제목 : IPSec 을 이용하여 특정 IP 및 트래픽 제어하기

목차

이번에는 윈도우 2000 에 필터링 서비스에 대한 좀 더 상세하게 알아 보겠다.
그 외 IP 보안 정책에 대한 좀 더 자세하게 얻을 수 있을 것이다. 얼마 전 제공 된 "IP 보안정책으로 Telnet 서비스 구축 하기 " 정보는 서버와 클라이언트에 대한 인증된 사용자만 접속 할 수 있는 정보이니 참고 하길 바란다.
그외 **특집 연재 강좌 : 윈도우 2000 누구나 쉽게 이해 하기** 을 참고 하시면 됩니다.

1.IP 보안 정책 개요

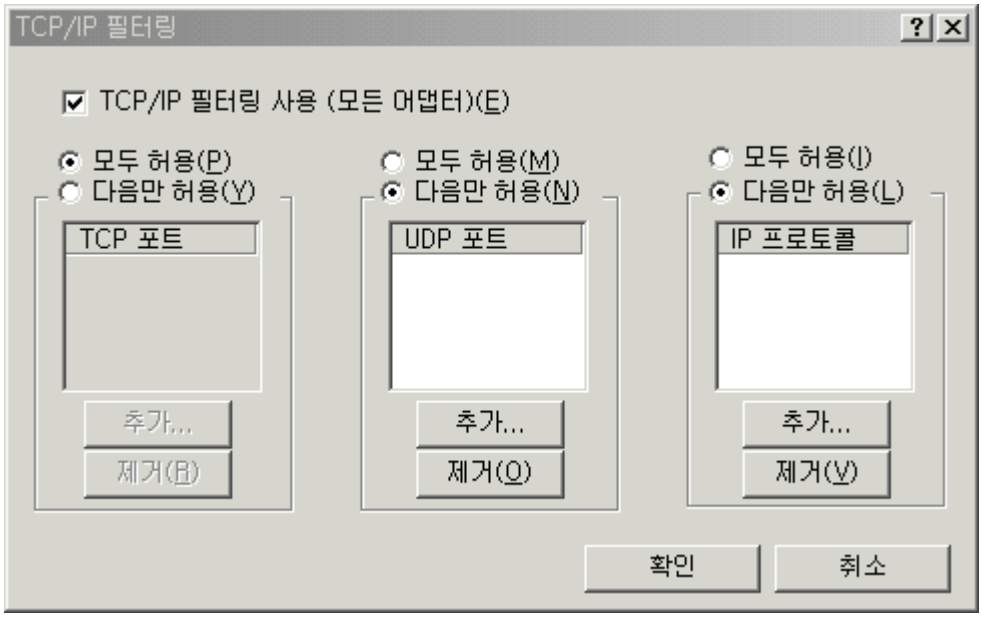
안녕하세요? 주원 아빠입니다.
이번 강좌는 Windows 2000에서 제공되는 트래픽 제어 기능에 대해서 다룹니다. 트래픽 제어에 관련된 기능에는 TCP/IP 필터링 과 IPSec 이 있습니다.

일반적으로 TCP/IP 에서 제공 되는 기본 필터링 방식 보다는 IPSec 에서 제공 되는 것은 다소 쉽게 구성을 할 수 있고 유연하게 할 수 있다고 할 수 있다.
그렇게 함으로서 필요 없는 IP 및 TCP 에 대한 정보를 쉽게 필터링 할 수 있는 기능이라고 생각하면 된다.

두가 지의 가장 큰 차이점을 다시 한번 언급하면,

기 능	IPSec 정책	TCP/IP 필터링
범 위	특정 주소/인터페이스에 적용가능	모든 Interface에 동일하게 적용
원본 주소	정책의 일부로 적용 가능	해당 사항 없음
재부팅 여부	해당 사항 없음	재부팅 해야 적용됨
차단된 트래 픽의 응답	없어짐(Discard) – 즉, 서버가 없는 것처럼 보여짐.	리 셋이 반환됨.
IPSec Policy Agent 클라이언트	필요	필요 없음

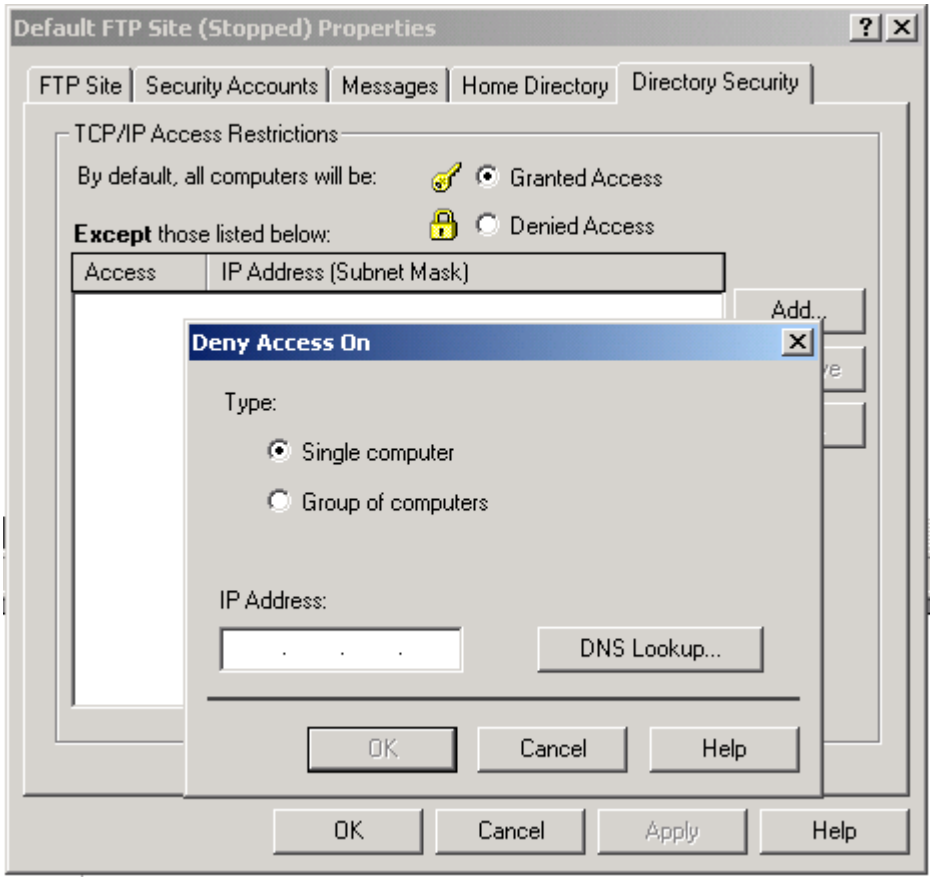
또한, 강좌란 을 보시면 ICMP 프로토콜을 차단하는 IPSec 예제 (http://www.ntfaq.co.kr/security/view.asp?pid=13) 가 있습니다.
Windows 2000에 ICMP 프로토콜을 차단하기 위한 리스트가 존재하지만, 사용법을 좀더 알아보기 위해 수동으로 직접 만들어 본 것 입니다. 한번 천천히 따라 해 보시면 아~ 그렇구 하고 이해가 되실 것입니다.



[그림 윈도우 2000 TCP/IP 등록정보에 제공 되는 기본 필터 링 서비스]

2. 주요 서비스 액세스 제어

Windows 2000에서는 대부분의 서비스에 액세스를 제한 또는 허가할 수 있는 기능이 포함되어 있습니다. 대표적인 예를 들어 보면, IIS 의 FTP를 보시면 등록정보에 특정 IP/ 대역 을 허가 또는 차단하는 기능이 있습니다. (아래 그림 참조)

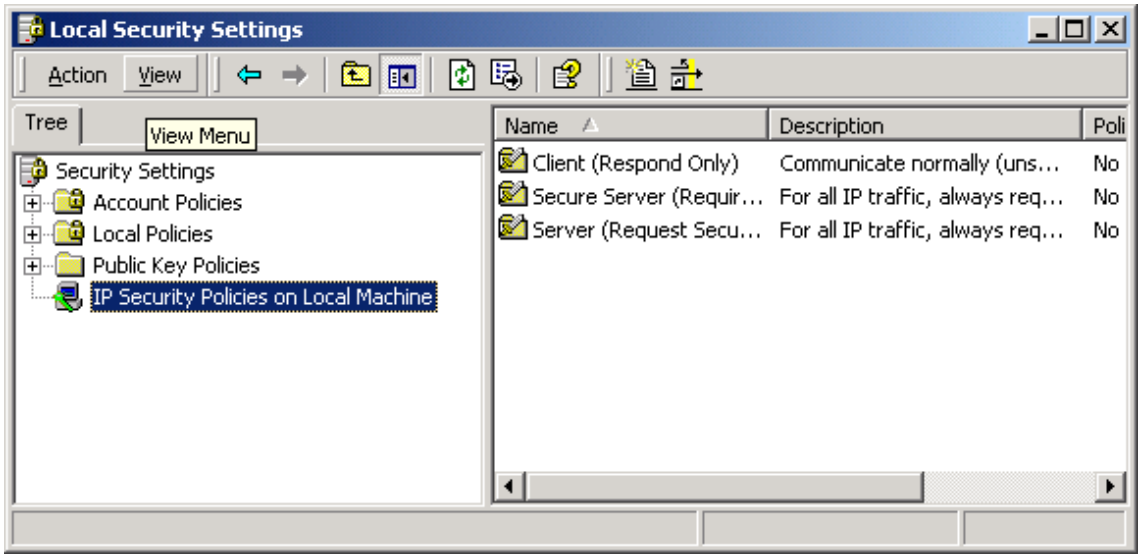


이 외에도 각각의 서비스를 주의 깊게 살펴보면, 액세스를 허가/차단 할 수 있는 기능을 볼 수 있습니다. 이것은 여러분의 몫으로 놔두죠. 그리고, 이에 관한 정보를 일목요연하게 정리해주실 분~ 적극 환영입니다.

3. IPSec을 이용하여 트래픽 제어

IPSec 정책은 다른 서비스와 달리 조금 복잡합니다.
IPSec 정책은 액티브 디렉터리 서비스에 그룹정책 서비스와 독립형 서버로 분리해서 사용 할 수 있다. 다소 차이는 있겠지만 일괄적인 관리 정책으로 구성 하지 못하는 것과 커버로스를 사용 할 수 없다는 점 이외에는 거의 유사하게 사용 할 수 있다.
위 말은 다소 차이가 있으며, 앞으로 계속 해서 새로운 정보와 글을 소개 되면서 좀 더 유연하게 설명 할 수 있을 것이라 생각 된다.
이번 주요 글은 독립형 서버를 기준으로 할 것이다.

먼저 IPSec이 어디에 있는지 살펴보죠. IPSec은 시작→프로그램→관리도구→로컬 보안 정책 내에 있습니다.



IPSec 정책을 구현하려면,

1. **필터 : 어떠한 트래 픽을 필터링 할지를 여부 결정**
2. **동작 : 필터에 만족하는 트래 픽을 허가/거부 등등의 동작을 결정**
3. **정책 : 필터와 동작을 결합하여 정책으로 구현.**

이렇게 3단계로 나뉩니다.

이제 특정 IP 차단을 위한 IPSec 정책을 구현해 보도록 하겠습니다. 일단 차단할 IP를 10.0.0.2, 트래 픽의 종류는 TCP라고 가정합니다.

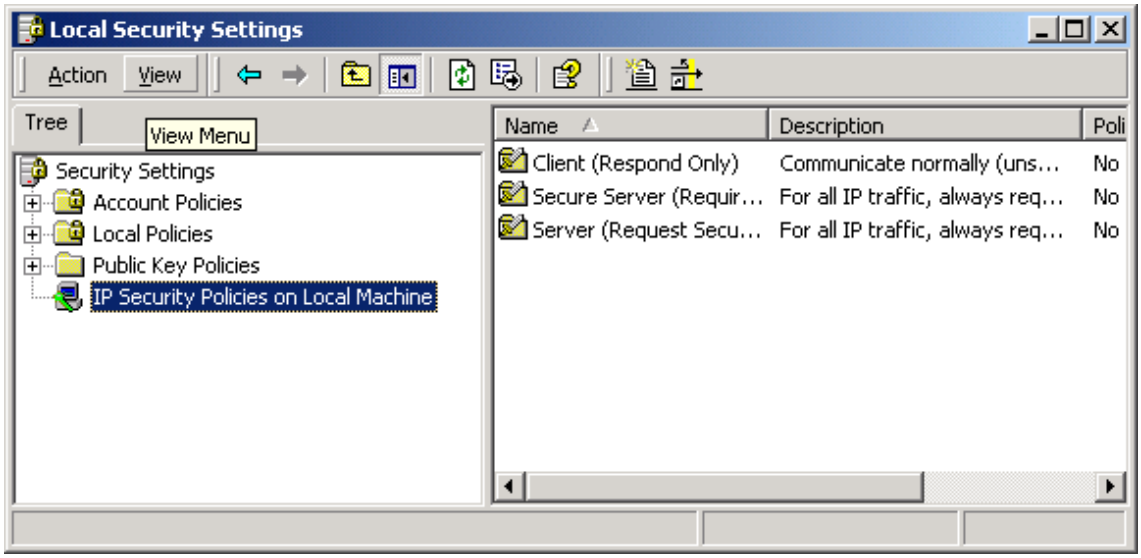
① 기본 IPSec 정책 설명

- □ 보안 서버 (보안 필요)
  - ■ 가장 높은 수준의 기본 보안이 요구될 때. 이 IPSec 정책은 IPSec에 의하여 보호될 수 없는 프로토콜을 제외하고 모든 프로토콜에 IPSec이 사용될 것을 요구한다. 서버로 전달되는 모든 트래 픽이 IPSec을 사용하여 보호되어야 한다. 가능하지 않은 경우 보호되지 않는 데이터 전송으로 수준을 낮추어 통신하는 것이 허용되지 않는다..윈도우 2000 기반 컴퓨터 만이 서버에 연결할 필요가 있다.IPSec 설정을 필요로 하는 모든 서버가 같은 OU 또는 OU 구조에 위치한다
- □ 서버 (보안 필요)
  - ■ 서버로 전달되는 모든 트래 픽이 IPSec을 사용하여 보호되어야 한다.구형 클라이언트를 위하여 가능하지 않은 경우 보호되지 않는 데이터 전송으로 수준을 낮추어 통신하는 것이 허용된다. 서버가 윈도우 2000과 비 윈도우 2000 클라이언트의 조합을 지원해야 한다.IPSec 설정을 필요로 하는 모든 서버가 같은 OU 또는 OU 구조에 위치한다.
- □ 클라이언트 (응답)
  - ■ 서버가 요청할 경우 윈도우 2000 컴퓨터가 IPSec 보호를 사용할 수 있도록 하기 위하

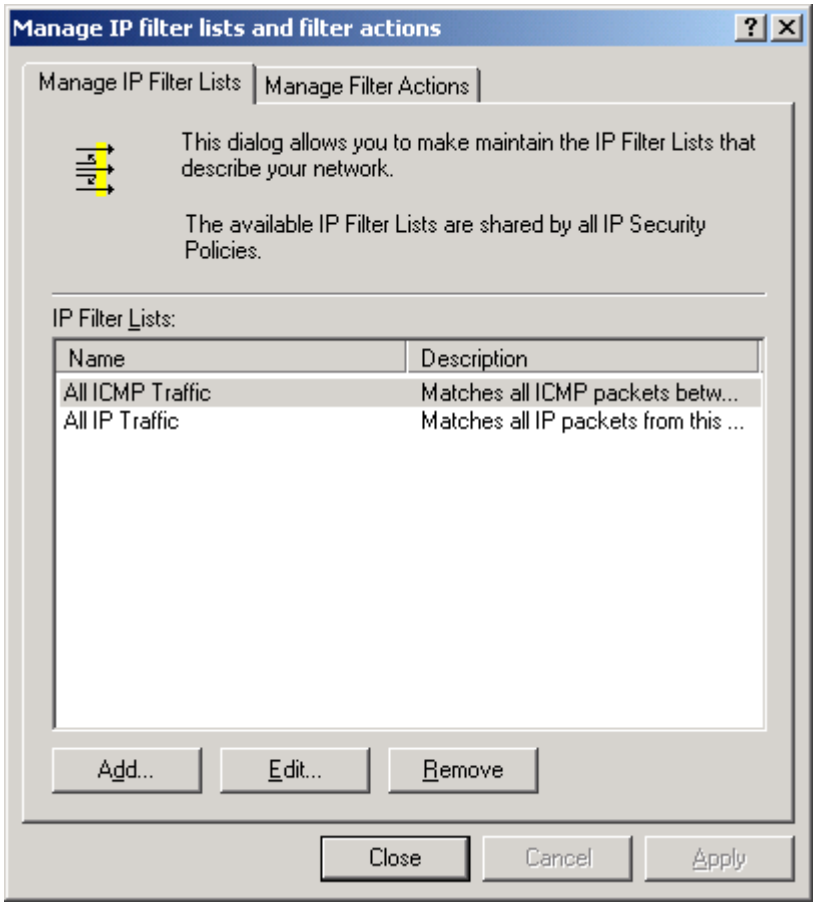
여 클라이언트 컴퓨터가 IPSec 보호를 초기화하지 않아야 한다.OU 또는 OU 구조 내부의 모든 컴퓨터에 IPSec 보호가 활성화되어 있다고 판단한 경우

② 필터 결정하기

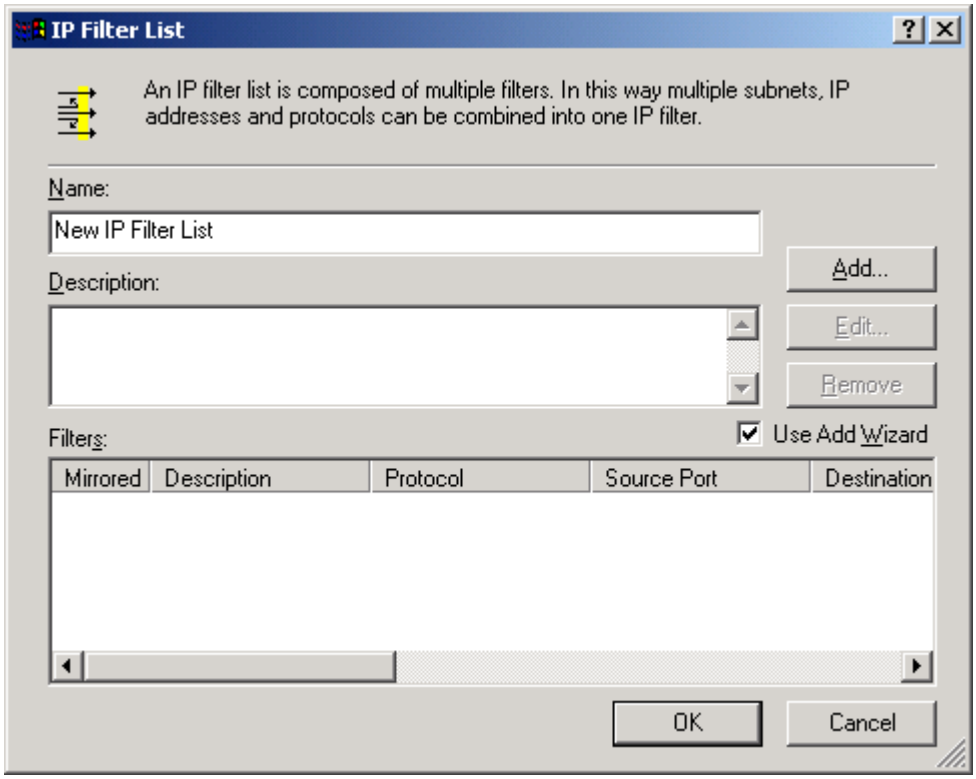
1. **시작→프로그램→관리도구→로컬 보안 정책** 을 실행하여 로컬 보안 정책 윈도우를 엽니다.



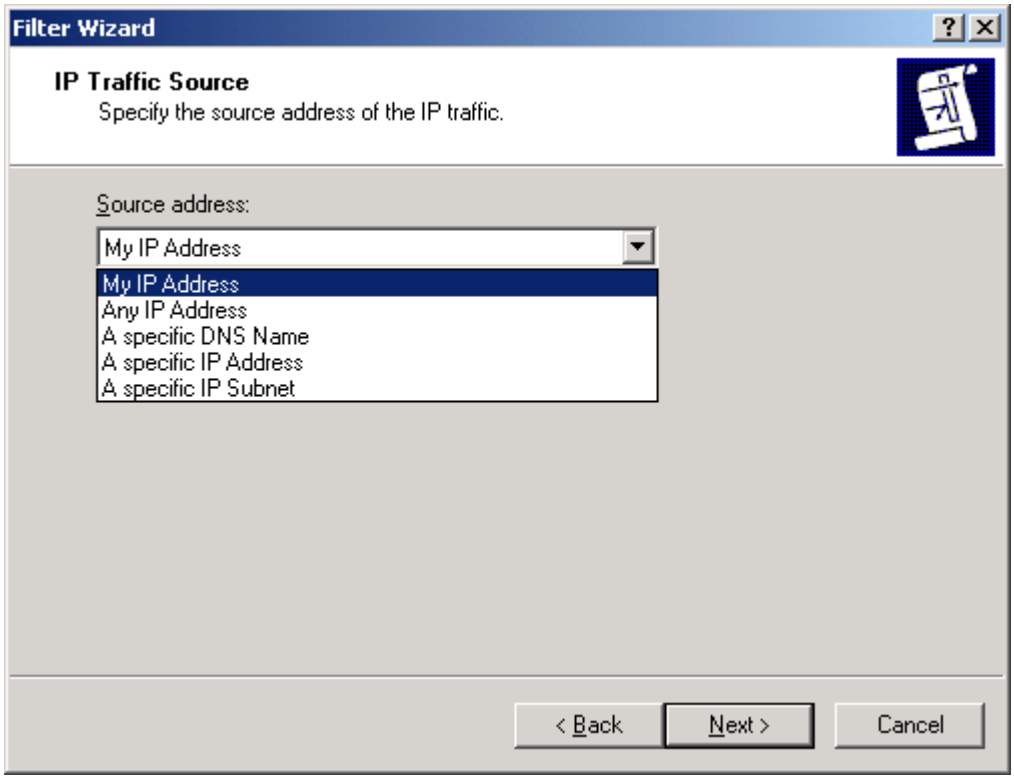
2. 왼쪽 창의 IP Security Policies on Local Machine 에서 오른 클릭하여 Manage IP Filter Lists and Filter Actions 을 선택합니다. 그러면 다음과 같은 화면을 볼 수 있습니다.



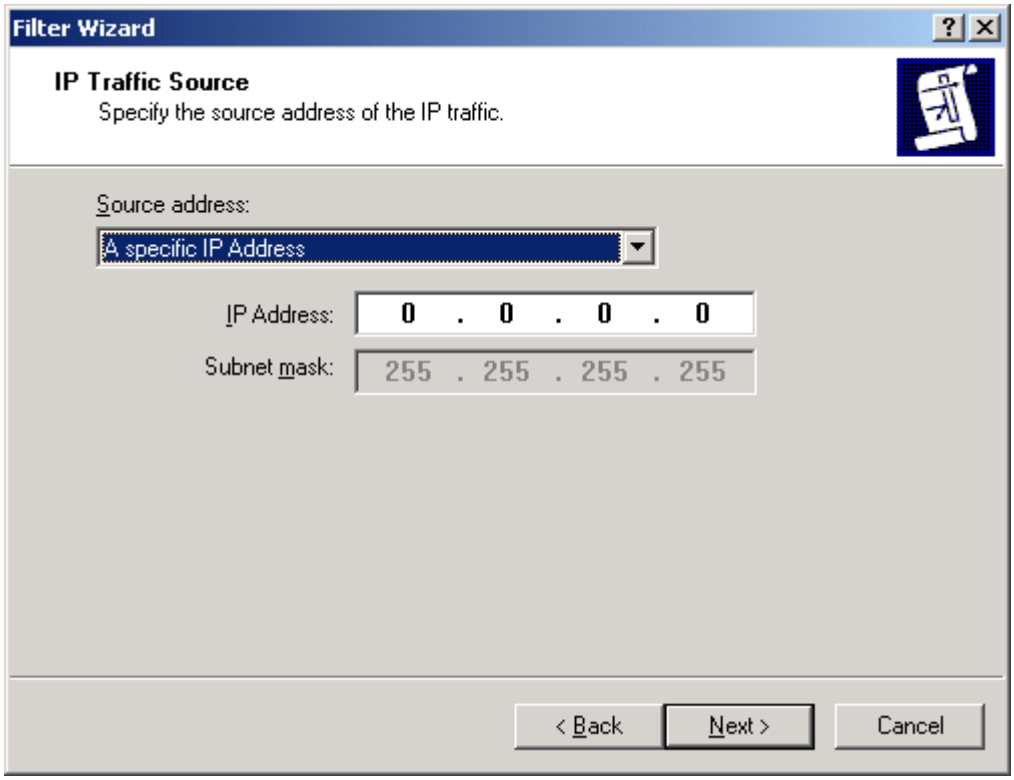
4. Add 버튼을 클릭합니다.



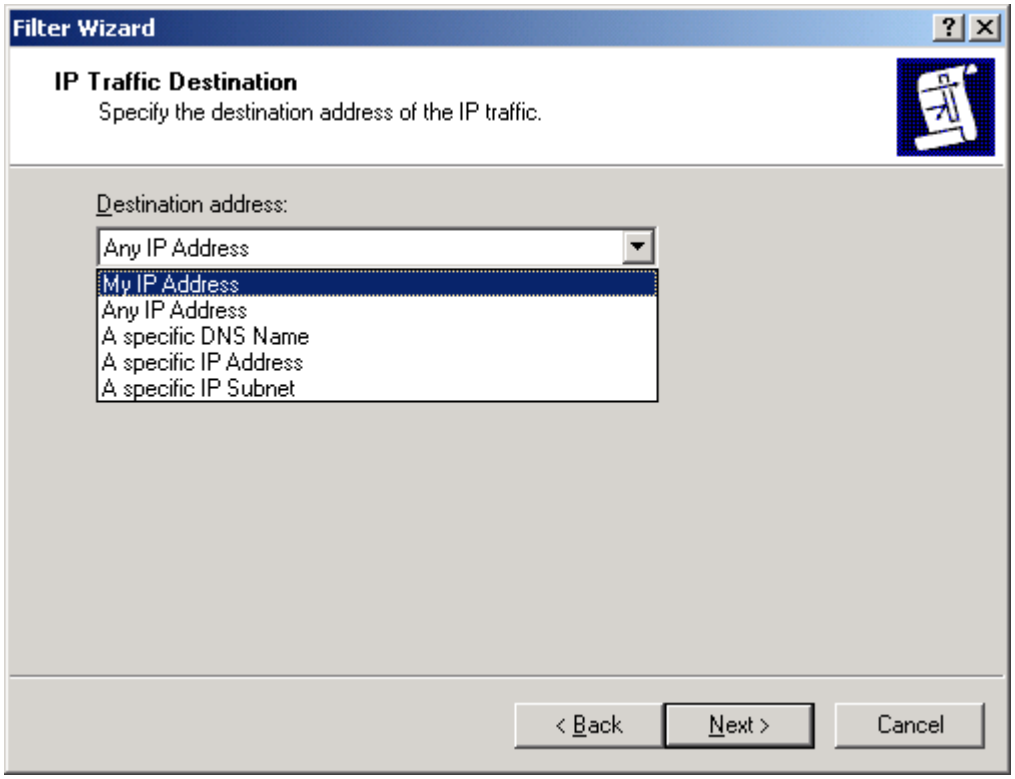
5. IP Filter List 대화상자에서 Add 버튼을 클릭합니다. 그러면 IP Filter 마법사 대화상자가 나옵니다. Next 을 클릭하고, IP traffic Source 부분에서 차단할 IP 주소를 입력해줍니다.



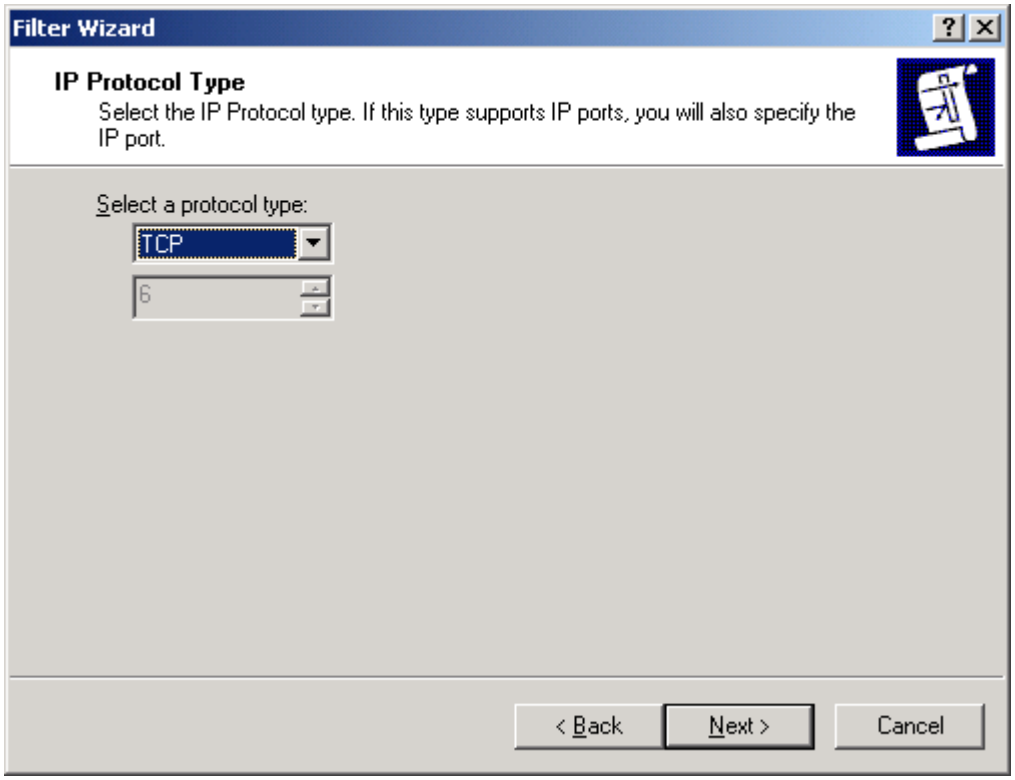
특정한 IP 주소를 차단하려고 할 때에는 A specified IP Address 을, 또한 특정 IP 대역대를 차단하려고 할 때에는 A specified IP Subnet을 선택합니다. 여기서는 A Specified IP Address 을 선택했습니다.



6. 차단할 IP를 입력해 주고 **Next** 을 클릭합니다. 그러면 IP Traffic Destination 대화상자가 나타나는데 여기서 **My IP Address** 을 선택합니다. (Any Ip Address 을 선택해도 관계없습니다.)



7. 다음은 트래 픽의 종류를 선택하는 대화상자 입니다. 우리가 차단하려고 하는 것은 TCP 이므로 메뉴에서 골라줍니다. TCP의 프로토콜 번호는 6번 입니다.

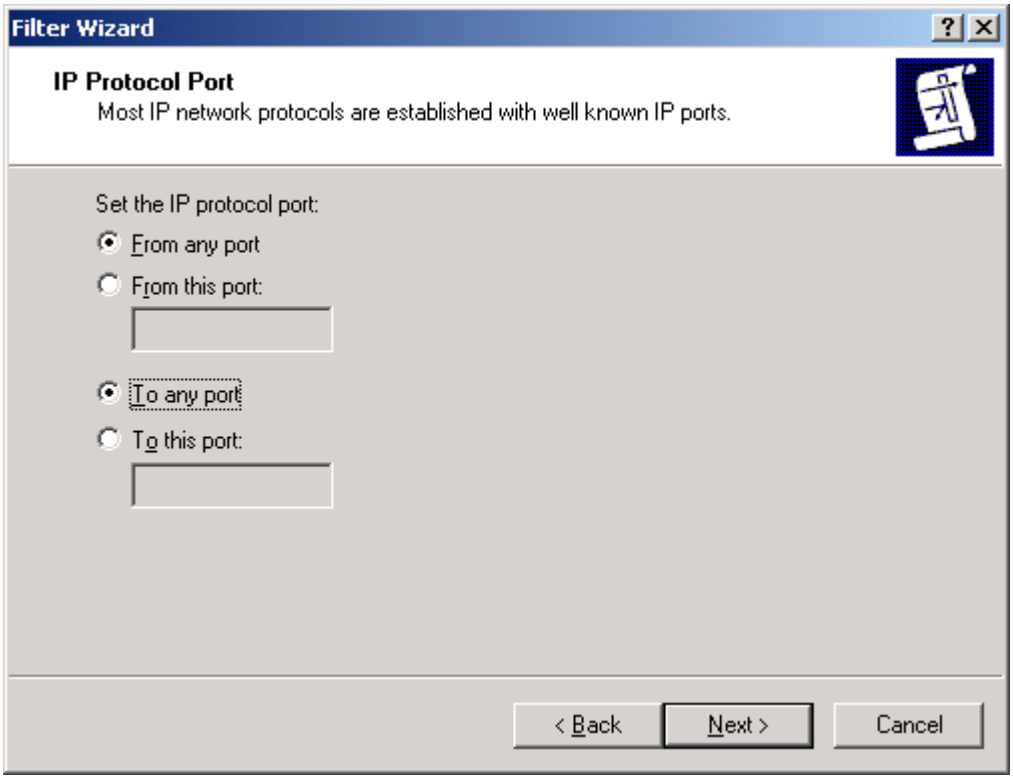


8. 다음은 IP 프로코톨의 포트를 설정해 주는 화면이 나타납니다. 만약, SMTP를 차단하고자 한다면 25번을 그리고 메신저와 같은 특정한 애플리케이션의 송수신을 차단하려면 해당 포트를 차단해 줍니다. 여기서는 특정 IP의 모든 TCP 트래 픽을 차단하기 때문에 아래와 같이 구성합니다.

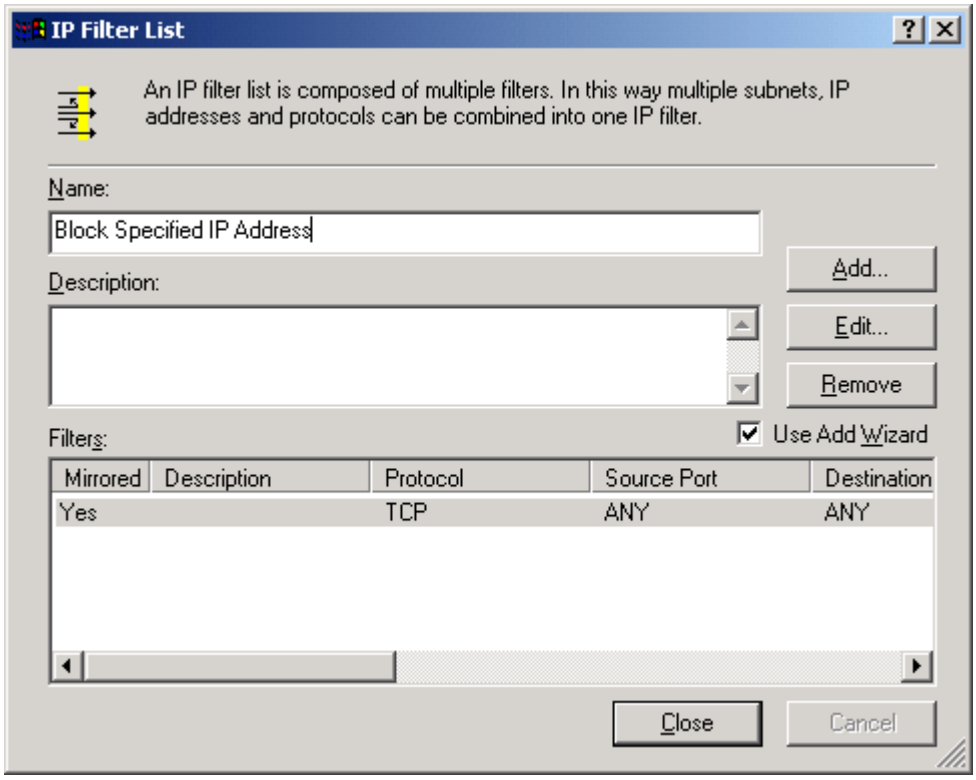
애플리케이션이 사용하는 포트는 다음 URL을 참고하시면 됩니다.

http://www.sygate.co.kr/Apprule.cfg

예를 들어, MSN 메신저는 TCP 1863 을 차단합니다.



9. 마지막으로 완료 대화상자가 나옵니다. Finish 을 클릭합니다. Name 부분을 아래 그림과 같이 변경합니다. 나중에 알아보기 쉽게 하기 위해서 입니다. 마지막으로 Close 을 선택하여 창을 닫습니다.

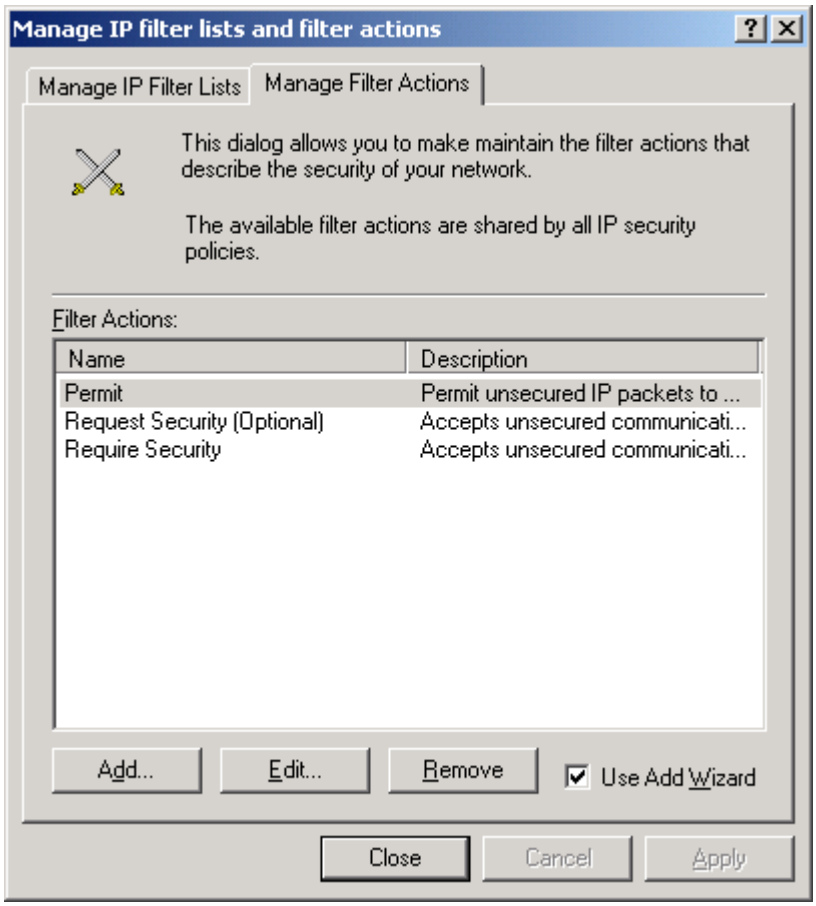


③ 동작 결정하기

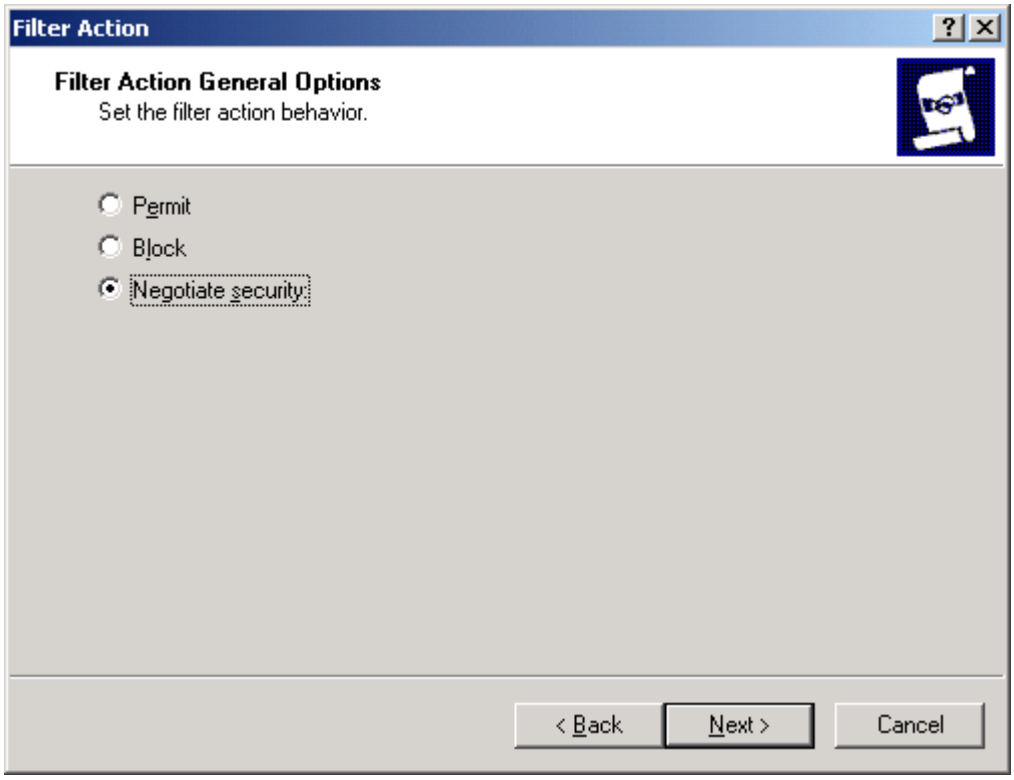
동작에는 허용(Permit) , 협상(negociate) 등의 다양한 동작이 포함됩니다. 이들은 대부분 Active Directory에서 사용됩니다. 물론, 인증서 서비스를 구현하거나 미리 공유된 키를 사용하여 사용할 수 있지만, 여기서는 "차단" 이 목적이므로, 특정 트래 픽이 수신되었을 때 이 트래 픽을 차단하는 동작에 대해 구성해 보도록 합니다.

1. **시작→프로그램→관리도구→로컬 보안 정책** 을 실행하여 로컬 보안 정책 윈도우를 엽니다. 그리고 왼쪽 창의 IP Security Policies on Local Machine 에서 오른 클릭하여 Manage IP Filter Lists and Filter Actions 을 선택합니다. 좀 전과 동일한 화면을 볼 수 있습니다.

2. 아래와 같이 Manage Filter Actions 탭을 선택합니다. 현재 동작에는 허용, 보안 요청(옵션), 보안 필요 이렇게 3가지 동작만이 존재합니다. 여기에 차단 이라는 동작을 추가하는 것입니다.



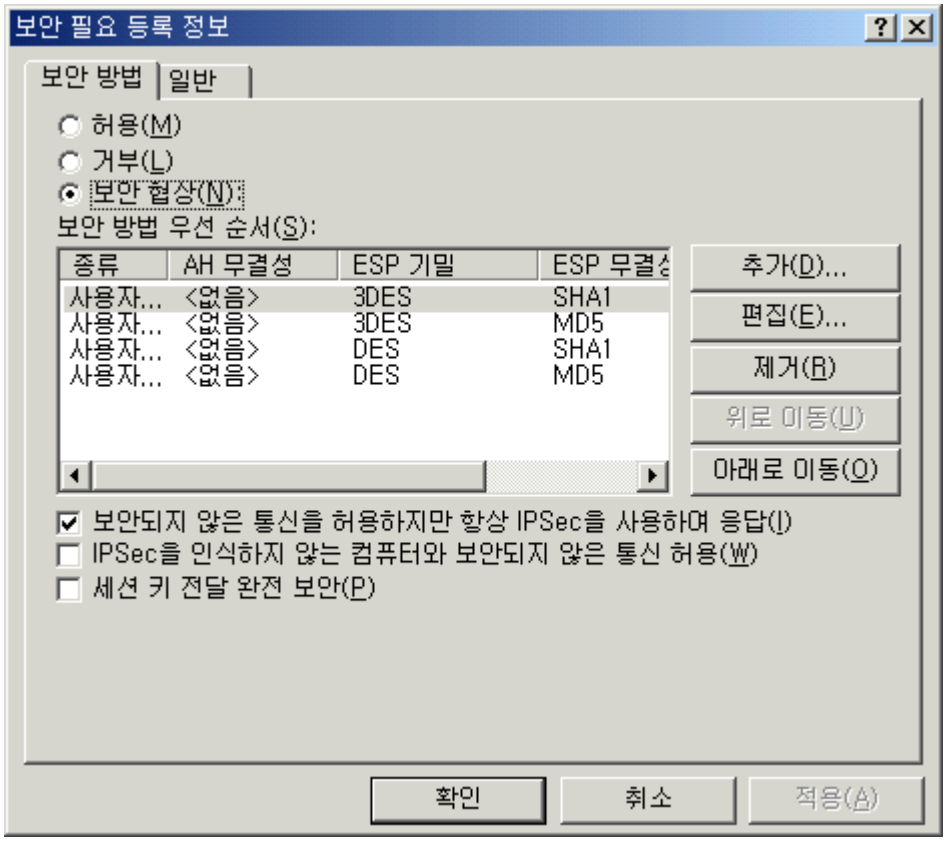
3. Add 버튼을 클릭하면, Filter Action 마법사 화면이 나옵니다. Next 을 클릭합니다. 필터 동작의 이름을 적어줍니다. 여기서는 Block TCP Traffic 이라고 적어주고, Next 을 클릭합니다. 그러면 다음과 같은 화면이 나타납니다.



4. 여기서 Block 을 선택합니다. 그리고 Next 을 클릭합니다. 마지막으로 Finish 을 클릭합니다. 이로서 차단 동작을 구성하였습니다. **마지막으로 필터 와 동작 을 이용하여 정책을 구현하는 것입니다.**

5. Close 을 클릭하여 화면을 닫습니다.

동작	주요 내용
허용	□ IPSec 보호 없이 전송 한다.클라이언트나 서버에서 암호화되지 않은 데이터 전송을 허용하고자 할 때. 프로토콜이 암호화되지 않아야 할 때 이 동작을 사용한다
거부	□ IPSec 필터와 일치 하는 프로토콜이 네트워크 상의 존재 할 수 없도록 제한 하는 것
보안 교섭	□ IPSec 필터가 일치 할 때, 데이터 전송의 보안을 위해 사용되어야 하는 암호화 알고리즘과 해시 알고리즘을 관리자가 제공



[그림. IPSec 보안 필요 등록 정보 화면]

그 외 추가적인 기능 설명

세부 기능	주요 설명
보안 되지 않는 통신을 허용하지만 항상 IPSec 사용 하여 응답	이 옵션은 IPSec 보호가 클라이언트가 아닌 서버에서만 강제될 때 사용한다. 전형적인 IPSec 전개에서, 클라이언트들은 서버에서 요청 받는다면 IPSec을 사용하도록 설정되어 있으며, IPSec SA을 시작하지는 않는다. 이 설정은 초기 패킷이 서버에서 수신되고, 그 다음 클라이언트와 서버간에 SA을 교섭하는 IKE 프로세스가 시작되도록 한다. 일반 텍스트를 사용하는 데이터 전송의 초기 패킷을 수락하는 것이 좀 위험하지만, SA가 성립될 때까지는 서버의 응답 패킷은 전송되지 않는다.
IPSec 을 인식하지 않는 컴퓨터와 보안 되지 않는 통신 허용	혼합 네트워크에서, 이 옵션은 IPSec을 인지하지 못하는 클라이언트들이 서버에 연결할 수 있도록 한다. 이렇게 설정되었다면 윈도우 2000 클라이언트는 서버에 연결하고 IPSec SA를 교섭한다. 한편 비-IPSec 클라이언트는 보호되지 않은 데이터 스트림으로 여전히 통신할 수 있다.
세션 키 전달 완전 보안 (Session Key Perfect Forward Secrecy)	IPSec 패킷에 대한 데이터 암호화는 세션 키를 사용하여 제공된다. 이 동작은 기존의 키가 새로운 키의 생성에 절대로 사용되지 않도록 한다. 모든 키는 기존의 키를 사용하지 않고 생성된다. 이 동작은 이전의 키로 새로운 키를 판별할 수 없으므로, 키에 대한 노출 위험을

	줄인다.

위에서 **인증 방법**을 선택 하는 곳이 있을 것이다. 물론 협상정책을 선택 해야만 적용 할 수 있으며, 그럴 경우는 3가지 인증 방식을 선택 할 수 있다.

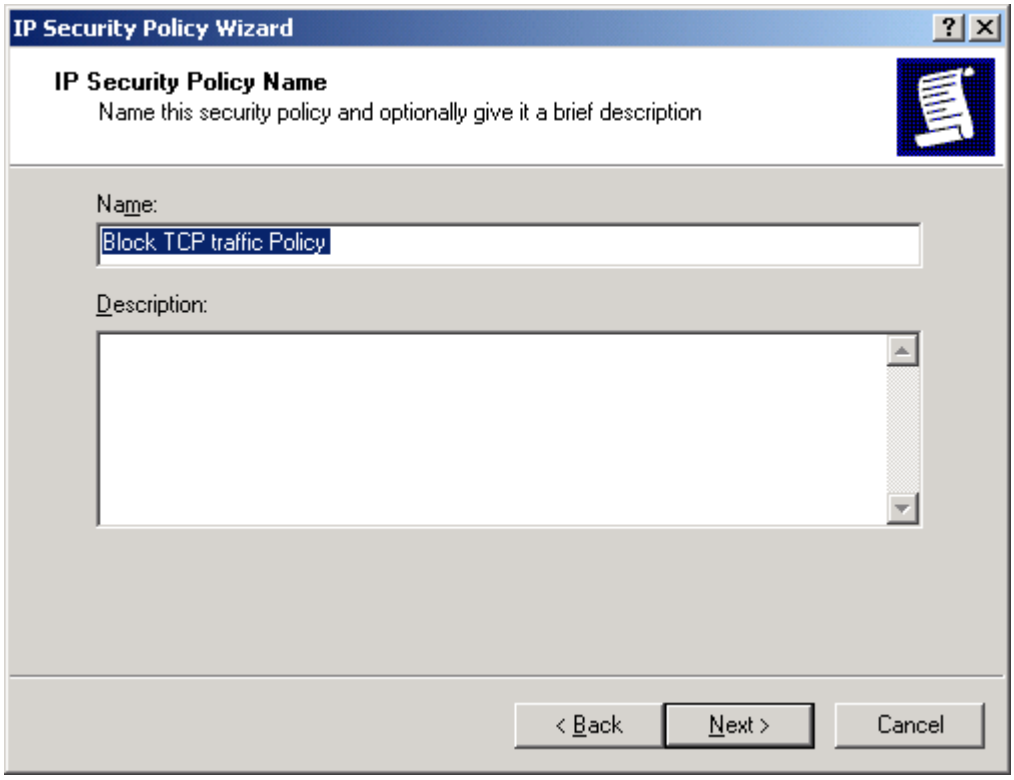
인증 방법	주요 내용
Kerberos	□ 액티브 디렉터리 포리스트의 멤버인 경우
인증서	□ 액티브 디렉터리 및 독립형 서버 모두 적용 가능, 그 외 인증키를 받아서 적용도 가능함 □ 같은 포리스트에 있지 않는 호스트 간의 강력한 인증을 하고자 할 경우 □ VPN 솔루션에 L2TP/IPSec을 사용하고자 할 때. L2TP/IPSec은 인증에 사용되는 컴퓨터 인증 서를 필요
미리 공유된 키 (Preshared keys)	□ 커버로스나 인증 서를 사용할 수 없는 상황 □ 일반적으로 인증 서비스 테스트를 할 경우 적용됨 □ 두 호스트간에 IPSec SA를 설정하였고, 이 SA가 두 호스트 사이에서만 존재할 때.

④ 정책 구현하기

정책 구현은 아주 간단합니다. 이전에 구성한 필터 와 동작을 서로 일치시켜 주면 됩니다.

1. **작→프로그램→관리도구→로컬 보안 정책** 을 실행하여 로컬 보안 정책 윈도우를 엽니다. 그리고 왼쪽 창의 IP Security Policies on Local Machine 에서 오른 클릭하여 Create IP Security Policy 을 선택합니다.

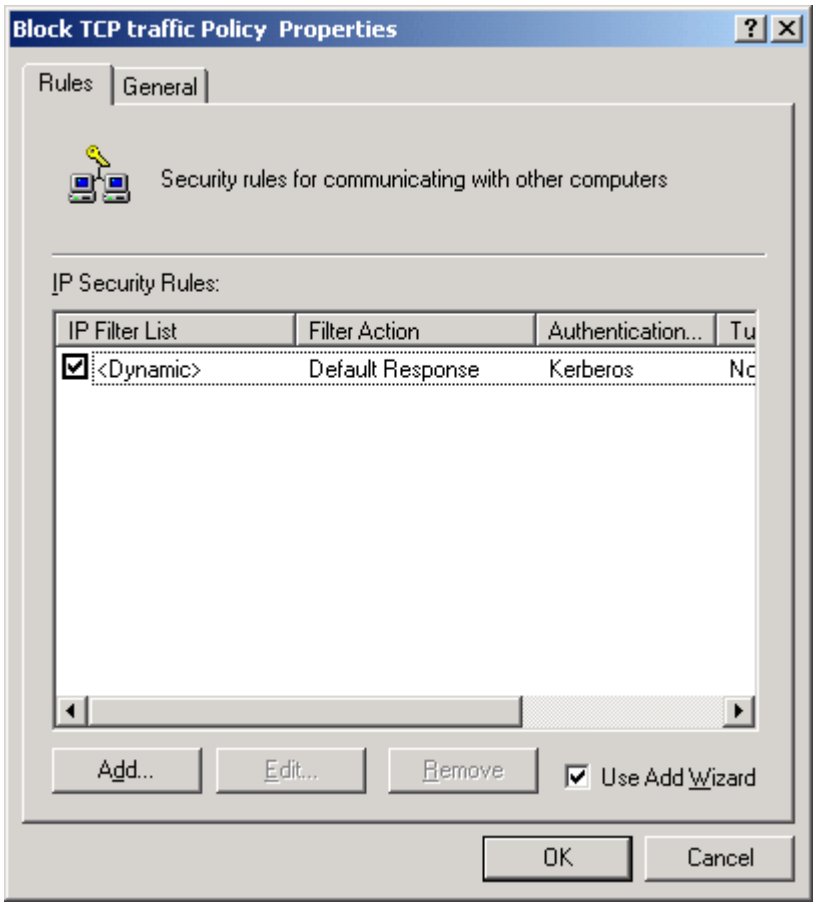
2. IP Security Policy 마법사가 나오는데 Next 을 클릭합니다. 정책의 이름을 설정할 수 있는 대화상자가 나타납니다. 여기서는 Block TCP traffic Policy 이라고 적고 Next 을 클릭합니다



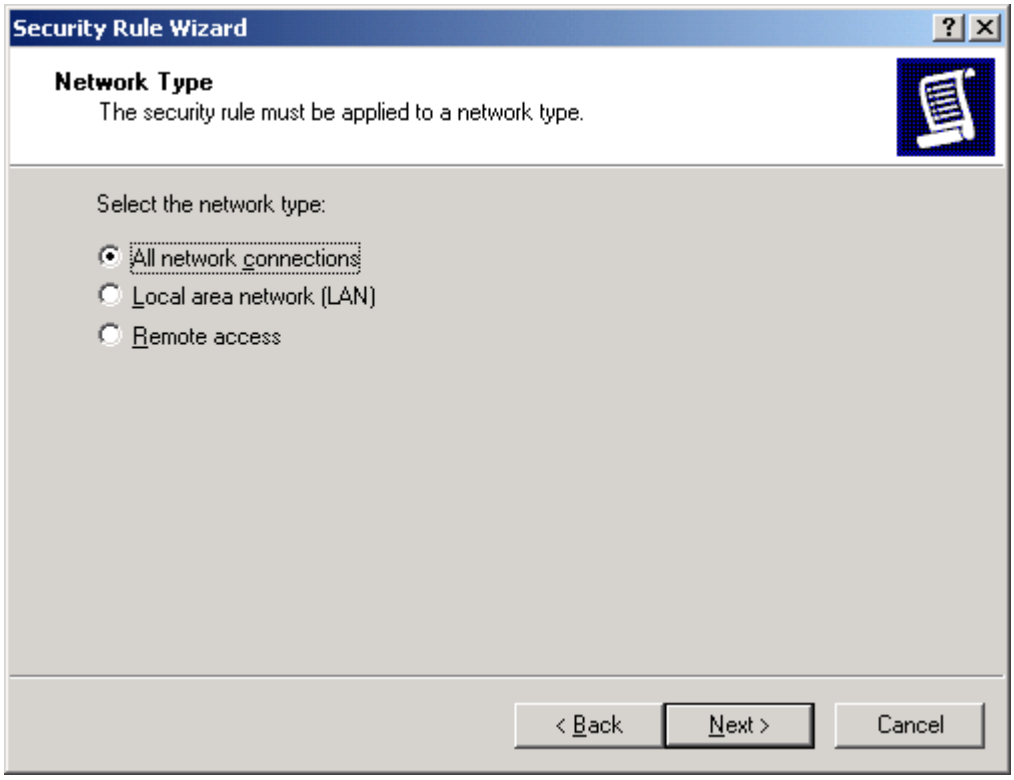
3. Request for Secure Communication 화면이 나오는데 그냥 무시하고 Next 을 클릭합니다.

4. Default Response Rule Authentification Method 화면에서 Windows 2000 Default(Kerberos V5 Protocol) 을 선택하고 Next 을 클릭합니다. 경고 대화상자 가 나오는데 그냥 Yes 을 누릅니다. 마지막으로 Finish 을 클릭합니다.

5. 그러면 다음과 같은 대화상자를 볼 수 있습니다.

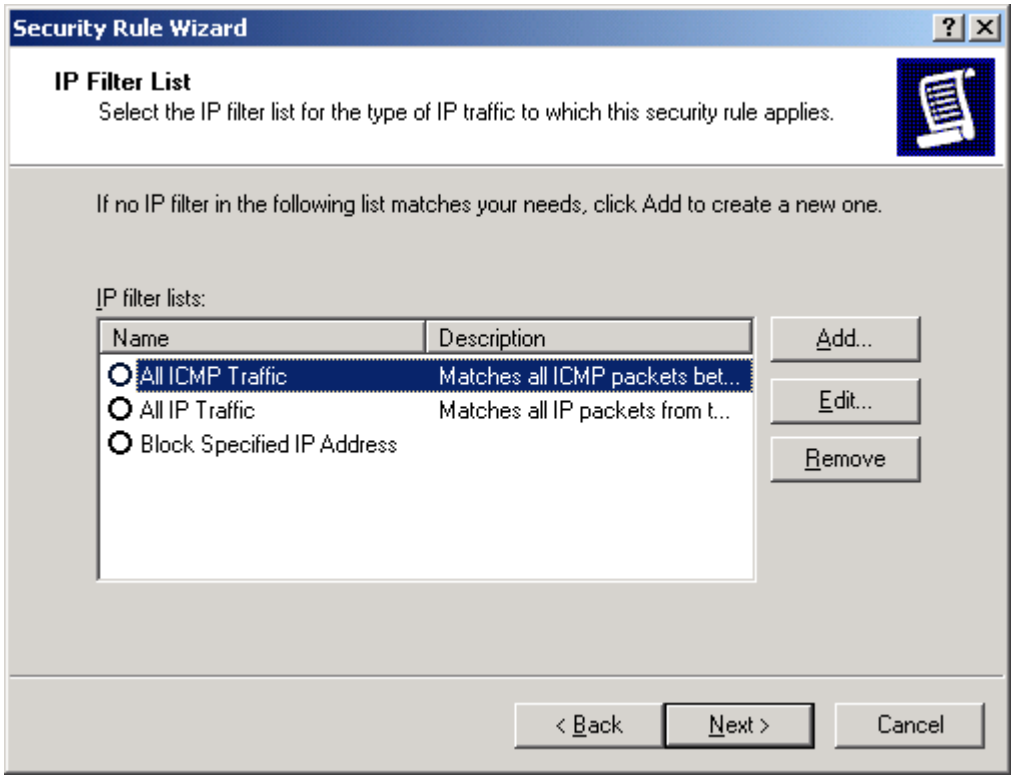


6. Add 버튼을 클릭하면 Security Rule 마법사가 실행됩니다. Next 을 클릭합니다. Tunnel Endpoint 대화상자에서 Next 을 클릭하고, 아래 그림과 같이 Network Type 대화상자에서 원하는 연결 을 선택해 줍니다. 여기서는 Local area network(LAN) 을 선택해 줍니다.

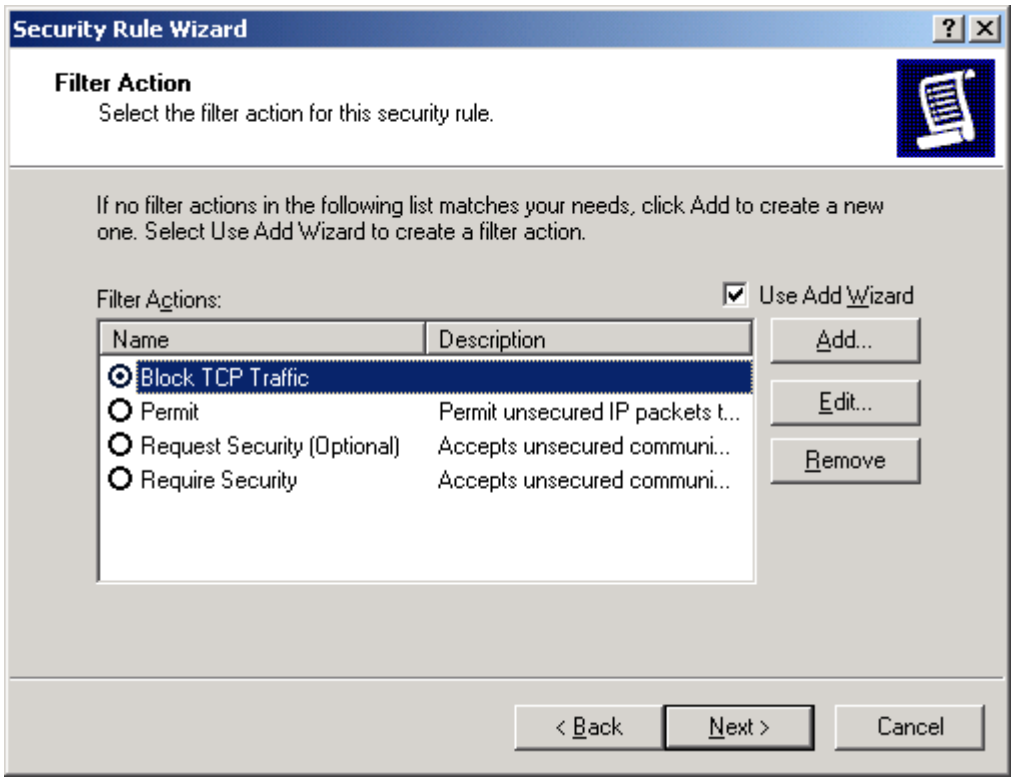


7. Authentification Method 대화상자에서 Windows 2000 Default 을 선택하고 Next 을 클릭하면 경고 대화상자가 나오는데 여기서 Yes 을 클릭합니다.

8. 아래와 같은 대화상자에서, 아까 만들었던 Block Specified IP Address 을 선택하고 Next 을 클릭합니다.



9. 아래와 같이 Filter Action 대화상자에서 **"Block TCP Traffic"**을 선택하고 **Next** 을 클릭합니다.

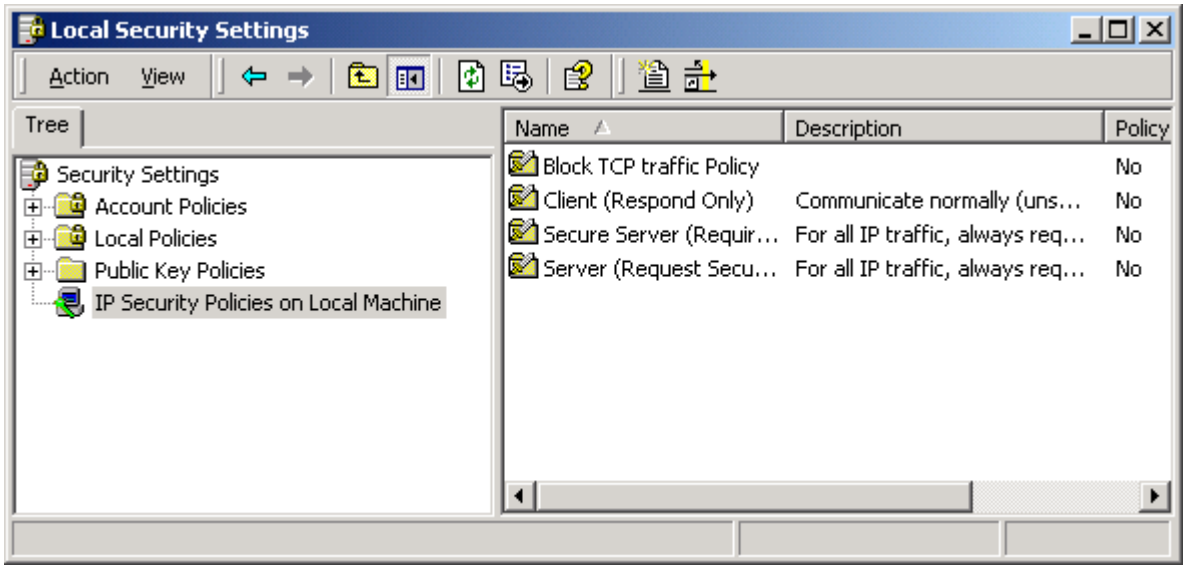


10. 마지막 대화상자에서 Finish 을 클릭합니다. 그러면 정책 구현이 끝나게 됩니다.

⑤ 정책 할당하기

IP 보안 정책은 하나의 규칙만 할당해서 적용 할 수 있으며, 하나의 규칙에는 여러 개 필터를 정의 할 수 있으며 그러면서 여러 서비스를 제어 할 수 있다는 것이다.
각각의 필터에 따른 동작을 구성 할 수 있으니 참고 하길 바란다.

이제 까지 의 과정을 모두 따라 해 본 사람이라면 IPSec 정책 화면이 다음과 같이 나올 것입니다.



우리가 작성한 Block TCP traffic Policy를 실제 동작시키려면 오른쪽 창의 Block TCP traffic Policy 을 오른쪽 클릭하고 할당(Assign)을 선택하여 주면 됩니다. 반대로 이 정책을 사용하지 않으려면 Unassign(할당해제)을 선택해 주면 됩니다.

4. 결론

IPSec 에 대한 내용은 너무나 방대합니다. 제가 계속 연재하는 부분은 Standalone(독립형 서버)국한 된 것입니다. 나중에 기회가 되면 AD 상의 IPSec 그리고 커맨드 프롬프트상에서 IPSec 을 편집하는 유틸리티에 대해서도 다루었으면 합니다.

글의 틀린 사항 또는 추가해야 할 사항이 있다면 security@mcse.co.kr 로 부담 없이 메일 주시면 감사하겠습니다.

이렇게 마무리를 쓰는 이유는 모 사이트에서 제가 번역하여 작성한 글을 자기 글인냥 올려 놓은 것을 보았기 때문입니다. 최소한의 네티켓을 지켜주시면 대단히 고맙겠습니다.

작성자 : 문일준 (security@mcse.co.kr)