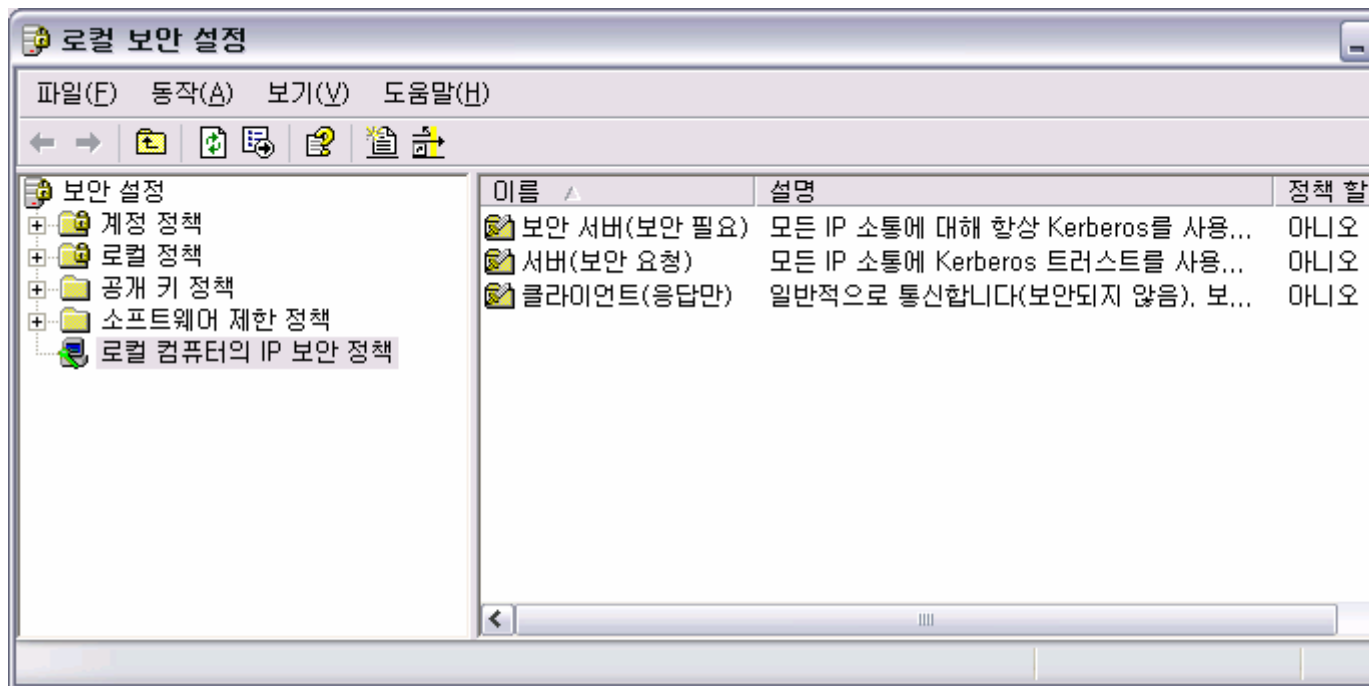
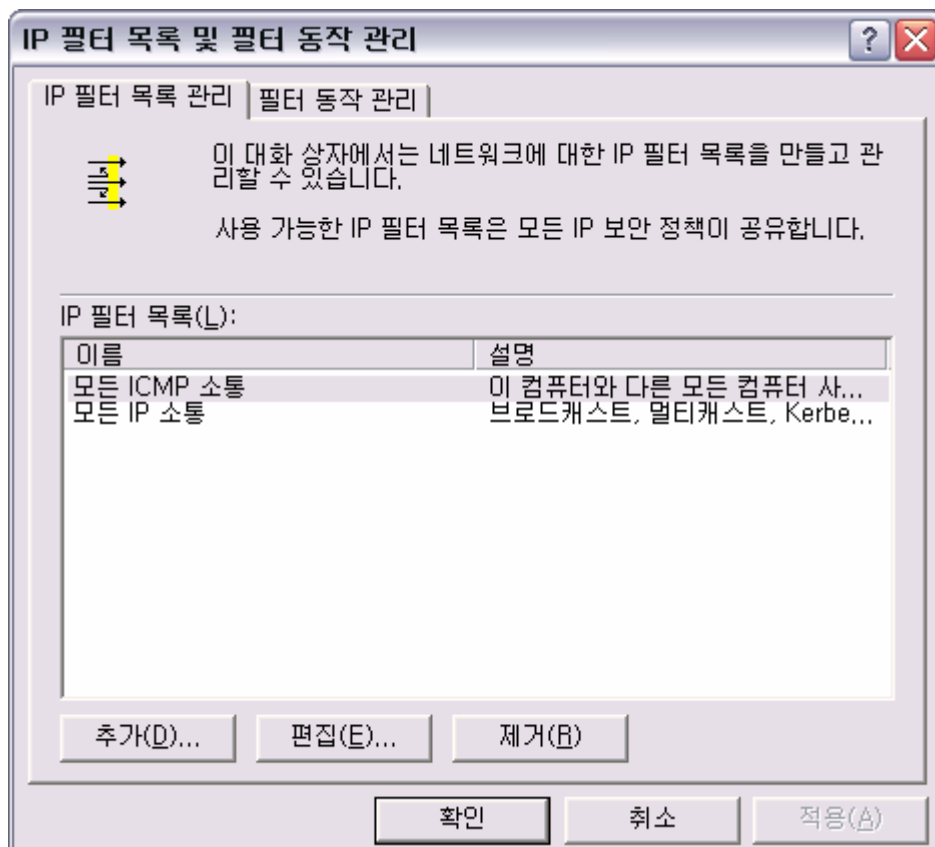


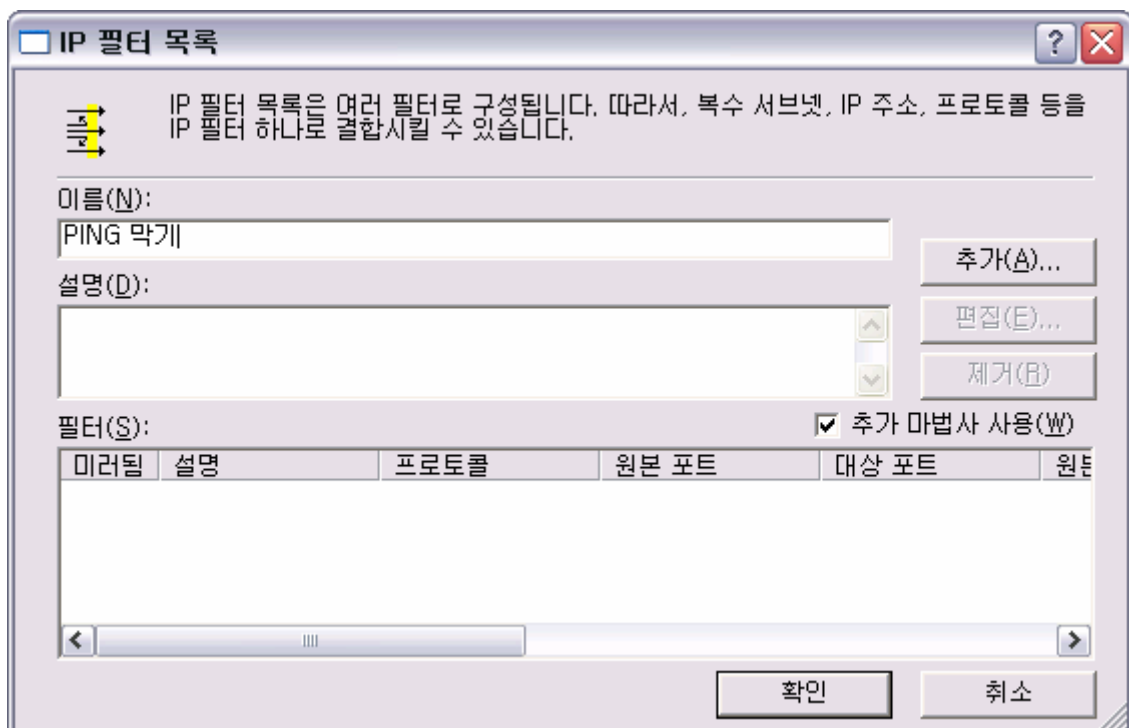
IPSEC (PING)



IP -> IP



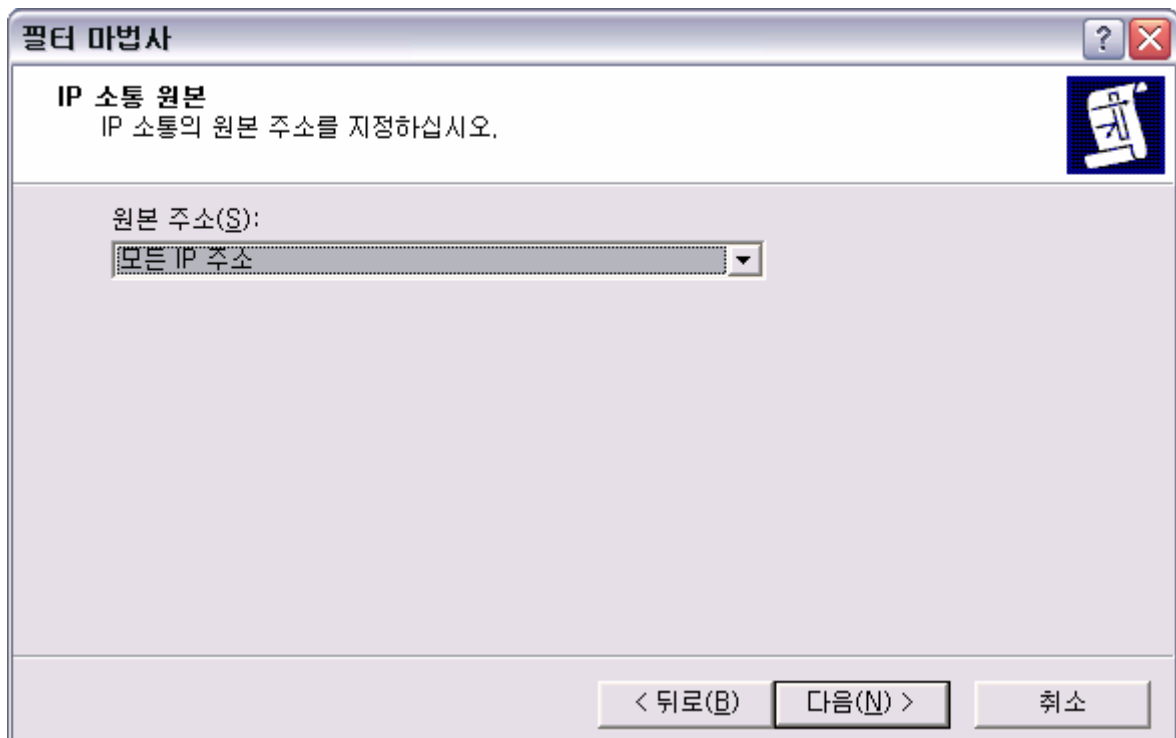
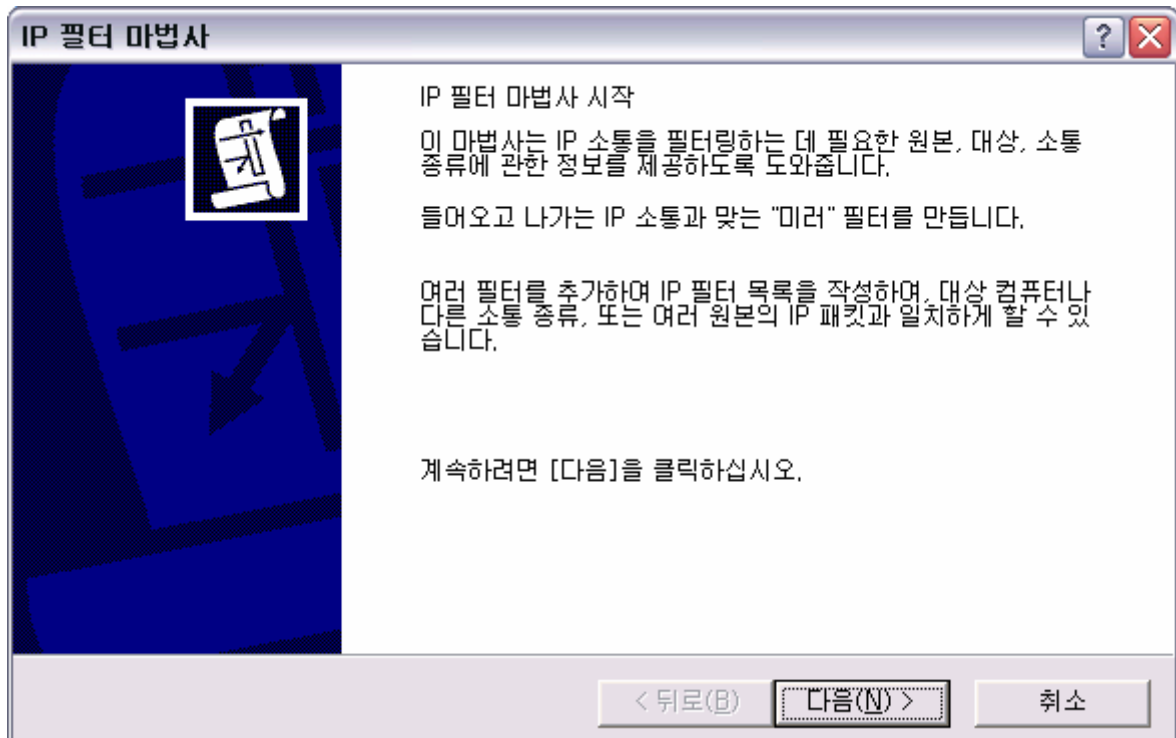
가



PING

가

.



IP

.

필터 마법사 [?] [X]

IP 소통 대상
IP 소통의 대상 주소를 지정하십시오.

대상 주소(D):
[대 IP 주소 ▼]

< 뒤로(B) 다음(N) > 취소

IP

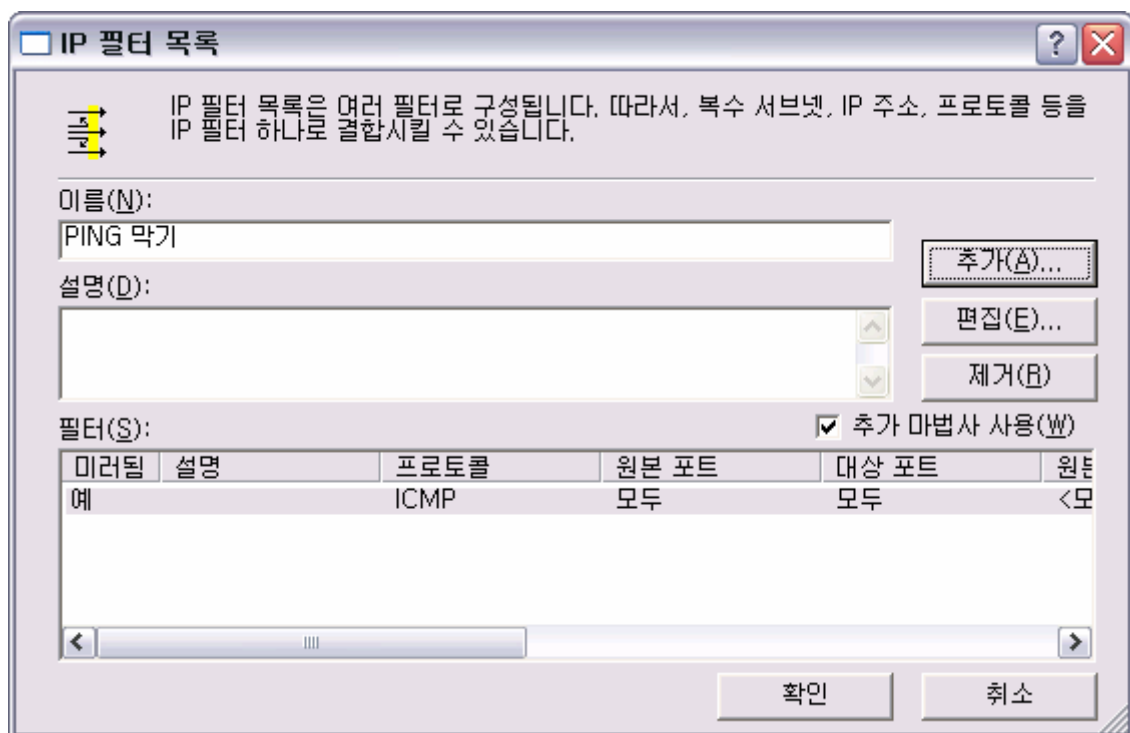
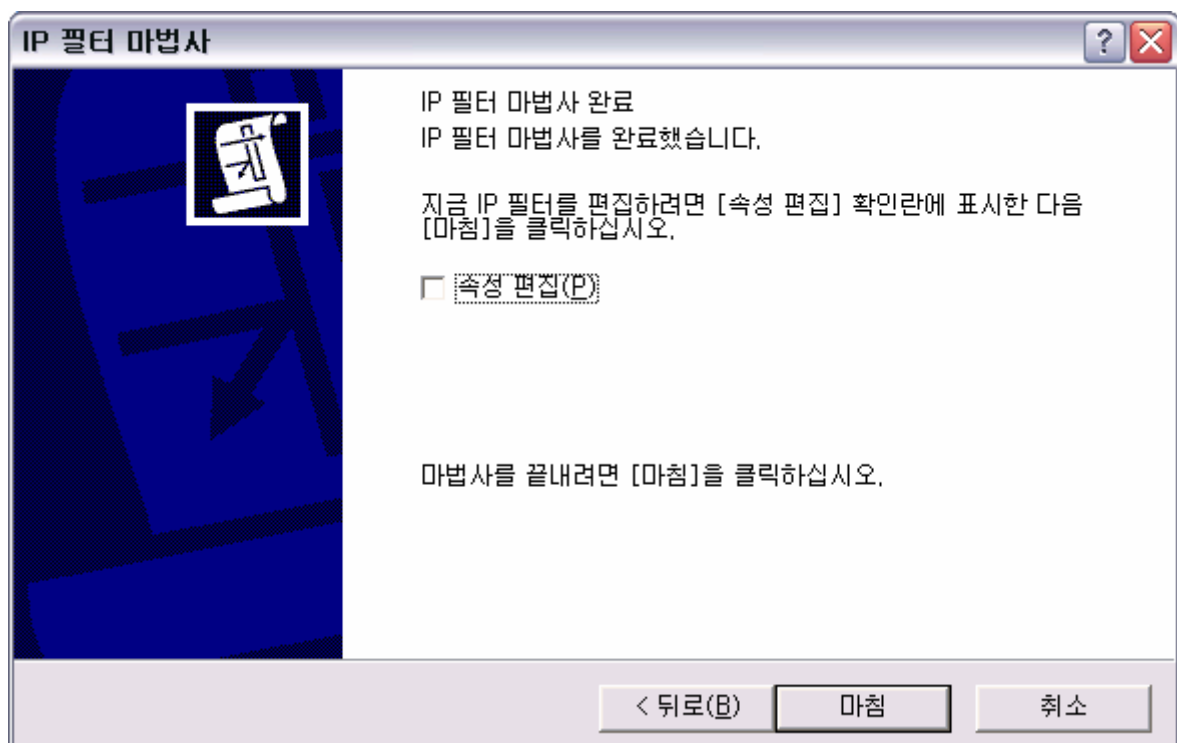
필터 마법사 [?] [X]

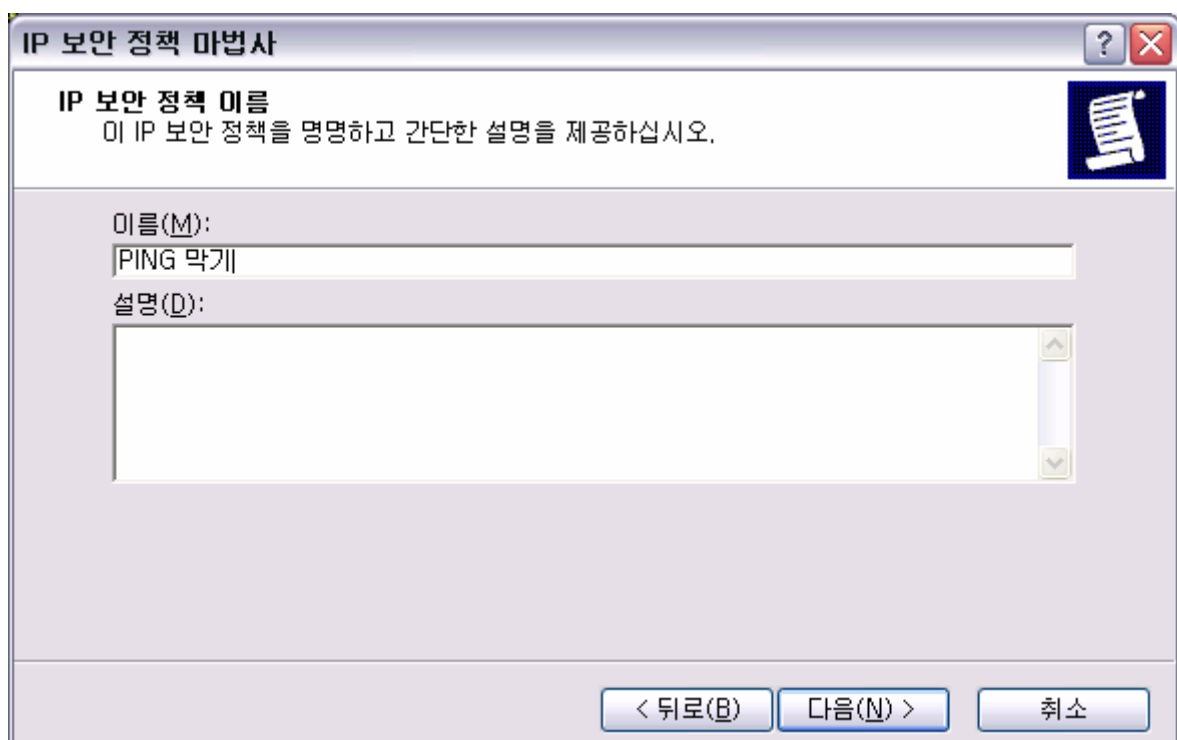
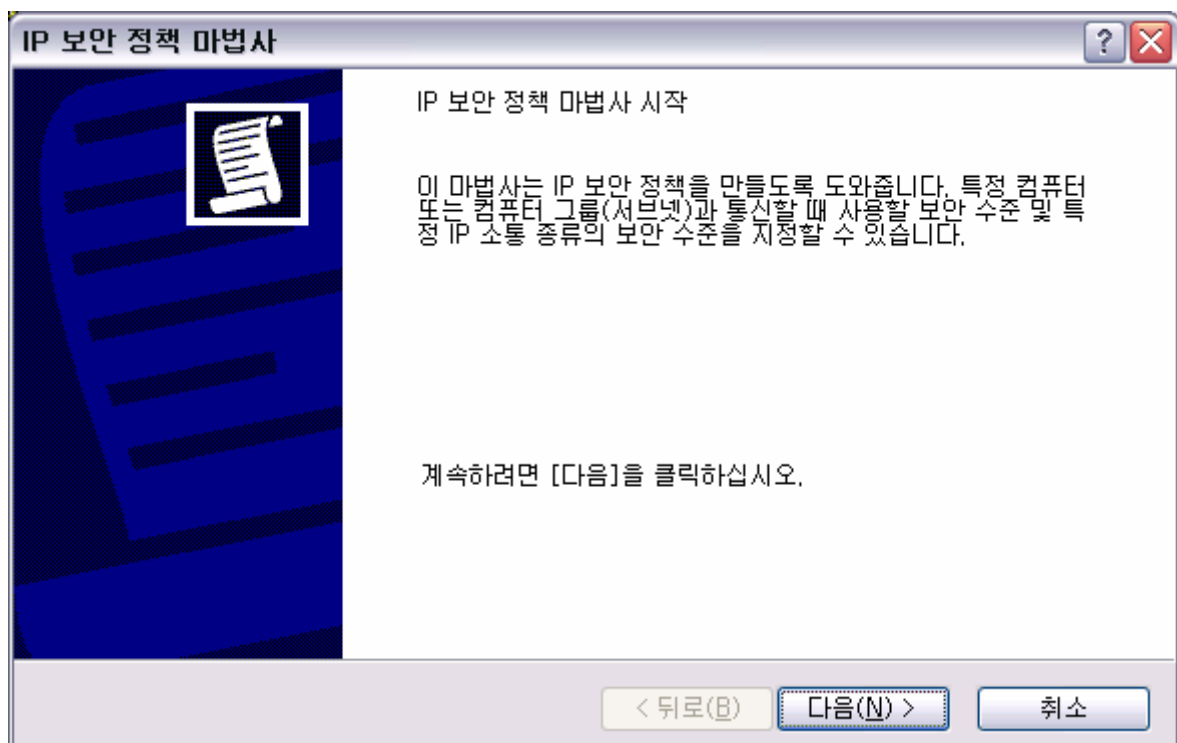
IP 프로토콜 종류
IP 프로토콜 종류를 선택하십시오. 이 종류가 TCP 또는 UDP이면, 원본 및 대상 포트도 지정해야 합니다.

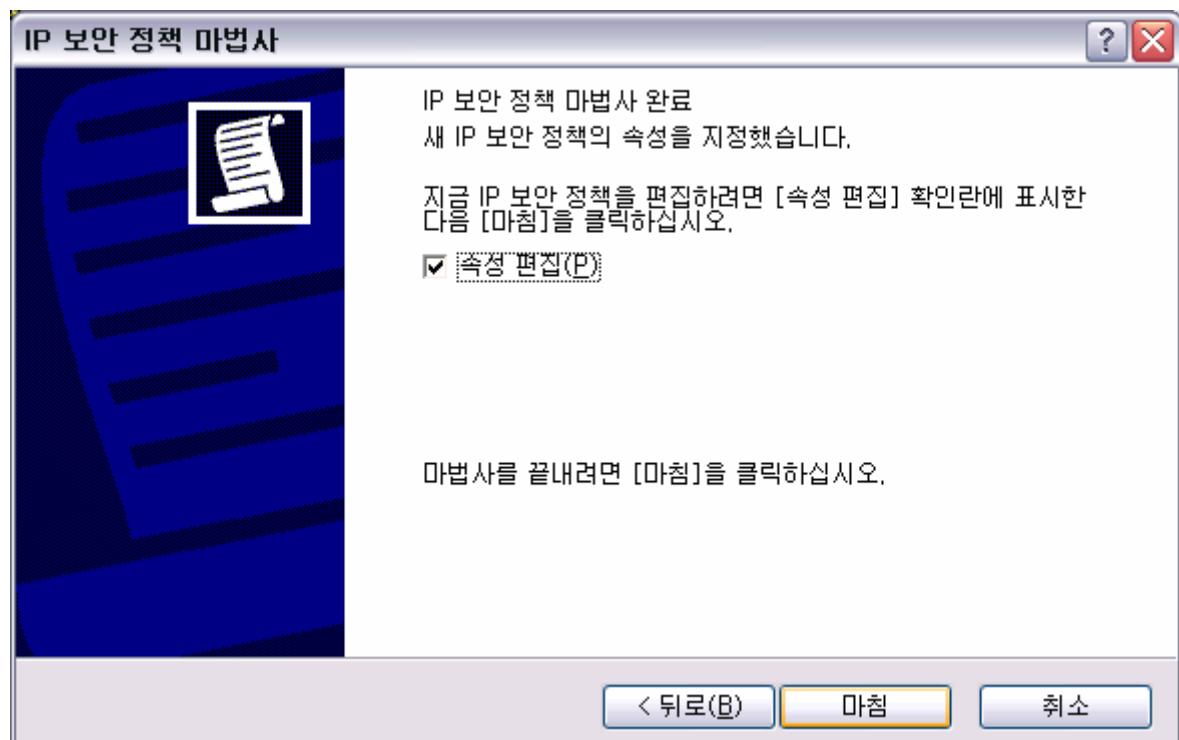
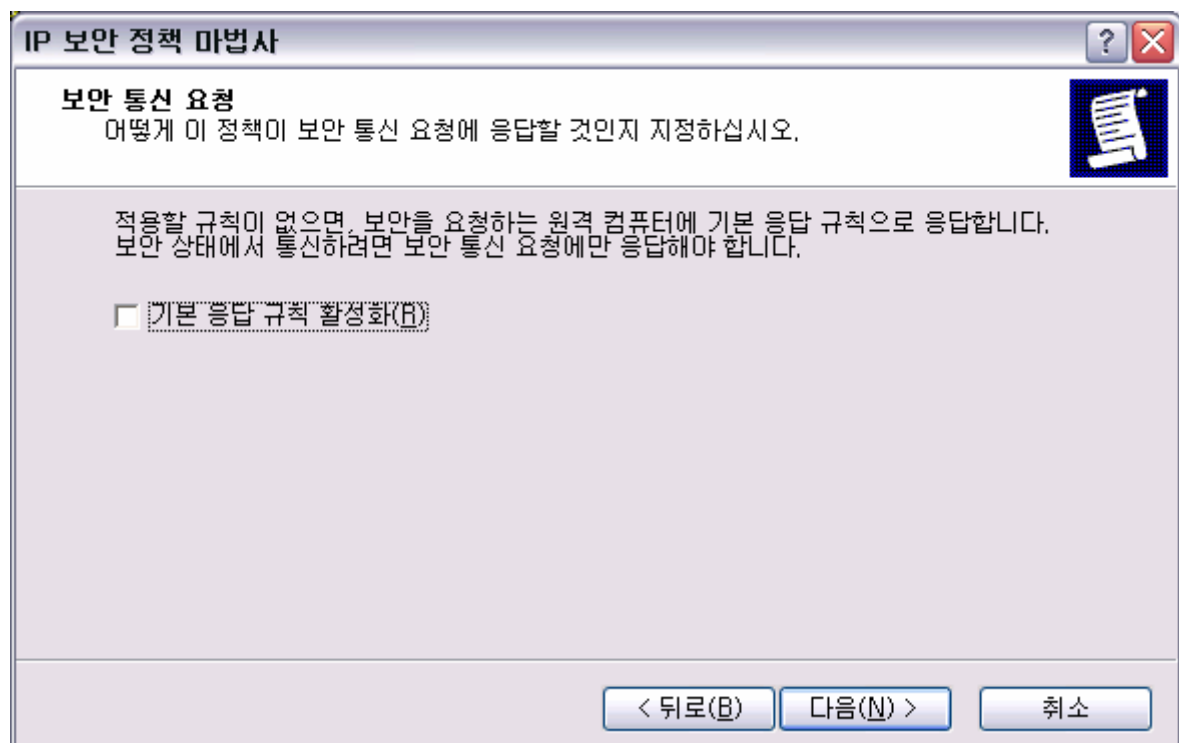
프로토콜 종류 선택(S):
[ICMP ▼]
[1 ▼]

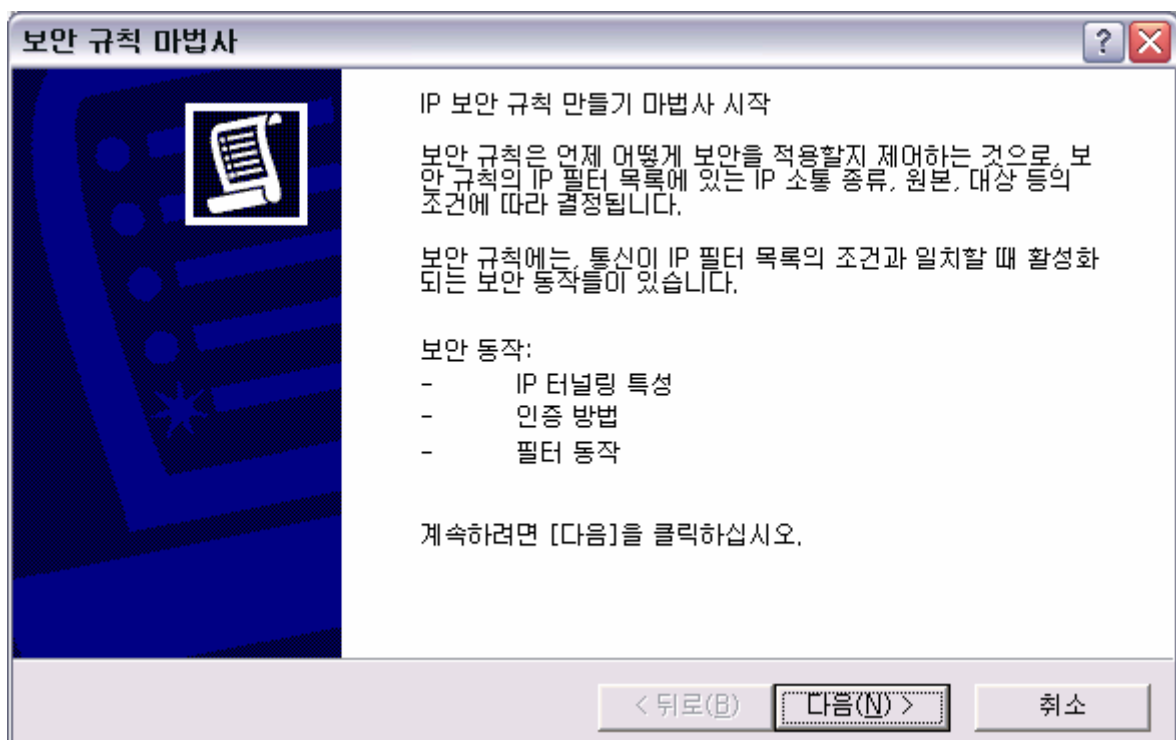
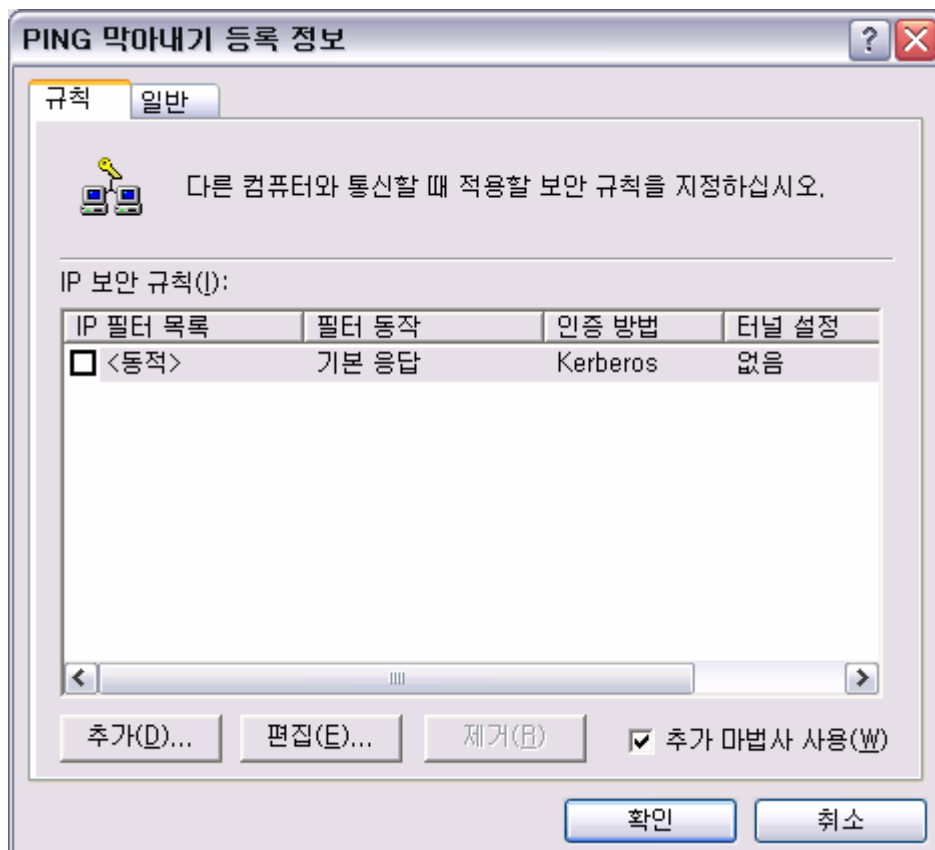
< 뒤로(B) 다음(N) > 취소

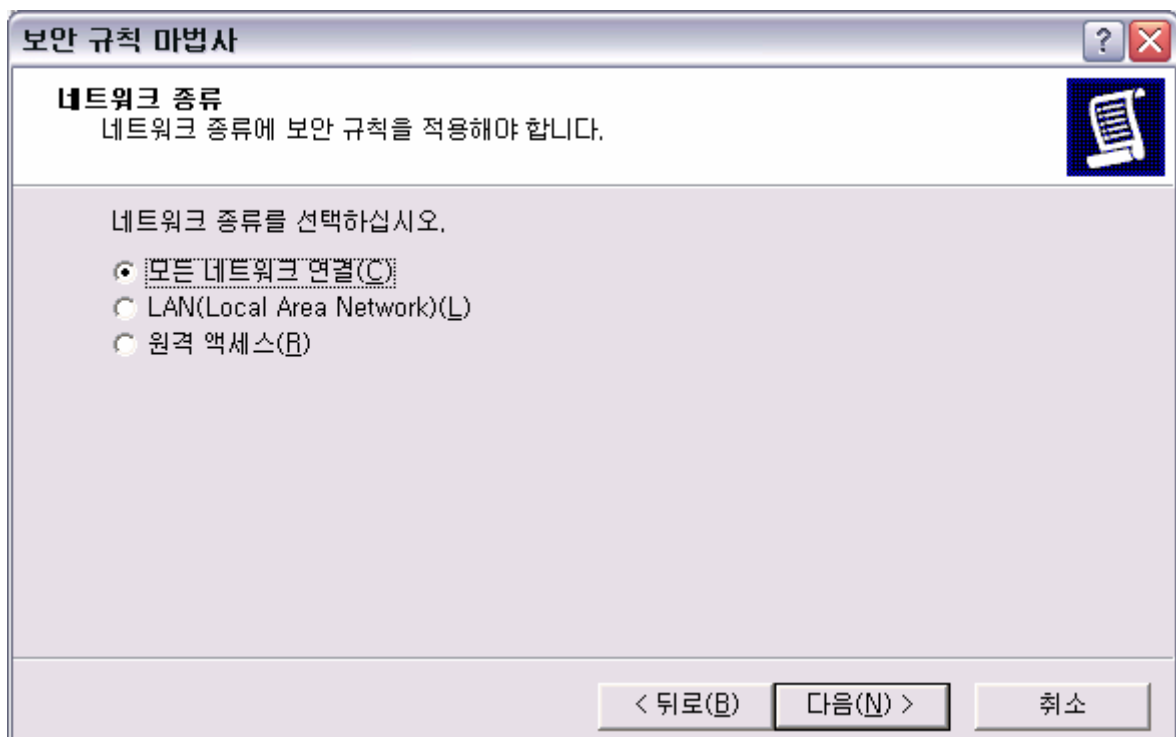
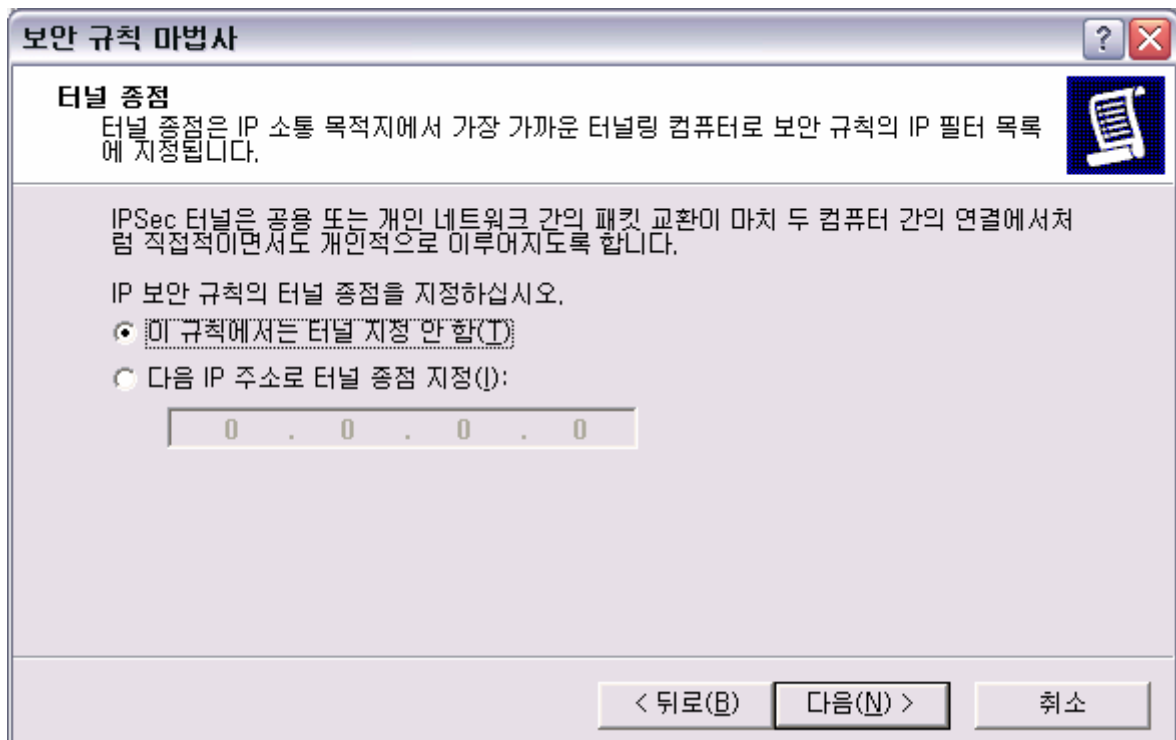
ICMP











?

✕

보안 규칙 마법사

인증 방법

여러 인증 방법을 추가하려면, IP 보안 규칙 마법사를 완료한 다음 보안 규칙을 편집하십시오.

이 보안 규칙의 초기 인증 방법을 설정하십시오.

☒ Active Directory 기본값(Kerberos V5 프로토콜)(D)

☐ 다음 인증 기관(CA)의 인증서 사용(C):

찾아보기(B)...

☐ 다음 문자열을 사용하여 키 교환(미리 공유한 키) 보호(S):


< 뒤로(B)

다음(N) >

취소

✕

경고



경고!

이 규칙이 도메인의 구성원인 컴퓨터에서 사용하게 될 경우에만 Kerberos가 유효합니다. 이 컴퓨터는 도메인의 구성원이 아닙니다. 계속하여 규칙 속성을 저장하시겠습니까?

예(Y)

아니오(N)

?

✕

보안 규칙 마법사

IP 필터 목록

이 보안 규칙이 적용될 IP 소통 종류에 대한 IP 필터 목록을 선택하십시오.

필요에 맞는 IP 필터가 다음 목록에 없으면, [추가]를 클릭하여 새 필터를 만드십시오.

IP 필터 목록(I):

이름	설명
<input type="radio"/> 모든 ICMP 소통	이 컴퓨터와 다른 모든 컴퓨터 ...
<input type="radio"/> 모든 IP 소통	브로드캐스트, 멀티캐스트, Ke...
<input checked="" type="radio"/> PING 막기	

추가(A)...

편집(E)...

제거(R)

< 뒤로(B)

다음(N) >

취소

?

✕

보안 규칙 마법사

필터 동작

이 보안 규칙에 대한 필터 동작을 선택하십시오.

필요에 맞는 필터 동작이 다음 목록에 없으면, [추가]를 클릭하여 새 정책을 만드십시오.
마법사를 사용해 필터 동작을 만들려면 [추가 마법사 사용]을 선택하십시오.

필터 동작(C):

☒ 추가 마법사 사용(W)

이름	설명
<input type="radio"/> 보안 요청(옵션)	보안되지 않은 통신을 받아들...
<input type="radio"/> 보안 필요	보안되지 않은 통신을 받아들...
<input type="radio"/> 허용	보안되지 않은 IP 패킷이 통과...

추가(A)...

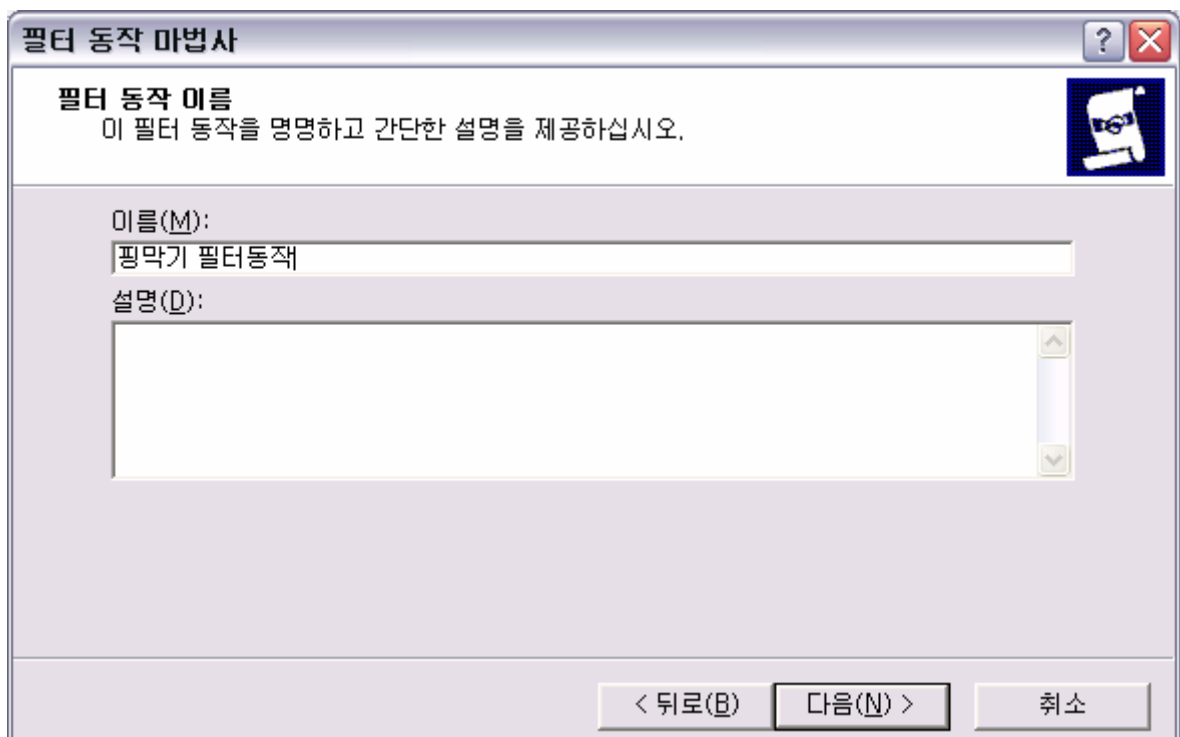
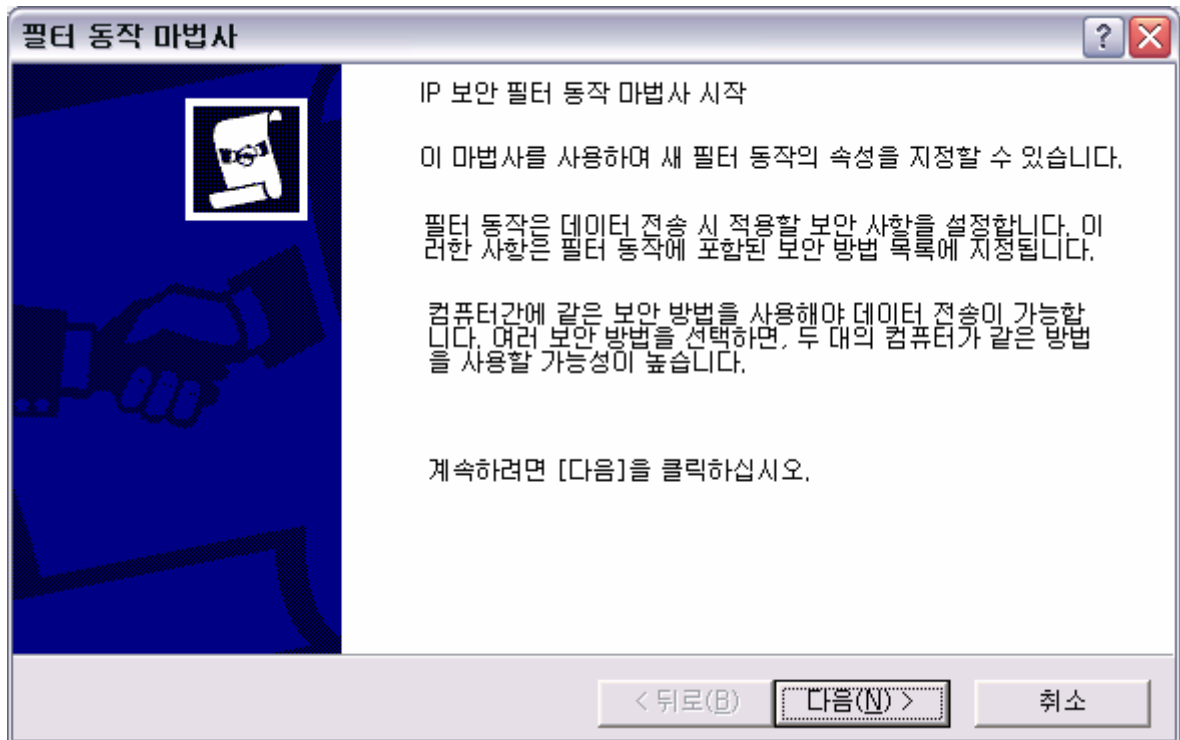
편집(E)...

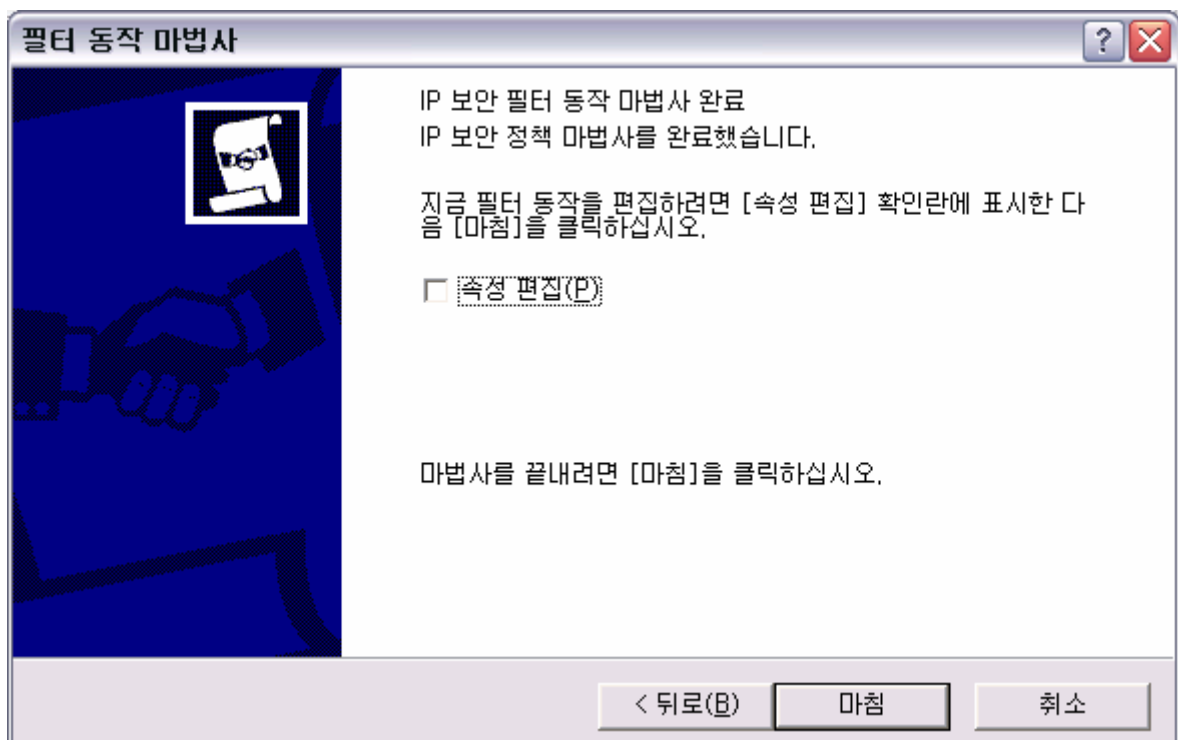
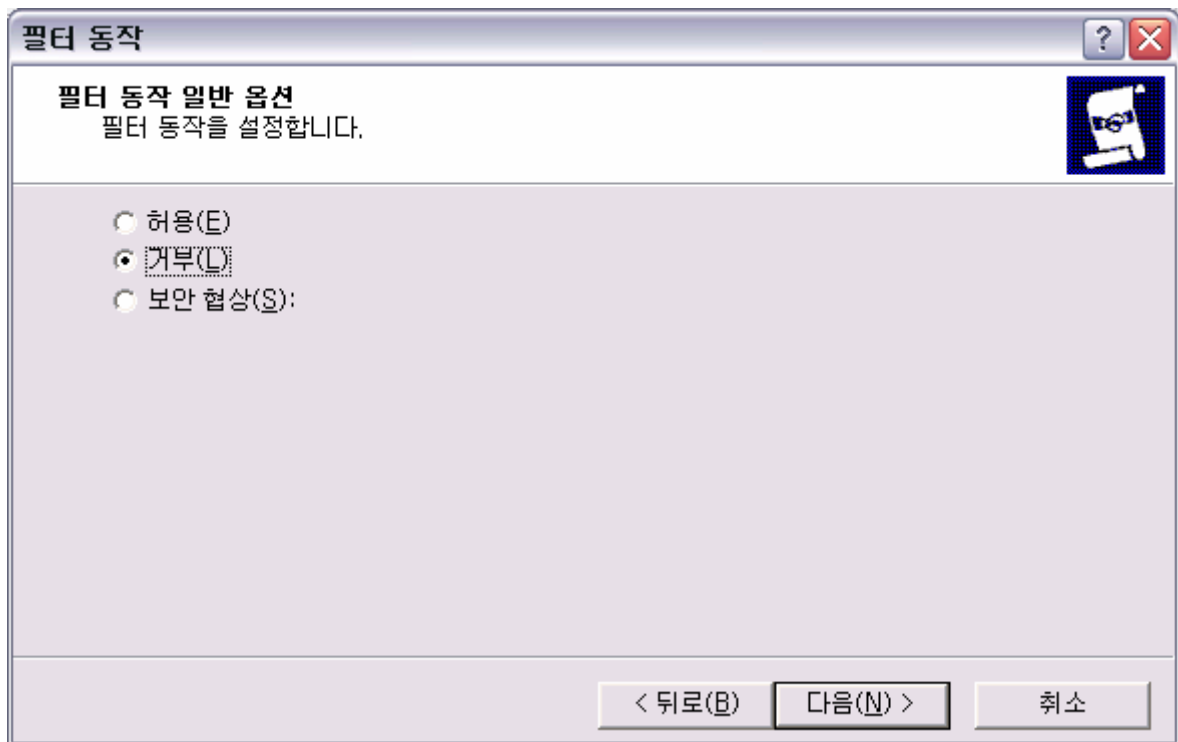
제거(R)

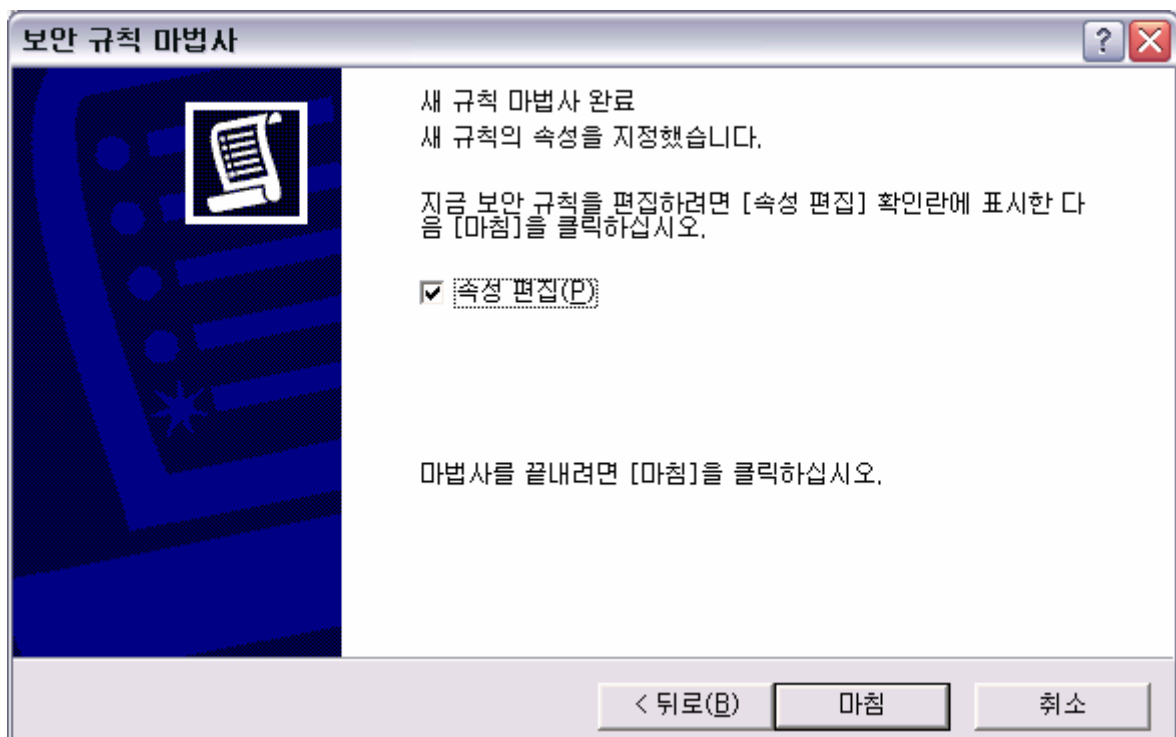
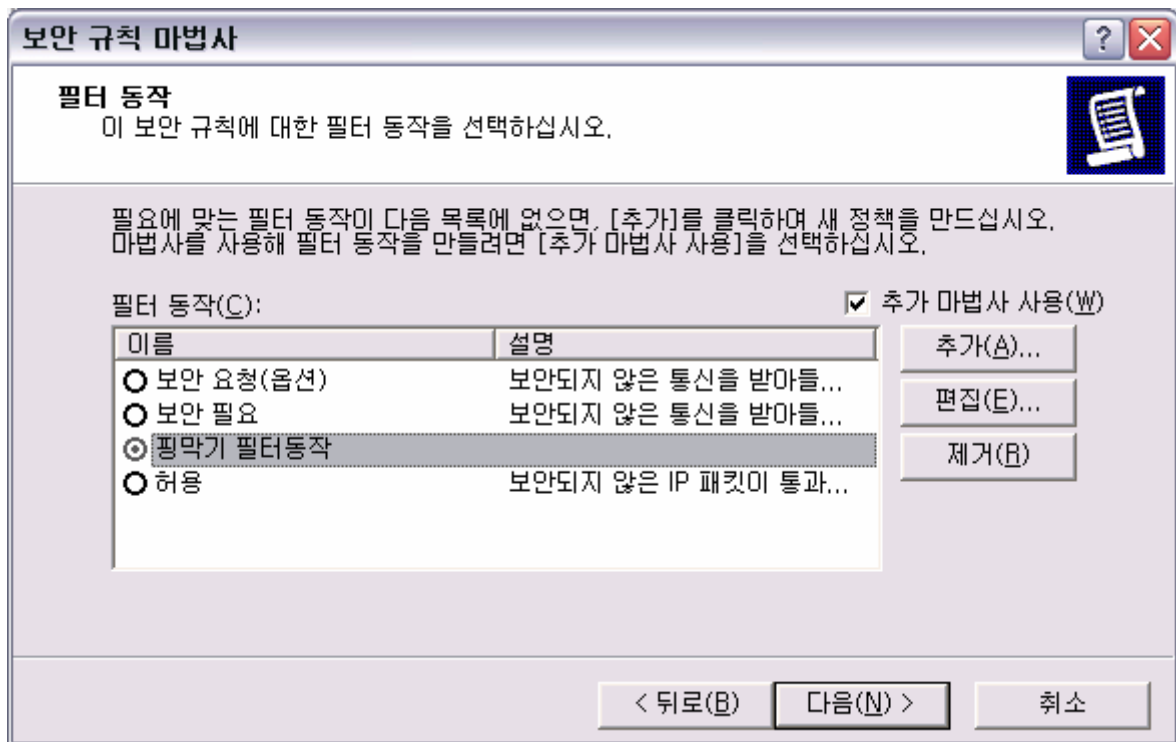
< 뒤로(B)

다음(N) >

취소







새 규칙 등록 정보

?

✕


IP 필터 목록

필터 동작

인증 방법

터널 설정

연결 형식



선택한 IP 필터 목록은 이 규칙으로 어떤 네트워크 소식이 영향을 받을 것인지 지정합니다.

IP 필터 목록(L):

이름	설명
<input type="radio"/> 모든 ICMP 소신	이 컴퓨터와 다른 모든 컴퓨터 사...
<input type="radio"/> 모든 IP 소신	브로드캐스트, 멀티캐스트, Kerb...
<input checked="" type="radio"/> PING 막기	

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 소신의 보안을 확보할 것인지 여부와 소신 보안 방법을 지정합니다.

필터 동작(E):

이름	설명
<input type="radio"/> 보안 요청(옵션)	보안되지 않은 통신을 받아들이...
<input type="radio"/> 보안 필요	보안되지 않은 통신을 받아들이...
<input checked="" type="radio"/> 핑막기 필터동작	
<input type="radio"/> 허용	보안되지 않은 IP 패킷이 통과할 ...

추가(D)...

편집(E)...

제거(R)

☒ 추가 마법사 사용(W)


확인

취소

적용(A)

새 규칙 등록 정보 [?] [X]

IP 필터 목록 | 필터 동작 | 인증 방법 | 터널 설정 | 연결 형식

 인증 방법은 컴퓨터 간의 신뢰 설립 방법을 지정합니다. 다른 컴퓨터와 보안을 협상할 때 이 인증 방법을 제안하고 받아들입니다.

인증 방법 우선 순위(M):


방법	자세히
Kerberos	

추가(A)...
편집(E)...
제거(R)
위로 이동(U)
아래로 이동(D)

확인 취소 적용(A)

새 규칙 등록 정보 [?] [X]

IP 필터 목록 | 필터 동작 | 인증 방법 | 터널 설정 | 연결 형식

 터널 종점은 IP 소스 목적지에서 가장 가까운 터널링 컴퓨터로, 연결된 IP 필터 목록에 지정됩니다. IPSec 터널을 설명하는 두 가지의 규칙이 있습니다.

☒ 이 규칙에서 IPSec 터널을 지정하지 않음(I)
☐ 다음 IP 주소로 터널 종점 지정(J):

0 . 0 . 0 . 0

확인 취소 적용(A)

