시작 -> 프로그램 -> 관리도구 -> 로컬보안정책 (실행 -> secpol.msc 실행)

로컬 컴퓨터의 IP 보안정책 클릭후 오른쪽 마우스를 누르고 IP 보안정책 만들기를 클릭

📑 로컬 보안 설정			
] 동작(<u>A</u>) 보기(<u>V</u>) ← →	🗈 🖬 😰 🗟 😫 🖯 🎦	≜	
트리	이름 🔺	설명	정책 할당
[] 보안 설정 편· [] 계정 정책 편· [] 로컬 정책 편· [] 공개 키 정책 편· [] 로컬 컴퓨터의 IP 보안 정책	♥ vnc ★ vnc ★ 보안 서비(보안 필요) ★ 세 IP 보안 정책 ★ 서비(보안 필요) ★ 클라이언트(응답만) IP 보안 정책 만들기(C) IP 보안 정책 만들기(C)	모든 IP 소통량에 대해 항 모든 IP 소통량에 대해 항 일반적으로 (비보안으로)	예 아니오 아니오 아니오 아니오
	IP 필터 복록 및 필터 동작 판리	(<u>M</u>)	
	모든 작업(<u>K</u>)	•	
	보기(⊻)	•	
	새로 고침(<u>F</u>) 목록 내보내기(<u>L</u>)		
	도움말(<u>H</u>)		

IP 보안 정책 마법사		? ×
	IP 보안 정책 마법사 시작	
	이 마법사는 IP 보안 정책을 만들도록 도와줍니다. 특정 컴퓨터 또는 컴퓨터 그룹(서브넷)과 통신할 때 사용할 보안 수준 및 특 정 IP 소통 종류의 보안 수준을 지정할 수 있습니다.	
	계속하려면 [다음]을 누르십시오.	
	< 뒤로(B) [[[음(N]) >] 취소	
[[] 부아 저채 [][비]]		
IP 보안 정책 이름 이 보안 정책을 명명하고 선택	백적으로 간단한 설명을 제공하십시오.	J
이름(<u>M</u>):		
포트 필터링		
설명(<u>D</u>):		
	<u> 〈 뒤로(B)</u> 다음(N) 〉 취소	

정책이름 설정



IP 보안 정책 마법사	? ×
기본 응답 규칙 인증 방법 여러 인증 방법을 추가하려면 마법사를 완료한 다음 기본 응답 규칙을 편집하십시오.	<u>I</u>
이 보안 규칙의 초기 인증 방법을 설정하십시오.	
 ♥indows 2000 기본값(Kerberos V5 프로토콜)(D) ○ 다음 인증 기관(CA)의 인증서 사용(C): 	1
○ 다음 문자열을 사용하여 키 교환(미리 공유한 키) 보호(<u>S</u>):	
< 뒤로(B) [다음(N) > 취소	





도메인서버 또는 도메인의 구성원이 아닐경우 위 경고메시지가 나타납니다. 예를 클릭하고 다음진행

포트 필터링 등록 정보			? ×
규칙 일반			
이 다른 김	범퓨터와 통신할 때 적용	용할 보안 규칙을 지정	하십시오.
IP 보안 규칙(): IP 필터 목록 □ <동적>	필터 동작 기본 응답	인증 방법 Kerberos	<u>터널 설정</u> 없음
•			Þ
추가(<u>D</u>)	편집(<u>E</u>) 제	거(ੴ)	과법사 사용(₩)
		닫기	취소

기본 설정된 항목에는 체크를 풀어준다

위 화면에서 추가버튼 클릭



그는 ㅠㅋ 미립시	Ľ
터널 종점 터널 종점은 IP 소통 목적지에서 가장 가까운 터널링 컴퓨터로, 보안 규칙의 IP 필터 목록에 지정됩니다.	圓
맘Sec 터널은 공용 또는 개인 네트워크 간의 팽킷 교환이 마치 두 컴퓨터 간의 연결에서쳐 맘 보안 규칙의 터널 종점을 지정하십시오. ● <u>미 규칙에서는 터널 지정 만함(T)</u> ● 다음 IP 주소로 터널 종점 지정(I): 	
< 뒤로(<u>B</u>) 다음(<u>N</u>) > 취급	<u>ځ</u>

보안 규칙 마법사			<u>? ×</u>
네트워크 종류 네트워크 종류에 보안 규칙을 적용해야 합니다			Ē
네트워크 종류를 선택하십시오. • <u>모든 네트워크 연결(C)</u> • LAN(Local Area Network)(<u>L</u>) • 원격 액세스(<u>B</u>)			
	< 뒤로(<u>B</u>)	다음(<u>N</u>) >	취소
IP 보안 정책 마법사			<u>? ×</u>
인증 방법 여러 인증 방법을 추가하려면, IP 보안 규칙 마 시오.	법사를 완료한 [다음 보안 규칙을	편집하십
이 보안 규칙의 초기 인증 방법을 설정하십시 ⓒ Windows 2000 기본값(Kerberos V5 프로 ⓒ 다음 인증 기관(CA)의 인증서 사용(<u>C</u>):	오. 토콜)(<u>D)</u>	ž	HOLE TIVE)
) ⓒ 다음 문자열을 사용하며 키 교환(미리 공위	유한 키) 보호(<u>S</u>)		01±27(<u>0</u> /
			×
	< 뒤로(<u>B</u>)	다음(<u>N</u>) >	취소

보안 규칙 마법사		<u>? ×</u>
IP 필터 목록 이 보안 규칙이 적용될 IP 소통 중	종류에 대한 IP 필터 목록을 선택하십시오	
필요에 맞는 IP 필터가 다음 목록 IP 필터 목록(I):	록에 없으면, [추가]를 눌러 새 필터를 만.	드십시오.
이름 이모든 ICMP 소통량 이모든 IP 소통량	설명 이 컴퓨터와 다른 임의의 컴퓨 이 시스템의 모든 IP 패킷을 다	추가(<u>A</u>) 편집(<u>E</u>) 제거(<u>B</u>)
	< 뒤로(B) 다음(N) >] 취소

필터목록을 추가합니다. (추가버튼 클릭)

tt 🖪	IP 필터 독	<u></u> 록				<u>? ×</u>
		IP 필터 목록은 여리 IP 필터 하나로 결합	네 필터로 구성됩니[よ시킬 수 있습니다.	다. 따라서, 복수 서	보넷, IP 주소, 3	프로토콜 등을
	이름(<u>N</u>):					
	포트필터	링				×7μ(Δ)
	설명(<u>D</u>):				_	+/\0/
	rpc 공격	관련 거뷔				편집(<u>E</u>),,,
					v	제거(<u>B</u>)
	필터(<u>S</u>):				🔽 추가 마법	법사 사용(₩)
	미러됨	설명	프로토콜	원본 포트	대상 포트	원분
	•					Þ
					확인	취소

필터목록을 추가합니다. (추가버튼 클릭)



			? ×
IP 소통 대상 IP 소통의 대상 주소를 지정하십시오.			Ē
대상 주소(<u>D</u>):			
모든 미 주소	_		
	< 뒤로(B)	[[[·[음(N) >]]	취소
필터 마법사			<u>? ×</u>
IP 프로토콜 종류			
IP 프로토콜 종류를 선택하십시오. 이 종류가 합니다.	IP 포트를 지원히	H면, IP 포트도 지정	명해야 표
IP 프로토콜 종류를 선택하십시오. 이 종류가 합니다. 프로토콜 종류 선택(<u>S</u>): TCP	IP 포트를 지원히	H면, IP 포트도 지정	Since
IP 프로토콜 종류를 선택하십시오. 이 종류가 합니다. 프로토콜 종류 선택(<u>S</u>): TCP 6 ᆕ	IP 포트를 지원히	H면, IP 포트도 지정	Signer E
IP 프로토콜 종류를 선택하십시오. 이 종류가 합니다. 프로토콜 종류 선택(<u>S</u>): TCP 6 异	IP 포트를 지원히	ŀ면, IP 포트도 지장	State State
IP 프로토콜 종류를 선택하십시오. 이 종류가 합니다. 프로토콜 종류 선택(<u>S</u>): TCP 6 글	IP 포트를 지원히	ŀ면, IP 포트도 지정	State State
IP 프로토콜 종류를 선택하십시오. 이 종류가 합니다. 프로토콜 종류 선택(<u>S</u>): TCP 6 글	IP 포트를 지원히	ŀ면, IP 포트도 지정	Statu:
IP 프로토콜 종류를 선택하십시오. 이 종류가 합니다. 프로토콜 종류 선택(<u>S</u>):	IP 포트를 지원히	ŀ면, IP 포트도 지정	Statu:
IP 프로토콜 종류를 선택하십시오. 이 종류가 합니다. 프로토콜 종류 선택(<u>S</u>): ICP ICP ICP ICP	IP 포트를 지원히	1면, IP 포트도 지정	250HOF
IP 프로토콜 종류를 선택하십시오. 이 종류가 합니다. 프로토콜 종류 선택(<u>S</u>): ICP ICP ICP ICP	IP 포트를 지원히	1면, IP 포트도 지정	State Stat

프로토콜종류 를 우선 TCP 부터 클릭합니다. (모든프로토콜을 체크하지 않도록 주의)



tt 🖪	IP 필터 목	목록				? ×	
		IP 필터 목록은 여긴 IP 필터 하나로 결합	법 필터로 구성됩니다 압시킬 수 있습니다.	, 따라서, 복수 서!	르넷, IP 주소, 3	프로토콜 등을	
	이름(<u>N</u>):						
	포트필터	1링				추가(<u>A</u>)	
	설명(<u>D</u>): Irpo 고격					 펴진(E)	
	1 pr 24	한만 기구					
	I						
	필터(<u>S</u>):				☑ 주가 바間	법사 사용(₩)	
	미러됨	실명	_ 프로토콜	원본 포트	대상 포트	원톤	
			TUP	135	보누	< LH	
				닫	기(<u>C</u>)	취소	
							1

위와같이 필터가 하나 생성이 되었습니다.

위와 같은 방식으로 포트를 추가합니다.

RPC 서비스시 문제를 일으킬수있는 수신 대기 포트는 아래와 같습니다.

epmap	135/tcp	loc-srv	#DCE endpoint resolution
epmap	135/udp	loc-srv	#DCE endpoint resolution
netbios-ns	137/tcp	nbname	#NETBIOS Name Service
netbios-ns	137/udp	nbname	#NETBIOS Name Service
netbios-dgm	138/udp	nbdatagram	#NETBIOS Datagram Service
netbios-ssn	139/tcp	nbsession	#NETBIOS Session Service
microsoft-ds	445/tcp		
microsoft-ds	445/udp		
593/tcp			

위 포트들을 추가한후 닫기를 합니다.

보안 규칙 마법사		<u>? ×</u>				
IP 필터 목록 이 보안 규칙이 적용될 IP 소통 종류에 대한 IP 필터 목록을 선택하십시오.						
필요에 맞는 IP 필터가 다음 목록에 IP 필터 목록(]):	없으면, [추가]를 눌러 새 필터를 만!	드십시오.				
이름	설명	추가(<u>A</u>)				
O 모든 ICMP 소통량	이 컴퓨터와 다른 임의의 컴퓨					
· · · · · · · · · · · · · · · · · · ·	이 시스템의 모든 IP 패킷을 다					
◎포트필터링	rpc 공격판련 거부	제거(<u>B</u>)				
,						
	< 뒤로(<u>B</u>) 다음(<u>N</u>)> 취소				

새로만든 포트필터링 을 체크한후 다음버튼 클릭

보안 규칙 마법사		? ×					
필터 동작 이 보안 규칙에 대한 필터 동작을 선택하십시오.							
필요에 맞는 필터 동작이 다음 목록(동작을 만들려면 [추가 마법사 사용	에 없으면, [추가]를 눌러 새 정책을]을 선택하십시오, 	만드십시오, 필터					
필터 동작(<u>C</u>):	N.	주가 바랍사 사용(班)					
이름	설명	_ <u>추가(A)</u>					
O 보안 요청(옵션)	보안되지 않은 통신을 받으나	INT/F)					
O 모안 필요	모안되지 않은 통신을 받으나						
O de	모안되지 않는 IP 패킷들 동과	제거(<u>B</u>)					
	< 뒤로(<u>B</u>) 다음(<u>b</u>	<u>)</u>) > 취소					

필터 동작을 추가합니다.(추가버튼 클릭)



이름(<u>M</u>):		
수신 거부		
설명(<u>D</u>):		
		X
	< 뒤로(<u>B</u>) 다음(<u>N</u>) >	취소

이제 위의 나열한 포트를 막는 동작을 추가합니다.

필터 동작	? 🗙
필터 동작 일반 옵션 필터 동작을 설정합니다.	<u>E</u>
○ 허용(E) ● <u>거부(L)</u> ○ 보안 협상(<u>S</u>):	
	< 뒤로(<u>B</u>) 다음(<u>N</u>) > 취소
보안 규칙 마법사	? ×
필터 동작 이 보안 규칙에 대한 필터 동작을 선	핵하십시오.
필요에 맞는 필터 동작이 다음 목록 동작을 만들려면 [추가 마법사 사용	에 없으면, [추가]를 눌러 새 정책을 만드십시오. 필터]을 선택하십시오.
필터 동작(<u>C</u>):	추가 마법사 사용(₩)
이 보안 요청(곱전)	보안되지 않은 동신을 받으나 편집(E)
◎ 수신 거부	
0 허용	보안되지 않은 IP 패킷을 통과
	<뒤로(<u>B</u>) 다음(<u>N</u>)> 취소

만든 수신거부 동작을 클릭한후 다음

포트 필터링 등록 정보			? ×			
규칙 일반]						
이 다른 컴퓨터와 통신할 때 적용할 보안 규칙을 지정하십시오.						
IP 보안 규칙([):						
IP 필터 목록	필터 동작	인증 방법	터널 설정			
☑ 포트필터링	수신 거부	Kerberos	없음			
□ <동적>	기본 응답	Kerberos	없음			
▲ <u>추フ⊦(D</u>)	편집(E) 기	데거(<u>B)</u> ▼ 추가	▶ 마법사 사용(₩)			
		닫기	취소			

위와같이 포트필터링 목록이 생성됩니다.

여기서 추가할 사항은 위포트들을 막을경우 윈도우의 네트웍 드라이브 연결을 거부합니다. 만약 네트웍 드라이브연결을 해야하는 서버가 있다면 포트를 열어주는 동작도 설정합니다.

(각 isp 업체마다 해당포트는 막혀있을것입니다. 정통부에서 의무적으로 해당포트를 막도록 지시가 되어있습니다.)

허나 같은 isp 업체내에서(라우터) 서비스 되는 서버끼리 연결할 경우 포트를 열어줍니다.

위 화면에서 추가 예외처리 를 추가합니다. (추가버튼 클릭) 앞에서 설정한것과 같은 화면이 나올것인데 똑 같은 절차를 밟으시면 됩니다.

보안 규칙 마법사 IP 필터 목록 이 보안 규칙이 적용될 IP 소통 종류에 대한 IP 필터 목록을 선택하십시오.							
필요 IP 및	3에 맞는 IP 필터가 다음 목록에 (필터 목록([):	없으면, [추가]를 눌러 새 필터를 만!	드십시오.				
0000	름 모든 ICMP 소통량 모든 IP 소통량 포트필터링	설명 이 컴퓨터와 다른 임의의 컴퓨 이 시스템의 모든 IP 패킷을 다 rpc 공격관련 거부	추가(<u>A</u>) 편집(<u>E</u>) 제거(<u>B</u>)				
		< 뒤로(<u>B</u>) 다음(<u>N</u>) > 취소				

여기서 예외처리 목록을 추가합니다. 추가버튼 클릭

1	IP 필터 목	¦록				? ×
		IP 필터 목록은 여러 IP 필터 하나로 결합	H 필터로 구성됩니다 사귈 수 있습니다.	다. 따라서, 복수 /	서보넷, IP 주소,	프로토콜 등을
	이름(<u>N</u>):					
	예외동작				í	本7#(A)
	설명(<u>D</u>):					
						편집(<u>E</u>),
					-	제거(<u>B</u>)
	필터(<u>S</u>):				☑ 추가 마	법사 사용(₩)
	미러됨	설명	프로토콜	원본 포트	대상 포트	원빈
	•					Þ
					확인	취소 ///

필터 추가 (추가버튼 클릭)

<mark>필터 마법사 IP 소통 원본</mark> IP 소통의 원본 주소를 지정하십시오.	× ?
원본 주소(<u>S</u>): 내 IP 주소	
< 뒤로(<u>B</u>) 다음(<u>N</u>) >	취소
할머마입자 IP 소통 대상 IP 소통의 대상 주소를 지정하십시오,	T ×
대상 주소(<u>D</u>): 특정 IP 주소	
IP 주소(<u>B</u>): 211 . 239 . 150 . 5	
서브넷 마스크(<u>K</u>): 255 . 255 . 255 . 255	
J	
< 뒤로(<u>B</u>) 다음(<u>N</u>) >	취소

대상주소에서 스크롤바를 내리면 ip 주소 및 서브넷 지정이 가능합니다. 1 ip 대역을 열수도 있습니다. 위에서 특정ip 주소만 열어줍니다. 다음

필터 마법사	?×
IP 프로토콜 종류 IP 프로토콜 종류를 선택하십시오, 이 종류가 IP 포트를 지원하면, IP 포트도 지정해야 합니다.	Ē
프로토콜 종류 선택(<u>S</u>): 모두 고 :	
< 뒤로(<u>B</u>) 다음(<u>N</u>) >	취소

프로토콜은 모든 프로토콜을 열어줍니다.(해당프로토콜만 열어줘도 됩니다.)

28 B	IP 필터 독	¦록								? ×
		IP 필터 IP 필터	목록은 여리 하나로 결합	:! 필터로 구(값시킬 수 있)	성됩니다. 습니다.	따라서, 복	수 서브!	퀸, IP 주소,	프로토콜 등	을
	이름(<u>N</u>):									
	예외동작								추가(<u>A</u>)	
	설명(<u>D</u>):								편집(<u>E</u>)	
								-	제거(<u>B</u>)	
	필터(<u>S</u>):							☞ 추가 마	법사 사용(⊻	Ď
	미러됨	설명		프로토콜		원본 포트		대상 포트		원분
	UHI .			보구		보구		보구		<u>SL</u> i
					1					
						[닫기	©	취소	

예외동작 생성

보안 규칙 마법사		<u>? ×</u>					
IP 필터 목록 이 보안 규칙이 적용될 IP 소통 종류에 대한 IP 필터 목록을 선택하십시오.							
필요에 맞는 IP 필터가 다음 목록에 IP 핀터 목록(1):	∥ 없으면, [추가]를 눌러 새 필터를 만!	드십시오.					
	[선명 [ネフル(ム)					
O 모든 ICMP 소통량	이 컴퓨터와 다른 임의의 컴퓨						
O 모든 IP 소통량	이 시스템의 모든 IP 패킷을 다	편집(<u>E</u>)					
⊙ 예외동작							
O 포트필터링	rpc 공격관련 거부						
	< 뒤로(<u>B</u>) 다음(<u>N</u>)> 취소					
	¥						

예외동작을 체크한후 다음

보안 규칙 마법사		<u>? ×</u>
필터 동작 이 보안 규칙에 대한 필터 동작을 선택	백하십시오.	Ē
필요에 맞는 필터 동작이 다음 목록(동작을 만들려면 [추가 마법사 사용] 필터 동작(<u>C</u>):	게 없으면, [추가]를 눌러 새 정책을]을 선택하십시오, IV	만드십시오. 필터 추가 마법사 사용(逊)
미를 ○ 보안 요청(옵션) ○ 보안 필요 ○ 수신 거부 ④ 허용	설명 보안되지 않은 통신을 받으나 보안되지 않은 통신을 받으나 보안되지 않은 IP 패킷을 통과	추가(<u>A</u>) 편집(<u>E</u>) 제거(<u>B</u>)
	< 뒤로(<u>B</u>) 다음(<u>N</u>	l) > 취소

예외동작을 허용해줍니다.

포.	트 필터링 등록 정보			?
	규칙 일반]			
	6			
	📑 🚊 다른 컴퓨	뛰어와 통신할 때 ?	적용할 보안 규칙을 지정	하십시오,
	IP 보안 규칙([):			
	· · · · · · · · · · · · · · · · · · ·	필터 동작	민중 방법	러달 설정
	▶ 포트필터링	수신 거부	Kerberos	없음
	☑ 예외동작	허용	Kerberos	없음
	┃□ <동적>	기본 응답	Kerberos	없음
	추가(<u>D</u>)	편집(<u>E</u>)	제거(<u>B</u>) 🔽 추가 [마법사 사용(<u>₩</u>)
			닫기	취소

위와같이 거부와 일부허용서버 허용 두가지를 체크합니다.

닫기를 누르면 아래 화면이 나타납니다.

Ľ	<mark>광</mark> 도킬 모만 설성				
] 동작(A) 보기(V) ⇐ → 🖻 📧 🖗 🔀 😤 🎦 🏪				
ſ	트리	이름 🔺	설명	정책 할당	
	 ▶ 보안 설정 ▶ ▲ 계정 정책 ▶ ▲ 로컬 정책 ▶ ▲ 로컬 정책 ▶ ▲ 공개 키 정책 ▶ ▲ 공개 키 정책 	 ▶ 보안 서버(보안 필요) ▶ 서버(보안 필요) ▶ 클라이언트(응답만) ▶ 포트 필터링 	모든 IP 소통량에 대해 항 모든 IP 소통량에 대해 항 일반적으로 (비보안으로)	아니오 아니오 아니오 아니오	

새로만든 포트필터링 정책을 할당해줍니다.

률로컬 보안 설정 동작(A) 보기(V) ← → 1 🗈 📧 🗙 📽 💀 🔒 🔒 🗎 🚹 🧕		
● 실정 ● 실정 ● 실 정책 ● 로컬 정책 ● 로컬 컴퓨터의 IP 보안 정책	안 필요) 모든 IP 소통량에 대해 항 아니오 요) 모든 IP 소통량에 대해 항 아니오 응답만) 일반적으로 (비보안으로) 아니오 아니오 아니오 아니오 아니오 아니오 다니오 아니오 아니오 다니오	

위 포트 이외에 각종 서비스 포트필터링을 설정할수있습니다.