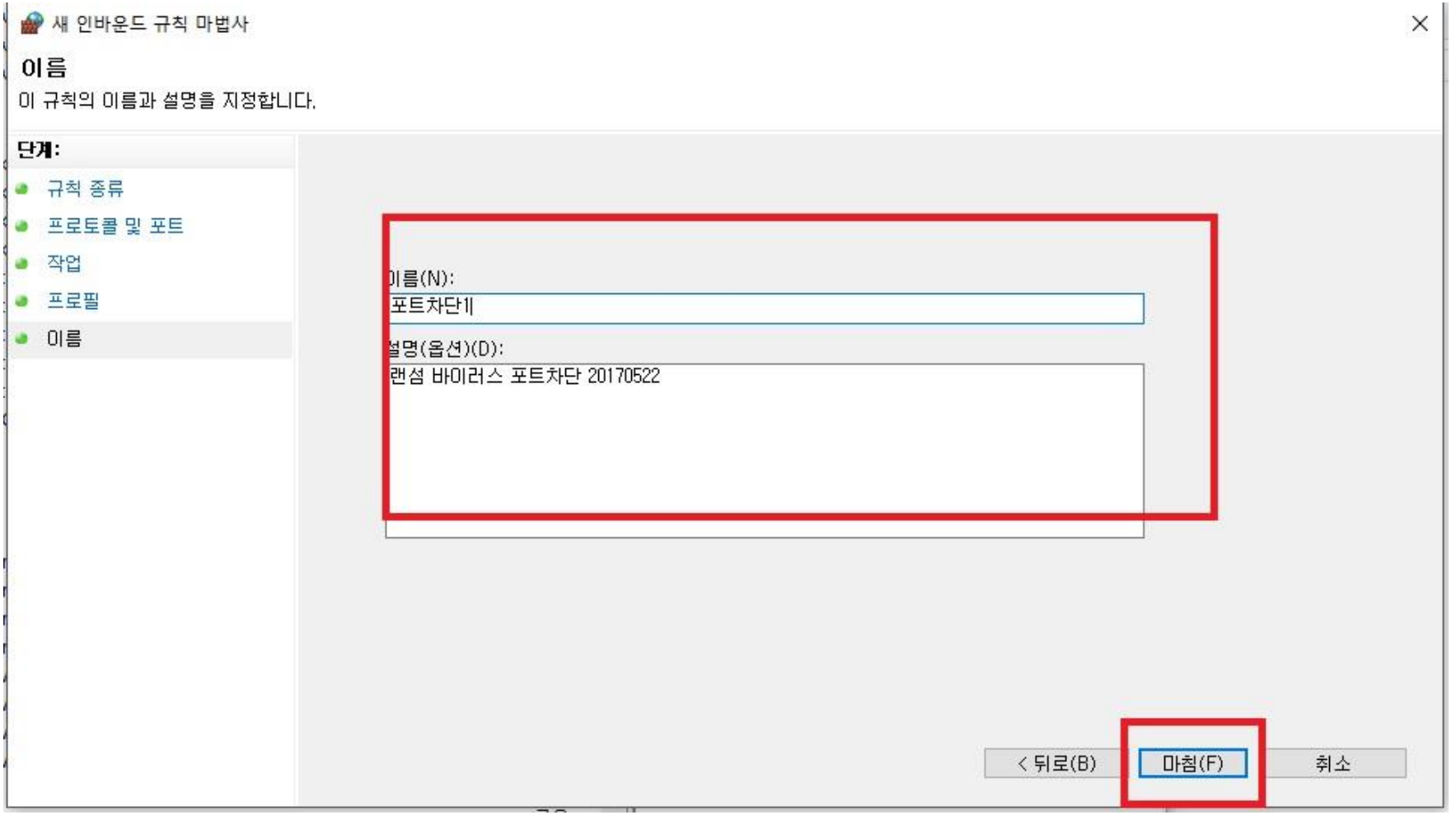
3. 포트차단설정

6. [다음] 선택



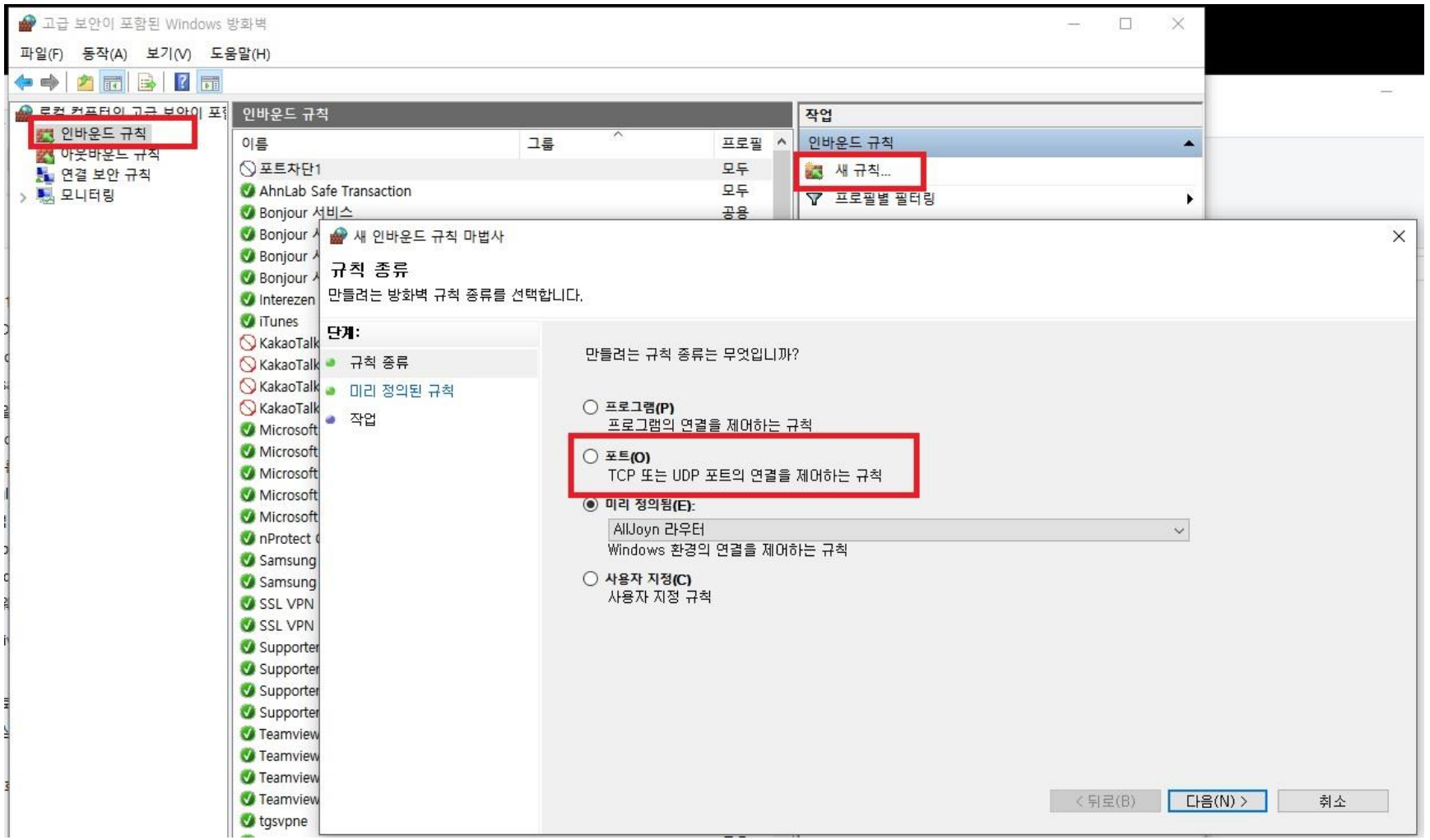
3. 포트차단설정

7. 아래 내용과 같이 입력 한 후 [마침] 선택



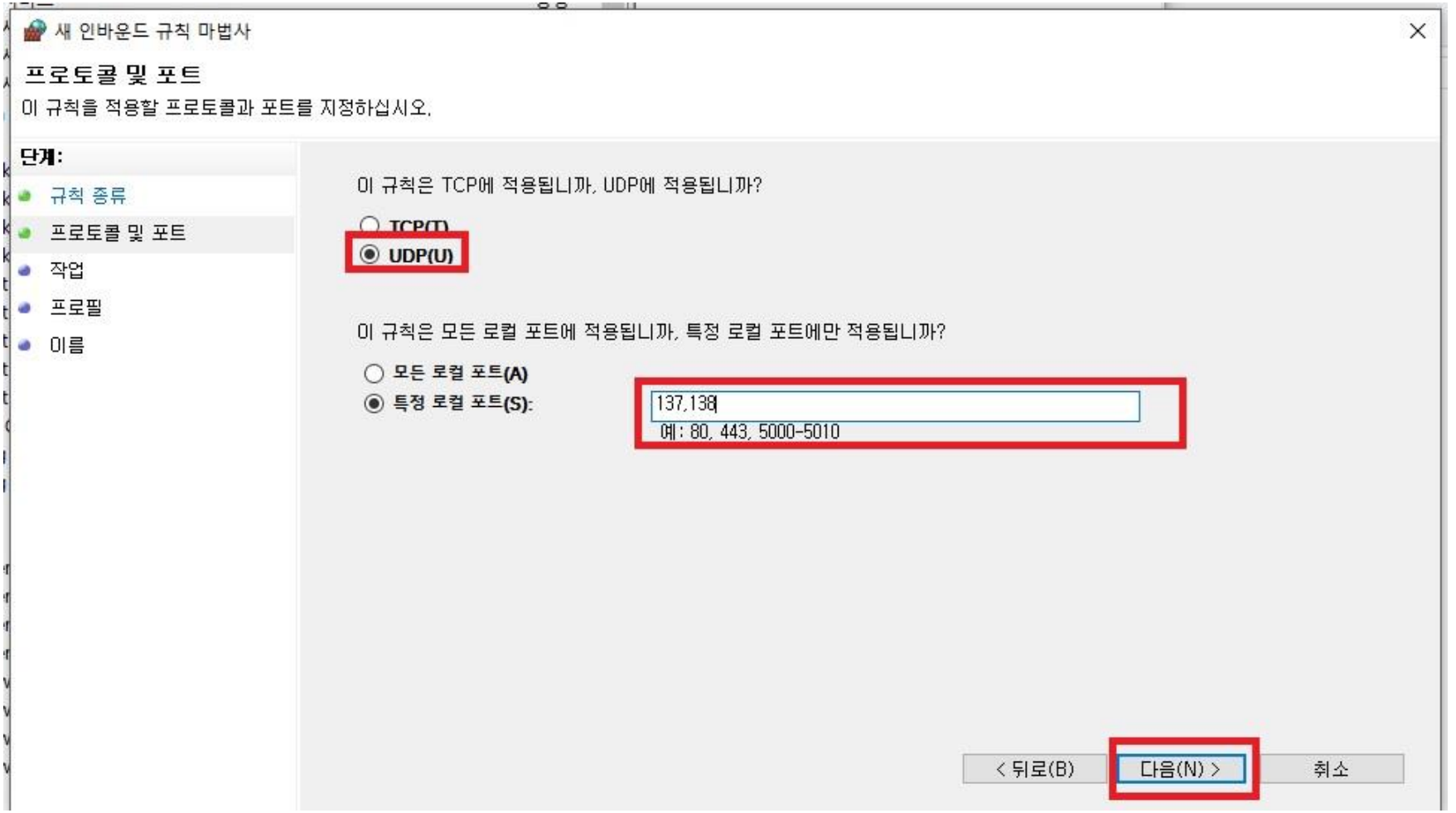
3. 포트차단설정

8. [인바운드규칙]-[새규칙] 선택 후 [포트]선택 후 [다음] 버튼 선택



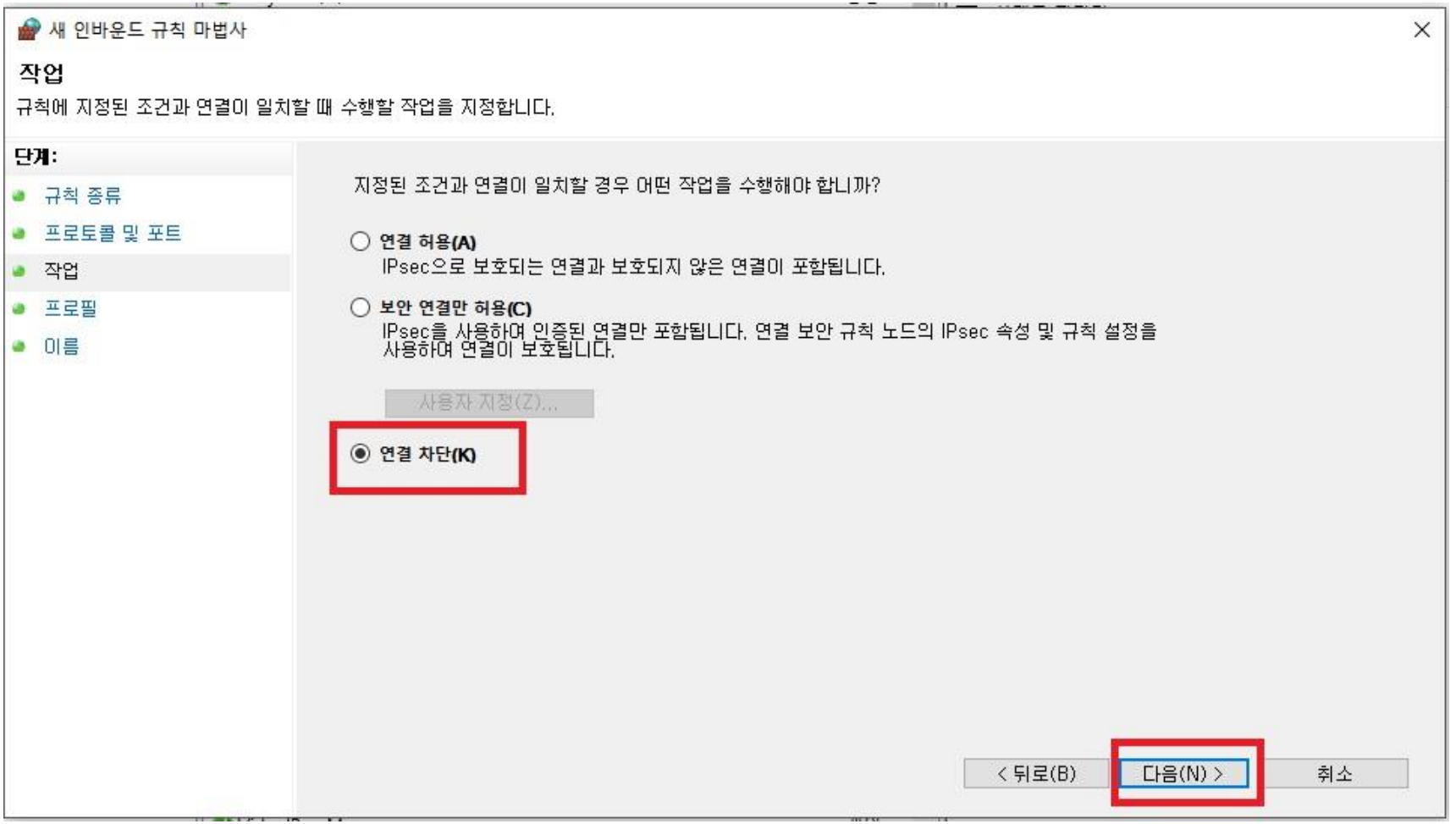
3. 포트차단설정

9. [UDP(U)] 선택 후 특정로컬포트(S)에 137,138 을 입력 후 [다음]버튼선택



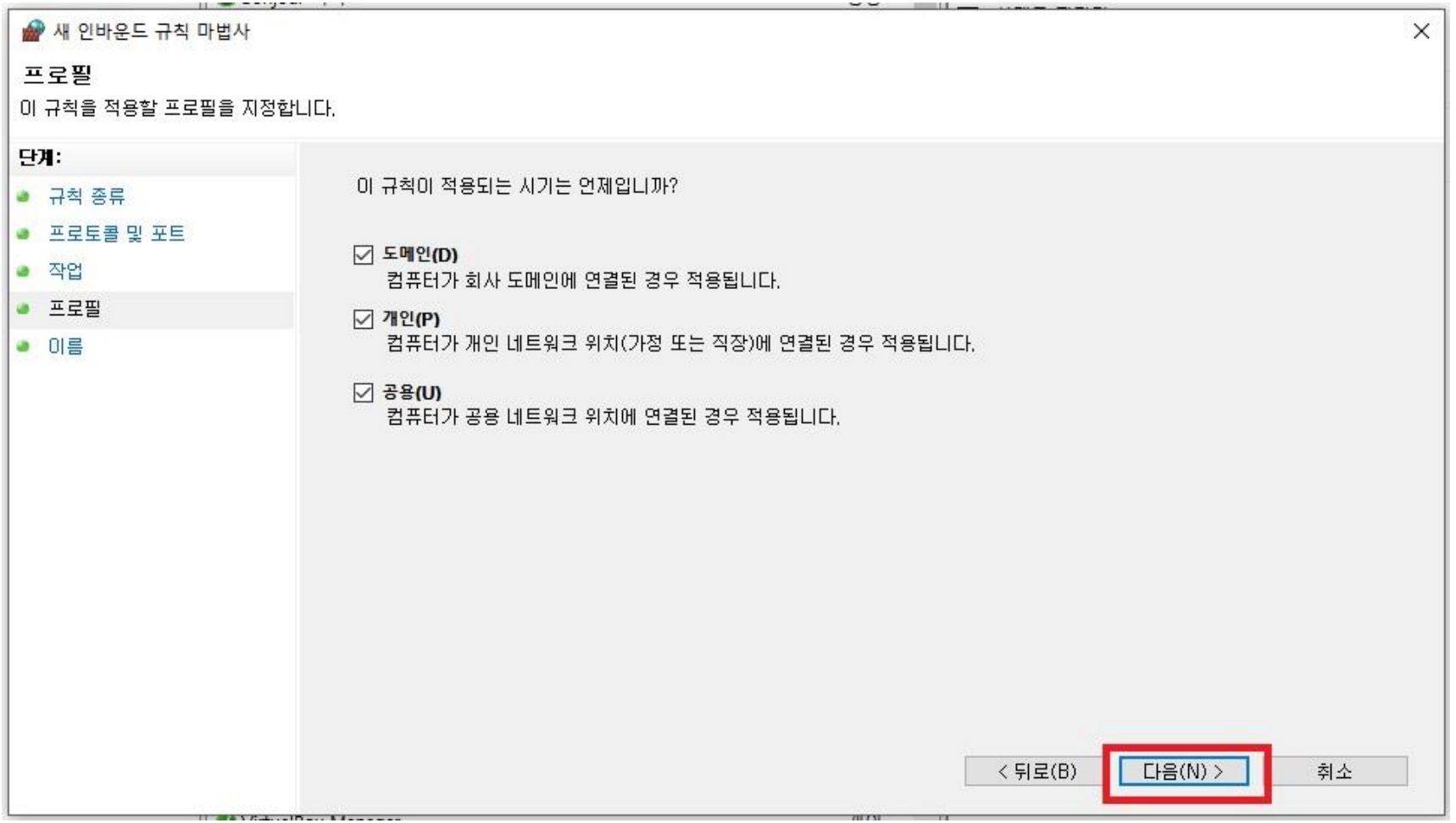
3. 포트차단설정

10. [연결차단]을 선택



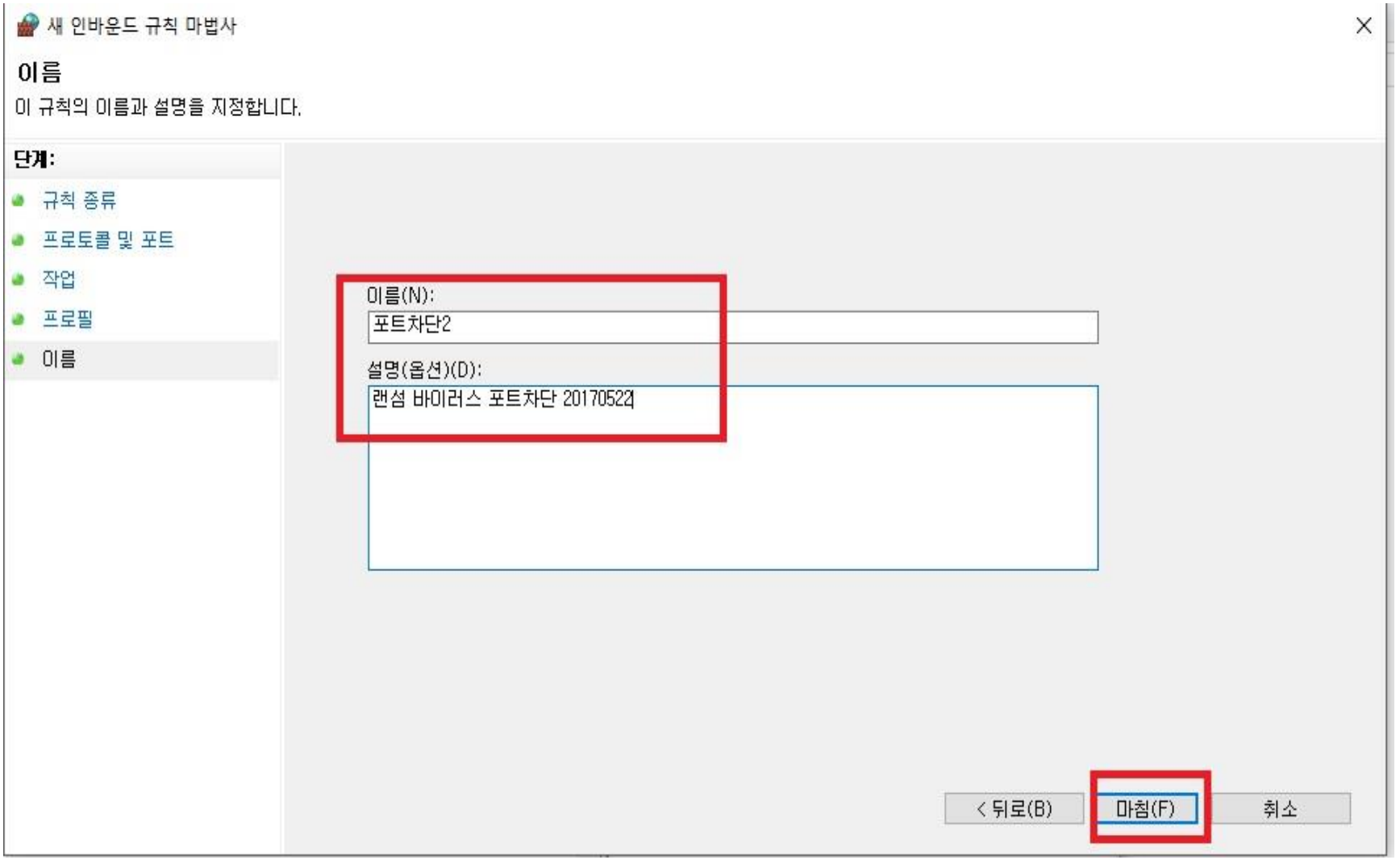
3. 포트차단설정

11. [다음] 선택



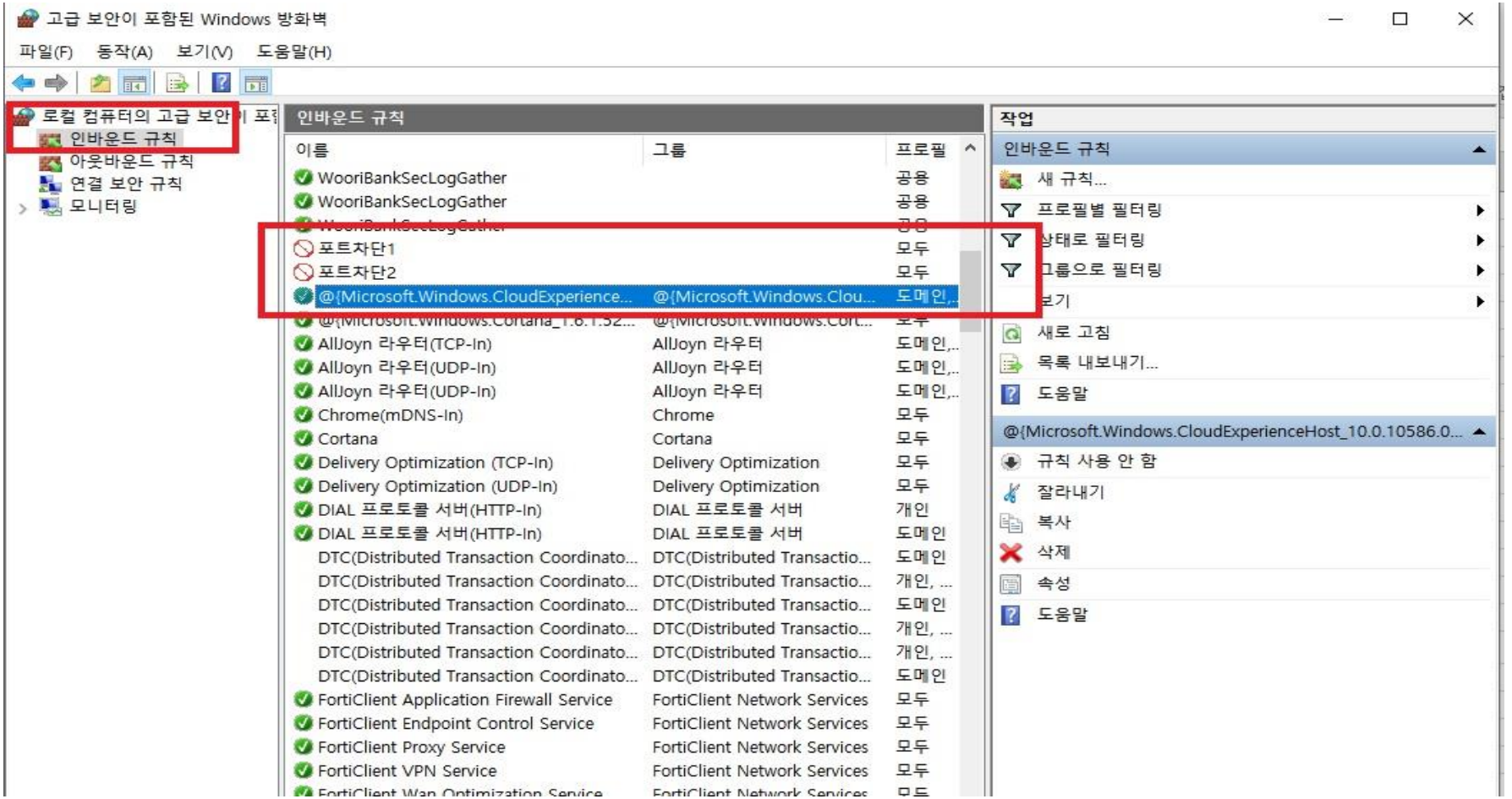
3. 포트차단설정

12. 아래 내용과 같이 입력 한 후 [마침] 선택



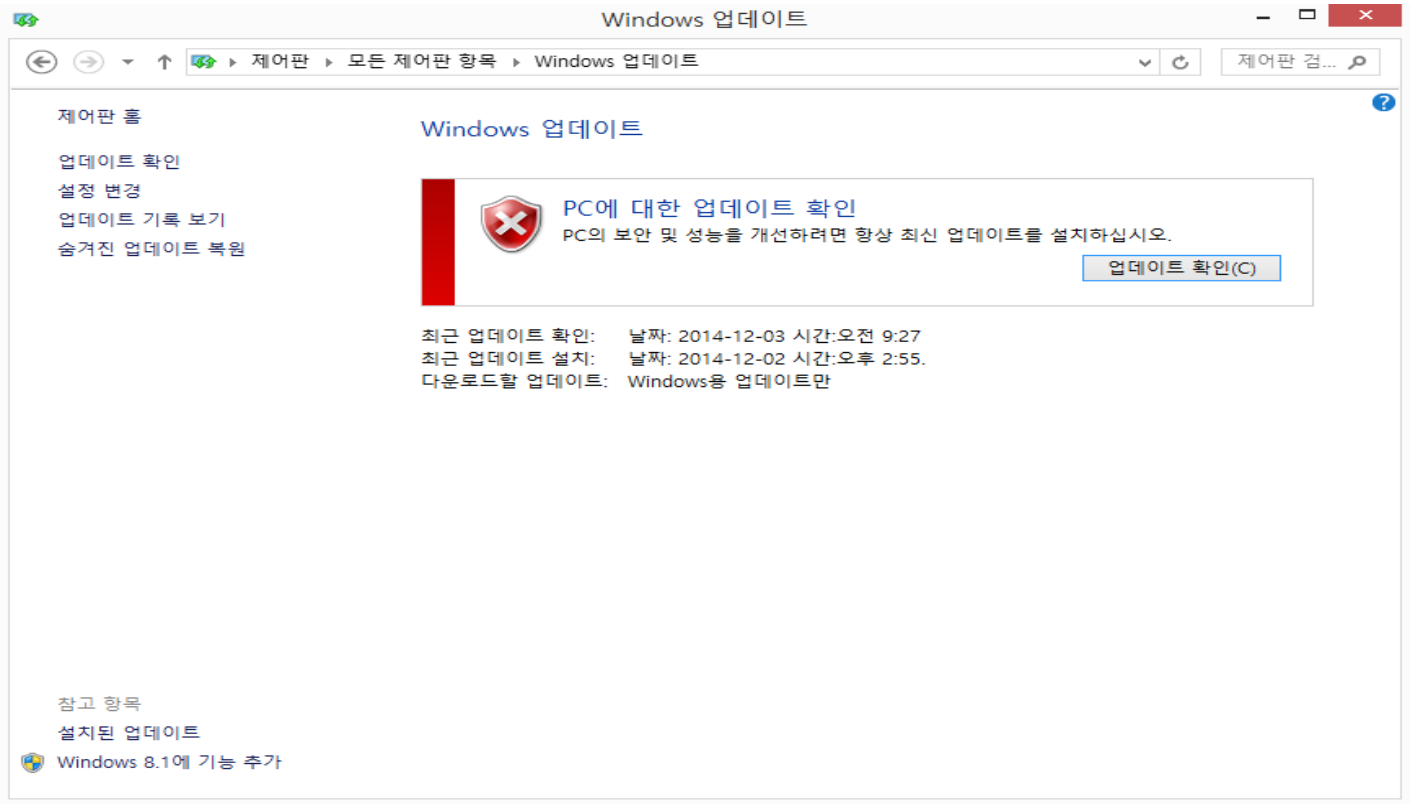
3. 포트차단설정

13. 아래 처럼 포트차단1, 포트차단2가 추가 되었는지 확인



14. [인바운드 규칙]과 동일한 방법으로 [아웃바운드규칙]도 포트차단1,2를 추가시켜주면 된다.

4. 윈도우 업데이트 실행



1. 윈도우 업데이트 이후 재부팅
2 .윈도우 기능 사용안함 살림
3. 포트 차단내역 삭제