

아이티이지 서비스 운영팀

[IPsec(IP보안정책) 설정 메뉴얼]



ITEASY

- ⇔ 문서 작성간에 테스트된 환경
 - Windows 2008 R2 Enterprise 64bit
- & 버전 정보
 - IP 보안 정책 관리 Microsoft Corporation v6.1
- & IPsec (Internet Protocol Security) 이란?
 - 안전에 취약한 인터넷에서 안전한 통신을 실현하는 통신규약으로 인터넷 상에 전용 회선과 같이
 이용 가능한 가상적인 전용회선을 구축하여 데이터를 도청당하는 등의 행위를 방지하기 위한 통
 신규약입니다.
 - IP 는 기본적으로 보안에 매우 취약합니다. IP 기반 네트워크를 보호하기 위한 방법으로 IP Security(IPsec)을 이용하여 보안을 강화시킬 수 있습니다. IPsec은 IP와 같은 계층(Layer)에서 작동 하는 응용프로그램 계층 프로토콜입니다.
- & 설정 순서
 - ① IP 보안 정책 명 생성
 - ② IP 필터 목록 생성
 - ③ 필터 설정 (허용/차단)
 - ④ 적용





1. IP 보안 정책 설정

⑤ [시작 > 모든 프로그램 > 관리도구 > 로컬 보안정책] 을 클릭합니다.

		🍌 원격 데스크톱 서비스 🔹 🕨
		 행 IIS(인터넷 정보 서비스) 관리자 ● ISCSI 초기자 ● Windows PowerShell Modules
명령 프롬프트	E.	🛞 Windows Server 백업 🝙 Windows 메모리 진단
Internet Explorer		☞ 고급 보안이 포함된 Windows 방화벽 중 공유 및 저장소 관리
🏹 IIS(인터넷 정보 서비스) 관리자	Administrator	🦗 구성 요소 서비스
에모장 •	문서	3 로컬 보안 정책
QR gertp	컴퓨터	·····································
FileZilla	네트워크	정능 모니터
() 성능 모니터	제어판	신스템 구성 값 이벤트 뷰머
iscsl 本フIスト	장치 및 프린터	 작업 스케줄러 국 저장소 탐색기
	관리 도구	출 컴퓨터 관리
1 2 도인 상역	도움말 및 지원	
	실행	
▶ 모든 프로그램	Windows 보안	
프로그램 및 파일 검색	로그오프 🔸	
🕅 🗸 🕌 🚺		

⑥ [로컬 보안 정책 > IP 보안 정책] 을 클릭합니다.

📕 로컬 보안 정책				
파일(F) 동작(A) 보기(V) 도움말(H)				
🗢 🔿 🙍 🐻 🤷 👘 🏠	<mark>∄</mark> •			
🔒 보안 설정	이름 🔺	설명	정책 할당	마지막 수정한
 표 계성 정책 단 2		현재 보기에서	표시할 항목이 없습니다.	



2. 정책 생성

⑦ [IP 보안 정책 (마우스 우클릭) > IP 보안 정책 만들기] 를 클릭합니다.

🖺 로컬 보안 정책				
파일(F) 동작(A) 보기(V) 도움	움말(H)			
🗢 🔿 🖄 📅 🙆 🗟 🛙 🖬	1 🖆 🔂			
보안 설정 ▲ 계정 정책 ● 로 컬 정책 ● 로 컬 정책 ● 급 보안이 포함된 Window: □ 네트워크 목록 관리자 정책 ● 급 공개 키 정책 ● 급 소프트웨어 제한 정책 ● 음용 프로그램 제어 정책 ● 급 감사 정책 구성	s 방화벽 IP 보안 정책 만들기(C) IP 필터 목록 및 필터 동작 편 모든 작업(K)	실명 현재 보기에서 : 관리(M) ▶	│ 정책 할당 표시할 항목이 없습니다.	마지막 수정한
	보기(V) 새로 고침(F) 목록 내보내기(L)	•		
	도움말(H)			
┃◀┃ IP 보안 정책을 만듭니다.				

⑧ 다음 단계로 진행합니다.



⑨ 생성할 정책 명을 지정한 뒤, 다음 단계로 진행합니다.

이름(M):		
설명(D):		
		<u> </u>
		-

⑩ 다음 단계로 진행합니다.

ΡĿ	코안 정책 마법사
	보안 통신 요청 어떻게 이 정책이 보안 통신 요청에 응답할 것인지 지정하십시오.
	적용할 규칙이 없으면, 보안을 요청하는 원격 컴퓨터에 기본 응답 규칙으로 응답합니다. 보안 상태에서 통신하려면 보안 통신 요청에만 응답해야 합니다.
	참고: 기본 응답 규칙은 Windows 2003 및 Windows XP를 실행하는 컴퓨터에서만 지원됩 니다.
	□ 기본 응답 규칙 활성화(이전 버전의 Windows만 해당)(R)
	< 뒤로(B) 다음(N) > 취소



ITEASY IT is easy, ITEASY

^{,칙} 일반			
다른 컴퓨	터와 통신할 때 적용	할 보안 규칙을 지 ³	정하십시오.
IP 보안 규칙(l):			
IP 필터 목록	필터 동작	인증 방법	터널 끝점
□ <동적>	기본 응답(이 <u>전</u>	Kerberos	(없음)
41		1	N
추가(D) 편	집(E) 제거	(R) マネフ	나 마법사 사용(\\)
		F	1

12 정책 생성 후, 속성 편집 창이 활성화 됩니다. (속성 창에서 정책을 설정할 수 있습니다.)

IP 보안 정책 마법사	2	C
	IP 보안 정책 마법사 완료	
	새 IP 보안 정책의 속성을 지정했습니다. 지금 IP 보아 정책을 펴지하려며 [소성 펴지] 화이라에 표시하	
	다음 [마침]을 클릭하십시오.	
	✓ 속성 편집(P)	
	마법사를 끝내려면 [마침]을 클릭하십시오.	
	< 뒤로(B) 마침 취소	

① 속성 편집이 체크 되어 있는 상태에서 마침을 클릭합니다.

KGIDC 주석

iteasy

2 1



③ 생성된 정책은 기본적으로 할당 해제되어 있는 상태로 생성이 됩니다.

🔒 보안 설정	이름 🔺	설명	정책 할당	마지막 수정
표 📆 계정 정책	KSIDC		아니요	2011-11-15
표 🛃 로컬 정책				
🗉 고급 보안이 포함된 Windows 방화	判			
🧾 네트워크 목록 관리자 정책				
🗉 🧮 공개 키 정책				
🗉 🧮 소프트웨어 제한 정책				
표 🧮 응용 프로그램 제어 정책				
🜏 IP 보안 정책(위치: 로컬 컴퓨터)				



3. IP 보안 규칙 설정

④ 열려 있는 속성 창에서 정책을 만들도록 합니다. 속성 창을 닫으셨을 경우 [정책명 > 마우스
 우클릭 > 속성] 을 클릭하여 속성 편집 창을 열도록 합니다.

🖺 로컬 보만 정책				
파일(F) 동작(A) 보기(V) 도움말(H)				
🗢 🄿 🔰 📅 💥 🖼 🗟 🛛 🖬 1	2 🔂 🛛 🗎			
🚡 보안 설정	이름 🔺	설명	전책 할당	마지막 수정한
 Ⅲ 1 → 1 → 1 → 3 → 3 → 4 → 1 → 1 → 1 → 1 → 1 → 1 → 1 → 1 → 1		할당(A)	아니요	2011-11-15 오
표 고급 보안이 포함된 Windows 방화벽		모든 작업(K) 🔹 🕨		
 ☑ 곱개 키 정책 ☑ 곱 소프트웨어 제한 정책 ☑ 곱 응용 프로그램 제어 정책 		삭제(D) 이름 바꾸기(M)		
IP 보안 정책(위치: 로컬 컴퓨터)		속성(R)		
표 🛄 꼬급 참자 정적 구성		도움말(H)		

(B) [속성 > 추가] 를 클릭하여 정책을 생성하도록 합니다.

SIDC 속성			? >
· · · · · · · · · · · · · · · · · · ·			
이 다른 등	컴퓨터와 통신할 때 적용	할 보안 규칙을 지정	하십시오,
IP 보안 규칙(l):			
IP 필터 목록	필터 동작	인증 방법	터널 끝점
□ <동적>	기본 응답(이전	, Kerberos	<없음>
 ₹7ŀ(D) 	며진(F) 제거		
			
		독근	키고



16 IP 보안 규칙을 생성합니다.

보안 규칙 마법사	×
	IP 보안 규칙 만들기 마법사 시작
	보안 규칙은 언제 어떻게 보안을 적용할지 제어하는 것으로, 보 안 규칙의 IP 필터 목록에 있는 IP 트래픽 종류, 원본, 대상 등의 조건에 따라 결정됩니다.
	보안 규칙에는, 통신이 IP 필터 목록의 조건과 일치할 때 활성화 되는 보안 동작들이 있습니다.
	보안 동작: - IP 터널링 특성 - 인증 방법 - 필터 동작
	계속하려면 [다음]을 클릭하십시오.
	< 뒤로(B) 다음(N) > 취소

17 다음 단계로 진행합니다.

IPsec 터널 직접적이면	은 공용 또는 개(서도 개인적인 5	인 네트워크의 패 2만 수준으로 이	킷 교환이 마치 ! 루어지도록 합니[두 컴퓨터 간의 연 나.	결에서처럼
IP 보안 규	칙의 터널 끝점을 에 나는 도너리 귀제	지정하십시오.			
이 나는 데	께서는 더될 시설 조소리 터널 끌게	3 안 얍(1) 3 지전(1):			
IPv4	부모모 더칠 같던 러널 끝점:				
I IPv6 I	러널 끝점:	5		_	



18 다음 단계로 진행합니다.

보안 규칙 마법사			×
네트워크 종류 네트워크 종류에 보안 규칙을 적용해야 합니다	ŀ.		
네트워크 종류를 선택하십시오.			
 ● 모든 네트워크 연결(C) ● LAN(Local Area Network)(L) ● 원격 액세스(R) 			
	< 뒤로(B)	다음(N) >	취소

19 [IP 필터 목록 > 추가] 하여, 필터링 할 port 를 지정합니다.

필요에 맞는 IP 필터가	'다음 목록에 없으면, [추가]{	를 클릭하여 새 필E	터를 만드십시오.
이름	설명		추가(A)
			편집(E),,,
			제거(8)

20 예시로 웹 접속에 대한 모두 허용 정책을 생성합니다.

IP 필터 목록				×
이 미 필터 목록은 하나의 미 필터	여러 필터로 구성됩니다 로 결합할 수 있습니다.	, 따라서, 다중 서보넷,	l, IP 주소, 프로토콜 등을	
이름(N):				19
웹 접속 (http)			추フト(A)	1
설명(D):			THE THE A	
			편집(디),,,	1
			제거(R)	
IP 필터(S):		•	▼ 추가 마법사 사용(₩)	26
미러됨 설명	원본 DNS 이름	원본 주소	대상 DNS 이를	
•		확인	▶ !취소]

21 다음 단계로 진행합니다.

IP 필터 마법사	>
IP 필터 설명 및 미러 속성 설명 필드를 사용하여 IP 필터의 이름이 각 방향의 필터를 지정하려면 [미러됨]	I나 자세한 설명을 지정하십시오. 확인란을 선택하십시오.
설명(D):	
웹 접속(http)	
	
🔽 미러됨. 원본 주소와 대상 주소가 정반대	H되는 패킷 연결(M)
	< 뒤로(B) 다음(N) > 취소





22 원본 주소 및 대상 주소 설정에서 모든 IP에서 허용되도록 설정합니다.



IP 필터 마법사	×
IP 트래픽 대상 IP 트래픽의 대상 주소를 지정하십시오.	
대상 주소(D): 모든 IP 주소	
	< 뒤로(B) 다음(N) > 취소



※ 특정 IP에서만 접속 할 수 있도록 설정할 경우, [원본주소 > 특정 IP 주소 또는 서브네트] 선 택 후, 접근 허용 IP를 설정해 주도록 합니다.

p				
원본 주 특정	소(S): 이주소 또는 서브너	IE		
IP 주소	: 또는 서브네트(I)	. <u>[111.111.111.11</u>	1	

23 프로토콜 종류를 선택합니다. 웹 서비스는 TCP 프로토콜을 이용하기 때문에, TCP 프토토콜을 선택 합니다.

IP 필터 마법사	×
IP 프로토콜 종류 IP 프로토콜 종류를 선택하십시오, 이 종류가 TCP 또는 UDP이면, 원본 및 대상 포트도 지정해야 합니다.	
프로토콜 종류 선택(S): TCP 6	
< 뒤로(B) 다음(N) > 취소	



iTEASY

24 서비스를 허용할 Port를 지정합니다. 웹 서비스의 경우 80 포트를 이용하기 때문에 80으로 지 정합니다.

IP 프로토 ⓒ 모든	[콜 포트 설정: 포트에서(F)		
	드에서(H): 푸트루(T)		
· 이 포 [80]	트로(0):		

25 IP 필터링 할 목록 생성이 완료되었습니다.

IP 필터 마법사	
	IP 필터 마법사 완료
	IP 필터 마법사를 완료했습니다.
	IP 필터를 지금 편집하려면 [속성 편집] 확인란을 선택하고 [마침]을 클릭하십시오,
	□ 속성 편집(P)
	마법사를 끝내려면 [마침]을 클릭하십시오.
	< 뒤로(B) 마침 취소



26 생성한 IP 필터링 목록을 허용/차단/보안접속 할 것인지 설정합니다.

안 규칙 마법사			100800, 2008.	
IP 필터 목록 이 보안 규칙이 적용될 IP 트래픽 종	류에 대한 IP 필	터 목록을 선	택하십시오,	
필요에 맞는 IP 필터가 다음 목록에	없으면, [추가]	를 클릭하여	새 필터를 만	드십시오,
IP 필터 목록(I): 이름 ☑ 웹 접속 (http)	실명	_		추가(A) 편집(E) 제거(R)
				-
		뒤로(B)	다음(N) >	취소

27 필터 동작 설정을 추가합니다.

아그치미배ル		
별터 동작 이 보안 규칙에 대한 필터	동작을 선택하십시오,	
필요한 필터 동작이 다음	: 목록에 없으면, [추가]를 클릭	하여 새 동작을 만드십시오. 마법
자를 사용하여 필터 동칙	을 만들려면 [추가 마법자 자용	:]을 선택하십시오.
필터 동작(C):		☞ 추가 마법사 사용(W)
이름	설명	추가(A)
		편집(E),
		제거(8)
	/ 티고	(B) 【 「P=(N) 〉 】 おん
	<u></u>	

iTEASY

28 다음 단계로 진행하도록 합니다.

필터 동작 마법사	×
	IP 보안 필터 동작 마법사 시작
	이 마법사를 사용하며 새 필터 동작의 속성을 지정할 수 있습니다.
	필터 동작은 데이터 전송 시 적용할 보안 사항을 설정합니다. 이 러한 사항은 필터 동작에 포함된 보안 방법 목록에 지정됩니다.
	같은 보안 방법을 사용하는 컴퓨터 간에만 데이터 전송이 가능 합니다. 여러 보안 방법을 선택하면 두 대의 컴퓨터가 같은 방 법을 사용할 가능성이 높아집니다.
	계속하려면 [다음]을 클릭하십시오.
	< 뒤로(B) 다음(N) > 취소

29 접속 허용 등 필터 동작 명을 지정 후, 다음 단계로 진행하도록 합니다.

접속허용		
설명(D):		A.
		_
		v
		11

30 허용 선택 후, 다음 단계로 진행하도록 합니다.





필터 동작 마법사	×
필터 동작 일반 옵션 필터 동작을 설정합니다.	
ⓒ 허용(E) ○ 거부(L)	
○ 보안 협상(S)	
	< 뒤로(B) 다음(N) > 취소

31 IP 보안 필터 동작 설정을 완료합니다.

필터 동작 마법사		×
	IP 보안 필터 동작 마법사 완료	
	IP 보안 필터 동작 마법사를 완료했습니다.	
	필터 동작을 지금 편집하려면 [속성 편집] 확인란을 선택하고 [마침]을 클릭하십시오.	
	□ 속성 편집(P)	
	마법사를 끝내려면 [마침]을 클릭하십시오.	
	< 뒤로(B) 마침 취소	1

32 생성한 필터 동작 선택 후, 다음 단계로 진행하도록 합니다.



필요한 필터 동작이 [사를 사용하여 필터 동)음 목록에 없으면, [추가] 종작을 만들려면 [추가 마법	를 클릭하여 새 동격 사 사용]을 선택하	작을 만드십시오, 마법 십시오,
필터 동작(C): 미르	[섬명		
⊙접속허용			편집(E)
			제거(R)

33 보안 규칙 설정을 완료합니다.

보안 규칙 마법사	×
	보안 규칙 마법사 완료
	새 규칙의 속성을 지정했습니다.
	지금 보안 규칙을 편집하려면 [속성 편집] 확인란을 선택하고 [마침]을 클릭하십시오.
	□ 속성 편집(P)
	마법사를 끝내려면 [마침]을 클릭하십시오.
	< 뒤로(B) 마침 취소





34 생성한 보안 규칙을 확인 할 수 있습니다.

 ' 보안 규칙(l):			
IP 필터 목록	필터 동작	인증 방법	티널 끝점
✔ 웹 접속 (http)	접속 허용	<없음>	없음

35 [속성 > IP 필터 목록 > 편집 > 규칙 편집 속성 > 편집] 에서 해당 IP 정책의 상세 내역을 확인 할 수 있습니다.

웹 접속	(http)								
설명(D):								<u></u>	까(A)
				*				편갑	입(E)
				*				제	거(R)
9 필터(8	S):			and a second				☞ 추가 마법사	사용(\
미러됨	설명	원본 DNS 이름	원본 주소	대상 DNS I	기름 대상 주소	원본 포트	대상 포트	프로토콜	
01I	웬 전속(httn)	<소주 및 금모>	<소주 위 금모>	주 ¶! 릉모>	소주 위 클모〉 <소	모두	80	TCP	



iteasy

36 허용해야 할 서비스 포트들을 모두 등록하신 뒤, 해당 포트 외에 다른 포트들은 모두 차단하도 록 설정합니다.

보안 규칙 마법사		×
	IP 보안 규칙 만들기 마법사 시작	
	보안 규칙은 언제 어떻게 보안을 적용할지 제어하는 것으로, 보 안 규칙의 IP 필터 목록에 있는 IP 트래픽 종류, 원본, 대상 등의 조건에 따라 결정됩니다.	
	보안 규칙에는, 통신이 IP 필터 목록의 조건과 일치할 때 활성화 되는 보안 동작들이 있습니다.	
	보안 동작: - IP 터널링 특성 - 인증 방법 - 필터 동작	
	계속하려면 [다음]을 클릭하십시오.	
	< 뒤로(B) 다음(N) > 취소	

37 다음	단계로 진행합니다. 보안 규칙 마법사 🛛
	터널 끝점 터널 끝점은 IP 트래픽 목적지에서 가장 가까운 터널링 컴퓨터로 보안 규칙의 IP 필터 목 록에 지정됩니다.
	IPsec 터널은 공용 또는 개인 네트워크의 패킷 교환이 마치 두 컴퓨터 간의 연결에서처럼 직접적이면서도 개인적인 보안 수준으로 이루어지도록 합니다.
	IP 보안 규칙의 터널 끝점을 지정하십시오. ⓒ 미 규칙에서는 터널 지정 안 함(T)
	○ 다음 IP 주소로 터널 끝점 지정(I): IPv4 터널 끝점:
	IPv6 터널 끝점:
	< 뒤로(B) 다음(N) > 취소



38 다음 단계로 진행합니다.

보안 규칙 마법사	×
네트워크 종류 네트워크 종류에 보안 규칙을 적용해야 합니	Eł.
네트워크 종류를 선택하십시오, ⓒ 모든 네트워크 연결(C) ⓒ LAN(Local Area Network)(L) ⓒ 원격 액세스(R)	
	< 뒤로(B) 다음(N) > 취소

39 새로운 IP 필터 목록을 추가 합니다.

IP 필터 목록(1):		
이름	설명	추가(A)
		편집(E)
		제거(8)

40 필터링 마법사를 통해 새로운 IP 필터 목록을 생성합니다.

IP 필터 마법사	×
	IP 필터 마법사 시작
	이 마법사는 IP 트래픽을 필터링하는 데 필요한 원본, 대상, 트 래픽 종류에 관한 정보를 제공하도록 도와줍니다.
	여러 필터를 추가하여 여러 원본 컴퓨터나 대상 컴퓨터 또는 여 러 트래픽 종류의 IP 패킷과 일치하는 IP 필터 목록을 작성할 수 있습니다.
	계속하려면 [다음]을 클릭하십시오.
	< 뒤로(B) 다음(N) > 취소

41 원본 주소 및 대상 주소를 모든 IP 주소로 설정 후, 다음 단계로 진행합니다.

열려 마법사		
IP 트래픽 원본		
IP 트래픽의 원본 주소를 지정하십시오.		
원본 주소(S):		
소주 <u>데 클모 </u>		
		-1.1
	< 뒤로(B) 다음(N) >	쥐소





P 필터 마법사			×
IP 트래픽 대상 IP 트래픽의 대상 주소를 지정하십시오.			
대상 주소(D):			
· 조수 데 르뫼			
	<뒤로(B)	다음(N) >	취소

42 프로토콜 종류를 [모두] 선택 후, 다음 단계로 진행합니다.

IP 필터 마법사	×
IP 프로토콜 종류 IP 프로토콜 종류를 선택하십시오, 이 종류가 TCP 또는 UDP이면, 원본 및 대상 포트도 지정해야 합니다.	
프로토콜 종류 선택(S): 모두	
< 뒤로(B) 다음(N) > 취소	

ITEASY IT is easy, ITEASY

43 설정된 내역을 아래와 같이 확인 할 수 있습니다.

IP 필터 목록	2			×
IP 필터 목록은 여러 필터로 구성됩니다. 따라서, 다중 서브; 	켓, IP 주소, 프로토콜 등을			
이름(N):				
모든 접속 차단				志7년(4)
설명(D):				
	<u> </u>			편집(E)
	<u>×</u>			제거(8)
IP 필터(S):				☑ 추가 마법사 사용(₩)
미러됨 설명 원본 DNS OI 를 원본 주소 예 모든 접속 차단 <모든 IP 주소> <모든 IP 주소>	대상 DNS 이름 대상 주소 〈모든 IP 주소〉 〈모든 IP	<u>원본 포트</u> 주소〉 모두	트 대상 포트 모두	프로토콜 모두
1			확인	인 취소
			확인	인 취소

필요에 맞는 IP 필터가 디	음 목록에 없으면, [추가]를 클릭;	하여 새 필터를 만드십시오.
IP 필터 목록(I): 이름 이데이터베이스 접속 (실명 MSSQL)	추가(A) 편집(E)
 ○ 원격터미널접속(RDF ○ 웹 접속 (http)))	제거(R)

44 IP 필터 목록 선택 후 다음 단계로 진행합니다.

45 필터 동작을 설정합니다.

안 규칙 마법사			Đ
필터 동작 이 보안 규칙에 대한 필터 -	동작을 선택하십시오.		
필요한 필터 동작이 다음 사를 사용하며 필터 동작을	목록에 없으면, [추가]를 클릭 한 만들려면 [추가 마법사 사	릭하며 새 동작을 만드 용]을 선택하십시오.	십시오, 마법
필터 동작(C):		교 추기	▶마법사 사용(₩)
이름	설명		추가(A)
0 접속 허용		[편집(E)
			제건(8)
	< 뒤로	로(B) 다음(N) >	취소

46 위에 추가하였던 허용을 제외한 모든 접속을 차단하는 부분으로 접속 차단 설정을 하도록 합 니다.

동작 마법사	
<mark>끌터 동작 이름</mark> 이 필터 동작을 명명하고 간단함	<u>!</u> 설명을 제공하십시오.
이름(M):	
집쪽 새릴	
실망(U):	
	-
	v
	1 and 1 a
	< <u>뒤도(D)</u> 다금(W) / 위소

47 필터 동작을 [거부] 선택 한, 뒤 다음 단계로 진행하도록 합니다.





필터 동작 마법사		×
필터 동작 일반 옵션 필터 동작을 설정합니다.		
 ○ 허용(E) ○ 거부(L) ○ 보안 협상(S) 		
-	< 뒤로(B) 다음(N) > 취소	

48 필터 동작 추가를 마칩니다.

필터 동작 마법사	×
	IP 보안 필터 동작 마법사 완료
	IP 보안 필터 동작 마법사를 완료했습니다.
	필터 동작을 지금 편집하려면 [속성 편집] 확인란을 선택하고 [마침]을 클릭하십시오.
	□ 속성 편집(P)
	마법사를 끝내려면 [마침]을 클릭하십시오.
	< 뒤로(B) 마침 취소

ITEASY IT is easy, ITEASY

49 생성한 접속 차단 선택 후, 다음 단계로 진행합니다.

iTEASY

보안 규칙 마법사	×
필터 동작 이 보안 규칙에 대한 필터 동작을 선택하십시오.	
필요한 필터 동작이 다음 목록에 없으면, [추가]를 클 사를 사용하여 필터 동작을 만들려면 [추가 마법사 /	를릭하며 새 동작을 만드십시오, 마법 사용]을 선택하십시오,
필터 동작(C):	☑ 추가 마법사 사용(₩)
이름	추가(A)
◎ 접속 차단	편집(E)
< 5	티로(B) [[[음(N) > 취소]]

50 모든 IP 차단 설정이 완료되었습니다.

보안 규칙 마법사	×
	보안 규칙 마법사 완료
	새 규칙의 속성을 지정했습니다.
	지금 보안 규칙을 편집하려면 [속성 편집] 확인란을 선택하고 [마침]을 클릭하십시오.
	□ 속성 편집(P)
	마법사를 끝내려면 [마침]을 클릭하십시오,
	< 뒤로(B) 마침 취소

4. IP 보안 정책 적용

51 해당 설정 적용 전 속성에 접속하여 등록된 부분을 확인합니다.



				[F II 4 22 74
기에저	古국 소 (bttp)	절대 중역 제조 체요	인동 방법 _ /어요\	이글 붙심
☑ 원격E ☑ 모든 [:] ☑ 데이E ☑ <동적	러미널접속 접속 차단 러베이스 >	접속 허용 접속 차단 접속 허용 기본 응답(미전	<없음> <없음> <없음> Kerberos	없음 없음 없음 <없음>

52 [정책명 > 마우스 우클릭 > 할당]으로 정책을 적용합니다.

🖺 로컬 보안 정책				
파일(F) 동작(A) 보기(V) 도움말(H)				
🗢 🔿 🖄 📅 💥 🖬 😖 🛛 🖬 🗍	1 🔂 🔁			
🛓 보안 설정	이름 👻	설명	정책 할당	마지막 수정한
 ⊞ Ⅲ ▲ 로컬 정책 		할당(A)		2011-11-15 오
⊞ 🧰 고급 보안이 포함된 Windows 방화벽 네트워크 목록 관리자 정책		모든 작업(K) →		
 ·····························		삭제(D) 이름 바꾸기(M)		
IP 보안 정책(위치: 로컬 컴퓨터)		속성(R)		
표 🧰 고급 감사 성책 구성		도움말(H)		

53 정책이 아래와 같이 허용된 것을 확인 할 수 있습니다.

iTE∧SY

🖥 로컬 보안 정책				_ 🗆 🗵
파일(F) 동작(A) 보기(V) 도움말(H)				
🔙 🔿 🛛 🖬 🔒 🛛 🖬 🖄 🎰				
🔒 보안 설정	이름 🔻	설명	정책 할당	마지막 수정한
🗉 📴 계정 정책	KSIDC		ଜା	2011-11-15 오
🗉 📴 로컬 정책				
🗉 🧾 고급 보안이 포함된 Windows 방화벽				
🛄 네트워크 목록 관리자 정책				
🗉 🧮 공개 키 정책				
🗉 🦲 소프트웨어 세한 성책				
표 🦲 응용 프로그램 세너 성책				
- 영 IP 모안 성책(위지: 로칠 컴퓨터)				
표 🔤 끄급 감사 장색 구장				

5. 정책 백업/복구



iteasy

54 추후, 재설정이 필요할 수 있기 때문에 기존 설정을 백업하도록 합니다.

정책 내보내기 설정을 통해 정책을 백업하도록 합니다.

🖺 로컬 보안 정책					_ 🗆 🗙
파일(F) 동작(A) 보기	(∀) 도움말(H)				
🗢 🔿 🖄 📅 🗖 🖬	» 🛛 🖬 🏦 :	<u>1</u>			
불 보안 설정 값 계정 정책 값 로컬 정책 값 로컬 정책 값 대트워크 목록 관리 값 대트워크 목록 관리 값 ご 공개 키 정책 값 ご 소프트웨어 제한 정 값 ご 유비 위전 적석(위치) 값 ご 고급 감사 정책 구	! Windows 방화벽 자 정책 ! 정책 P 보안 정책 만: P 필터 목록 및	0I를 ▼	설명	<u>정책</u> 할당 예	마지막 수정한 2011-11-15 오
	모든 작업(K) 보기(V)	•	IP 보안 정책 만들기 IP 필터 목록 및 필 정책 가져오기(!)	기(C) 터 동작 관리(M)	
	새로 고침(F) 목록 내보내기(L	J	정책 내보내기(E)		
	도움말(H)				

55 백업 경로 및 백업 파일 이름을 지정하도록 합니다.

> ○ ▽ 📃 바탕 화면	• 🛛 🕶	바탕 화면 검색 🚺
구성 ▼ 새 폴더		
☆ 즐겨찾기 ▲ 다운로드 ■ 바탕 화면	라이브러리 시스템 폴더	
1 최근 위치 1 라이브러리	Administrator 시스템 폴더	
 달성 ■ 비디오 ■ 사진 	12 컴퓨터 시스템 폴더	
♪ 음악 ,♥ 컴퓨터	네트워크 시스템 폴더	
📬 네트워크 👤	i crm_con 파일 폴더	
파일 이름(N): KSID	C_ipsec_backup	
파일 형식(T): IPse	c 정책 파일	

56 저장된 정책으로 복구할 경우 정책 가져오기를 통해 복구를 진행하면 되십니다.