. 네트워크 보안

편집: 홍익대학교(세종)
김혜영

01. 네트워크 보안의 개념과 필요성

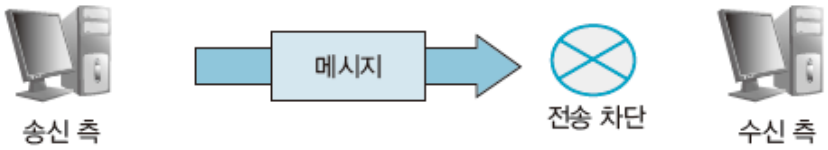
- 보안은 크게 컴퓨터 보안과 네트워크 보안으로 구분할 수 있다. 쉽게 말해, 컴퓨터 보안은 컴퓨터 자체의 데이터를 보호하는 것이고, 네트워크 보안은 컴퓨터 간에 데이터를 안전하게 전송하는 것이다.

- 보안 위협
  - 송신 측에서 수신 측에 메시지를 전송한다고 가정해 보자. 이때 네트워크 보안을 위협하는 위험 요소들도 함께 살펴보자.
  - [그림 9-1]은 정상적으로 전송한 예를 보여준다.

[그림 9-1] 정상적인 전송

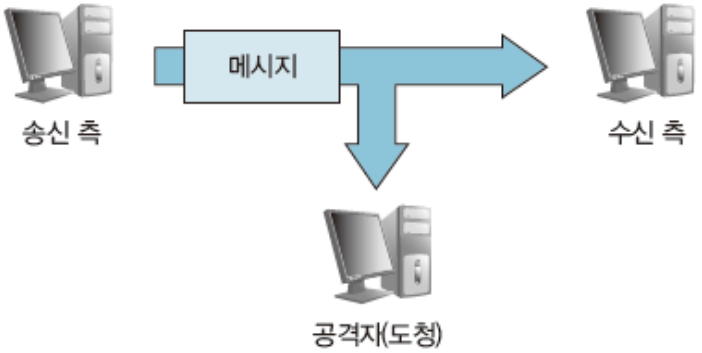
01. 네트워크 보안의 개념과 필요성

- 전송 차단
  - [그림 9-2]는 송신 측에서 수신 측에 메시지를 전송할 때 제3자가 수신 측과 연결할 수 없도록 하는 데이터 전송 차단을 보여준다.



[그림 9-2] 전송 차단

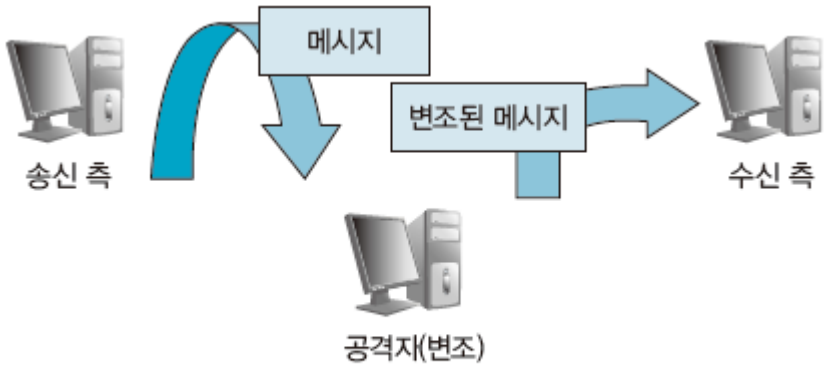
- 가로채기
  - [그림 9-3]은 송신 측과 수신 측이 데이터를 주고받는 사이 제3자(공격자)가 도청하는 예를 보여준다.
    - 이 경우를 가로채기(Interruption)라고 하며, 송신 측과 수신 측의 중요한 정보가 유출되는 심각한 문제가 발생할 수 있다.



[그림 9-3] 가로채기

01. 네트워크 보안의 개념과 필요성

- 변조
  - [그림 9-4]는 송신 측에서 수신 측으로 전송할 데이터를 제3자가 가로채서 데이터의 일부 또는 전부를 변경하여 잘못된 데이터를 수신 측에 전송하는 예를 보여준다.
  - 이 경우를 변조(Modification)라고 하며, 수신 측에서는 송신 측에서 잘못된 데이터를 전송한 것으로 오인할 수 있다.



[그림 9-4] 변조

01. 네트워크 보안의 개념과 필요성

- 위조
  - [그림 9-5]는 제3자가 마치 송신 측이 메시지를 전송한 것처럼 위조(Fabrication)하여 수신 측에 전송하는 예를 보여준다.
  - 이때는 변조와 달리 아예 송신 측에서 만들지 않은 메시지를 수신 측으로 전송하는 문제가 발생한다

[그림 9–5] 위조

01. 네트워크 보안의 개념과 필요성

네트워크 보안의 필요성

- 네트워크 보안
  - 방화벽은 인터넷과 내부 네트워크 간에 일종의 세관 역할을 수행한다. 외부 네트워크에서는 네트워크 전면에 있는 방화벽만 보이고, 그 뒤에 놓인 내부 네트워크는 보이지 않는다.
  - 따라서 해커가 침입하더라도 갈 수 있는 한계는 방화벽까지며, 그 뒤의 내부 네트워크와는 격리된다.
  - 보통 방화벽 자체에는 중요한 정보가 없는데, 외부의 접근을 차단하여 해킹 위험을 방지하는 것이다.

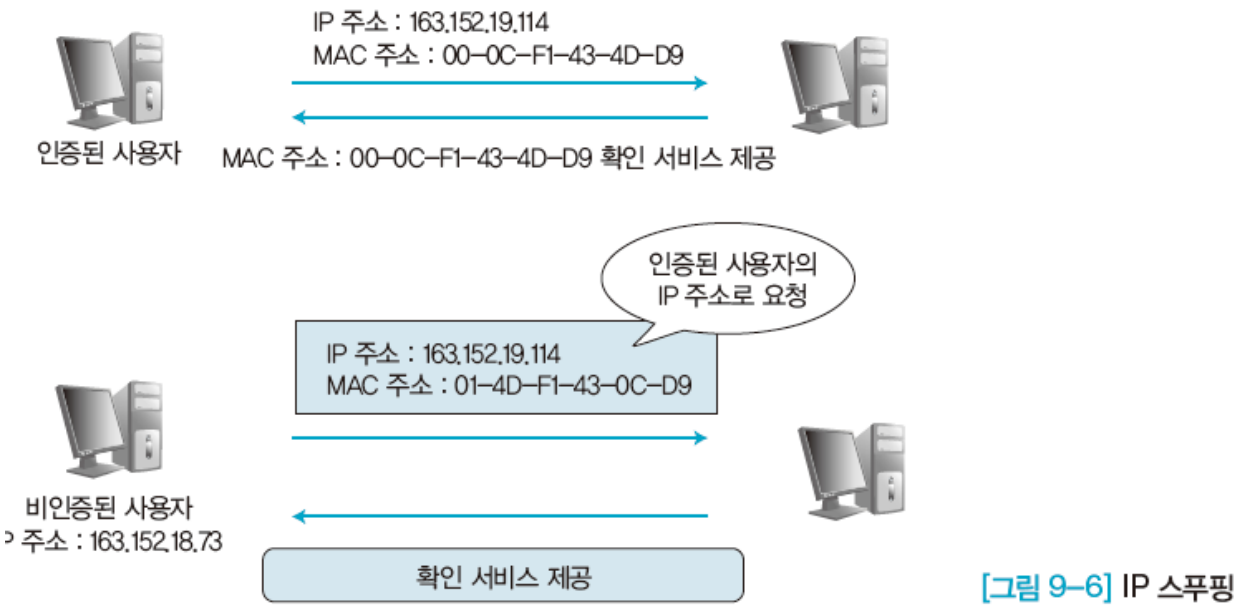
네트워크 보안의 요구 사항

- 비밀성
- 무결성
- 가용성

02. 네트워크 공격 기술

IP 스푸핑

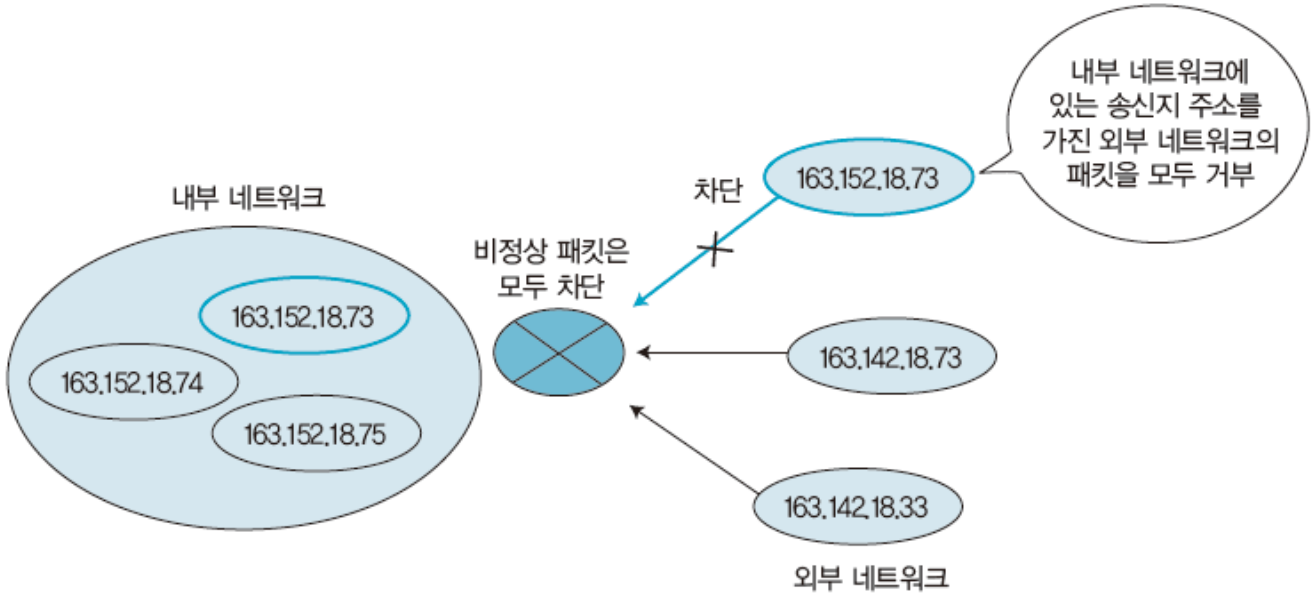
- IP 스푸핑(IP Spoofing)은 IP 주소를 속이는 행위를 말한다.
- '스푸핑'은 외부 네트워크 공격자가 임의로 웹사이트를 구성하여 일반 사용자의 방문을 유도하고, 인터넷 프로토콜인 TCP/IP의 구조적인 결함을 이용하여 사용자 시스템 권한을 획득한 후 정보를 빼가는 해킹 수법이다.



[그림 9-6] IP 스푸핑

02. 네트워크 공격 기술

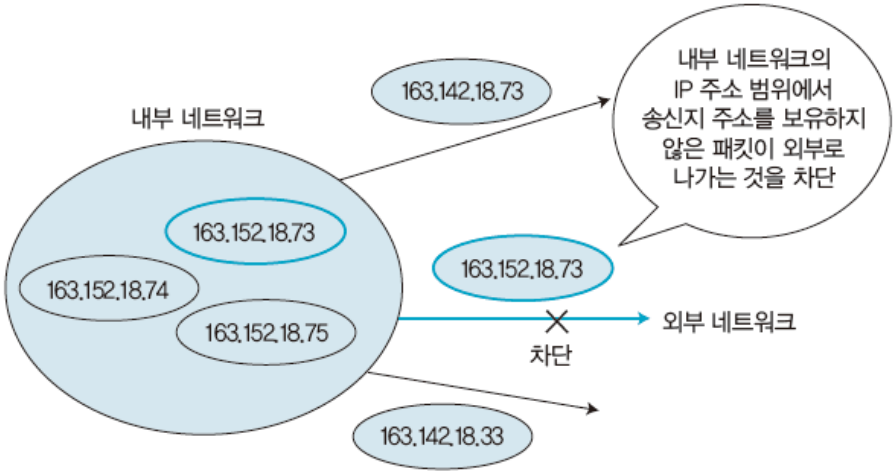
- IP 스푸핑을 차단하는 방법
  - 액세스 제어
    - 내부 네트워크에 있는 송신지 주소를 가진 외부 네트워크의 패킷을 모두 거부함으로써 IP 스푸핑 공격을 줄일 수 있다.



[그림 9-7] 액세스 제어

02. 네트워크 공격 기술

- 필터링
  - 내부 네트워크의 IP 주소 범위에서 송신지 주소를 보유하지 않은 패킷이 외부로 나가는 것을 차단함으로써 사용자가 다른 네트워크를 스푸핑하는 것을 막을 수 있다.



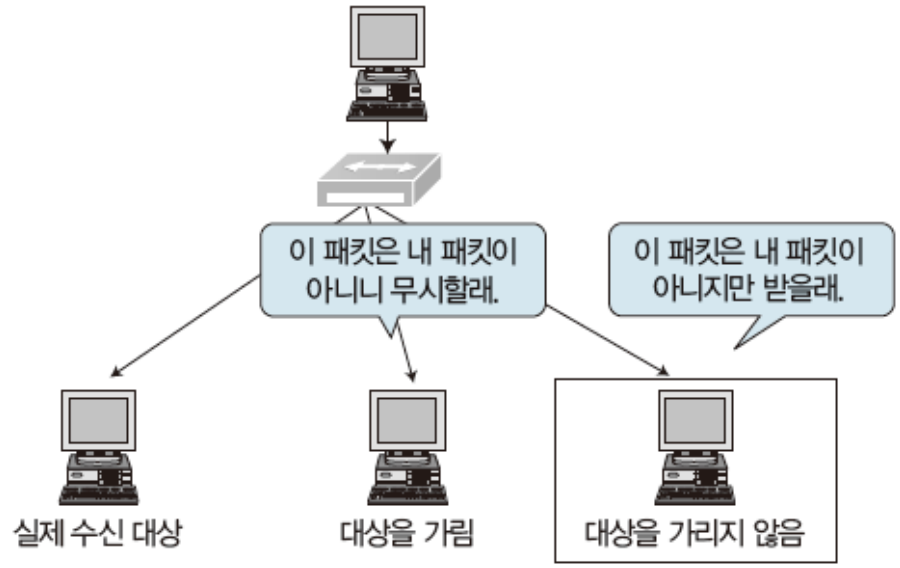
[그림 9-8] 필터링

- 암호화
  - IP 스푸핑을 차단하는 가장 좋은 방법은 패킷을 암호화하는 것이다.

02. 네트워크 공격 기술

IP 스니핑

- 스니핑(Sniffing)은 '코를 킁킁거리다' 또는 '냄새를 맡다'는 뜻으로 네트워크를 이용하여 전송하는 데이터를 엿듣는 일종의 도청 행위를 말한다.
- TCP/IP 프로토콜은 인터넷이 시작되기 전부터 설계된 프로토콜이기에 패킷 암호화 및 인증 등을 고려하지 않아 데이터 통신 보안의 기본 요소 중 비밀성과 무결성을 보장할 수 없었다. 특히 스니핑은 비밀성을 해치는 대표적인 공격 방법 중 하나다.



[그림 9-9] 스니핑

02. 네트워크 공격 기술

[표 9-1] 암호화 전송 프로토콜의 종류

종류	설명
SSL	• HTTP, POP, SMTP, 텔넷 등에 SSL을 적용하여 HTTPS, POP3S, SMTPS, 텔넷 등으로 대치 • HTTP에 가장 많이 활용하며, 이를 적용하여 아이디 및 패스워드를 암호화할 수 있음
SSH	암호화 통신을 제공하여 FTP, 텔넷을 대치할 수 있음
VPN	• 스니핑 피해가 우려되는 네트워크에 전용선을 직접 연결함으로써 중간에 도청되는 것을 막음 • 인터넷 회선을 이용하여 사설망의 효과를 줄 수 있는 것이 VPN인데, 각 VPN 장비 간의 암호화를 이용하여 도청을 막을 수 있음

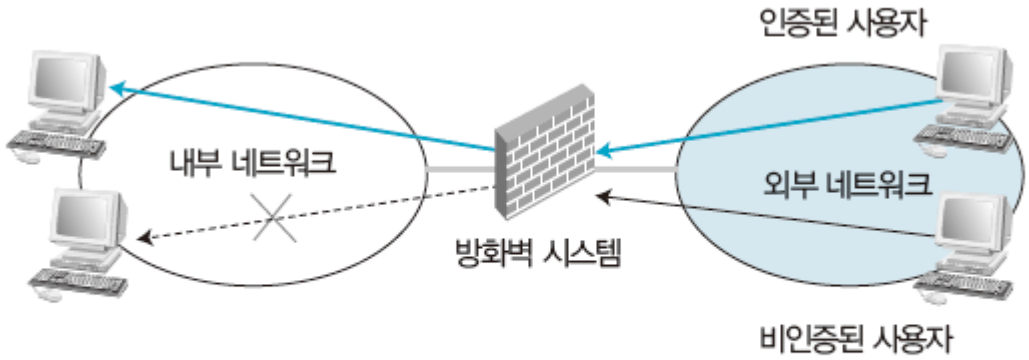
03. 시스템 보안 기술

[그림 9-10] 네트워크 시스템 보안의 분류

03. 시스템 보안 기술 : 방화벽

방화벽

- 방화벽(Firewall)은 외부 네트워크에서 내부 네트워크로 접근하려면 반드시 방화벽을 통과하도록 하여 내부 네트워크의 자원 및 정보를 보호하는 시스템이다.
- 외부와 내부 네트워크 간의 유일한 경로에 방화벽을 둠으로써 보안 서비스를 제공하여 불법적인 트래픽을 거부하거나 막을 수 있는 것이다. 투명성을 보장하지는 않지만, 내부 네트워크를 안전하게 보호할 수는 있다.



[그림 9-11] 방화벽의 구조

03. 시스템 보안 기술 : 방화벽

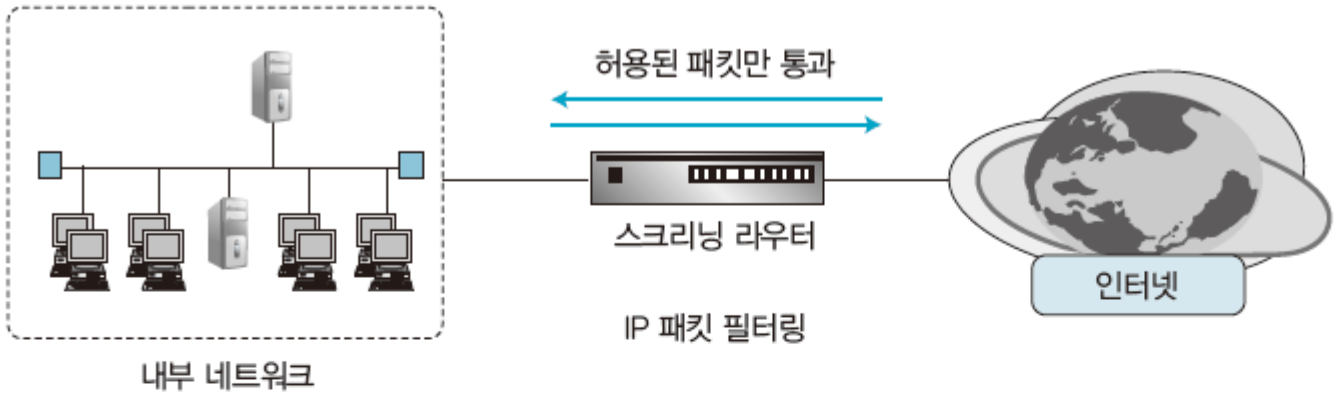
방화벽의 기본 구성요소

- 네트워크 정책
- 방화벽 사용자 인증 시스템
- 패킷 필터링
- 응용 계층 게이트웨이

방화벽의 종류

- 스크리닝 라우터
  - 스크리닝 라우터(Screening Router)는 네트워크에서 사용하는 프로토콜의 형태, 송신지주소와 수신지 주소, 프로토콜의 제어 필드, 통신에 사용하는 포트 번호를 분석하여 내부네트워크에서 외부 네트워크로 나가는 패킷 트래픽의 진입을 허가 또는 거절하거나 외부네트워크에서 내부 네트워크로 진입하는 패킷 트래픽의 진입을 허가 또는 거절하는 라우터를 말한다.
  - 스크리닝 라우터는 OSI 참조 모델의 3계층과 4계층에서 동작하기 때문에 3계층과 4계층에서 동작하는 프로토콜인 IP, TCP 또는 UDP의 헤더에 포함된 내용을 분석하여 동작한다

03. 시스템 보안 기술 : 방화벽



[그림 9-12] 스크리닝 라우터

[표 9-2] 스크리닝 라우터의 장단점

장점	단점
• 필터링 속도가 빠르고, 비용이 적게 듦 • 네트워크 및 전송 계층에서 동작하기 때문에 클라이언트와 서버에 변화가 없어도 됨 • 하나의 스크리닝 라우터로 보호하려는 네트워크 전체를 동일하게 보호할 수 있음	• 네트워크 계층과 전송 계층의 트래픽만 방어할 수 있음 • 패킷 필터링 규칙을 구성하여 검증하기 어려움 • 패킷 내의 데이터 공격을 차단하는 것은 불가능 • 스크리닝 라우터를 통과하거나 거절당한 패킷의 기록을 관리하기 힘듦

03. 시스템 보안 기술 : 방화벽

- 베스천(요새) 호스트
  - 보호된 네트워크에서 유일하게 외부의 공격에 노출된 컴퓨터 시스템을 말하며, 내부 네트워크와 외부 네트워크 간에 게이트웨이 역할을 한다.
  - 네트워크 보안상 가장 중요한 위치를 차지하므로 관리자가 철저하게 감시하며, 불법적인 침입의도로 접속한 모든 시스템의 기록을 주기적으로 검사해야 한다.

[그림 9-13] 베스천 호스트

[표 9-3] 베스천 호스트의 장단점

장점	단점
• 응용 서비스의 종류에 종속적이므로 스크리닝 라우터보다 안전성이 높음 • 데이터 공격을 확실하게 방어할 수 있음 • 로그 정보의 생성 및 관리가 용이	• 모든 보안 기능이 베스천 호스트에 집중되어 있으므로 베스천 호스트가 손상되면 내부 네트워크를 전혀 보호할 수 없음 • 각종 로그인 정보가 누출되면 방화벽 역할이 불가능 • 스크리닝 라우터와 베스천 호스트를 복합적으로 사용하여 방화벽의 효과를 배가시킬 수 있는 것으로 알려져 있음

03. 시스템 보안 기술 : 방화벽

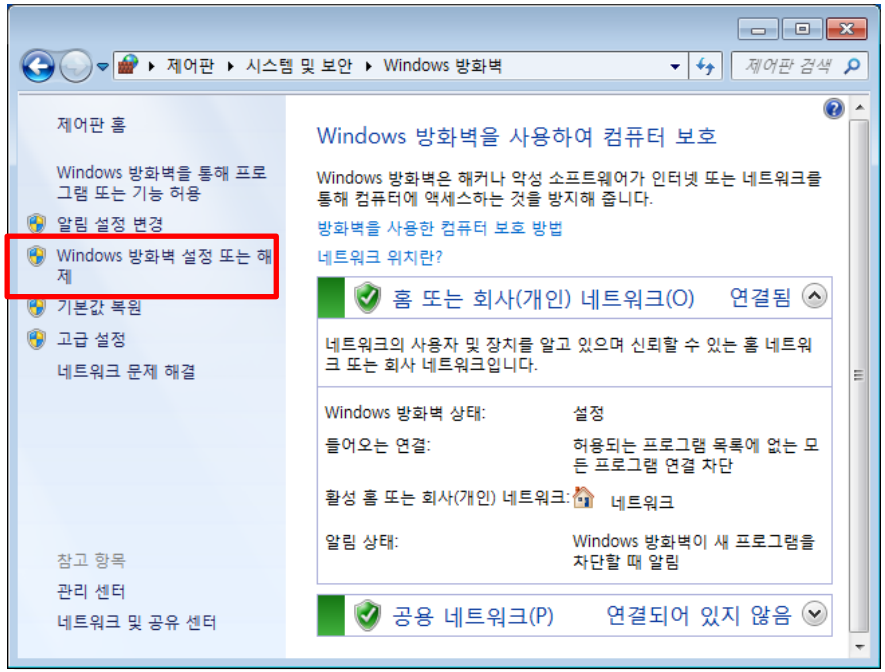
방화벽 시스템 방식

- 패킷 필터링 방식
  - 패킷 필터링 방식의 방화벽은 OSI 참조 모델의 네트워크 계층(IP 프로토콜)과 전송 계층(TCP 프로토콜)에서 패킷의 송신지 및 목적지 IP 주소 정보, 각 서비스의 포트 번호를 이용한 접속을 제어한다.
- 응용 프로그램 게이트웨이
  - 응용 프로그램 게이트웨이는 OSI 참조 모델의 응용 계층에 방화벽 기능이 들어 있다.
  - 각 서비스별 프록시를 이용하며, 패킷 필터링 방식처럼 IP 주소 및 TCP 포트를 이용하여 네트워크의 접근을 제어할 수 있다.
- 회로 레벨 게이트웨이
  - 회로 레벨 게이트웨이는 OSI 참조 모델에서 5계층과 7계층 사이에 있으며, 응용 프로그램 게이트웨이와는 달리 각 서비스별로 프록시가 있는 것이 아니고, 어느 응용 프로그램이든 이용할 수 있는 일반적인 프록시만 있다.
- 혼용 방화벽
  - 때에 따라 여러 유형의 방화벽을 복합적으로 구성할 수도 있다.

03. 시스템 보안 기술 : 방화벽

방화벽 설정

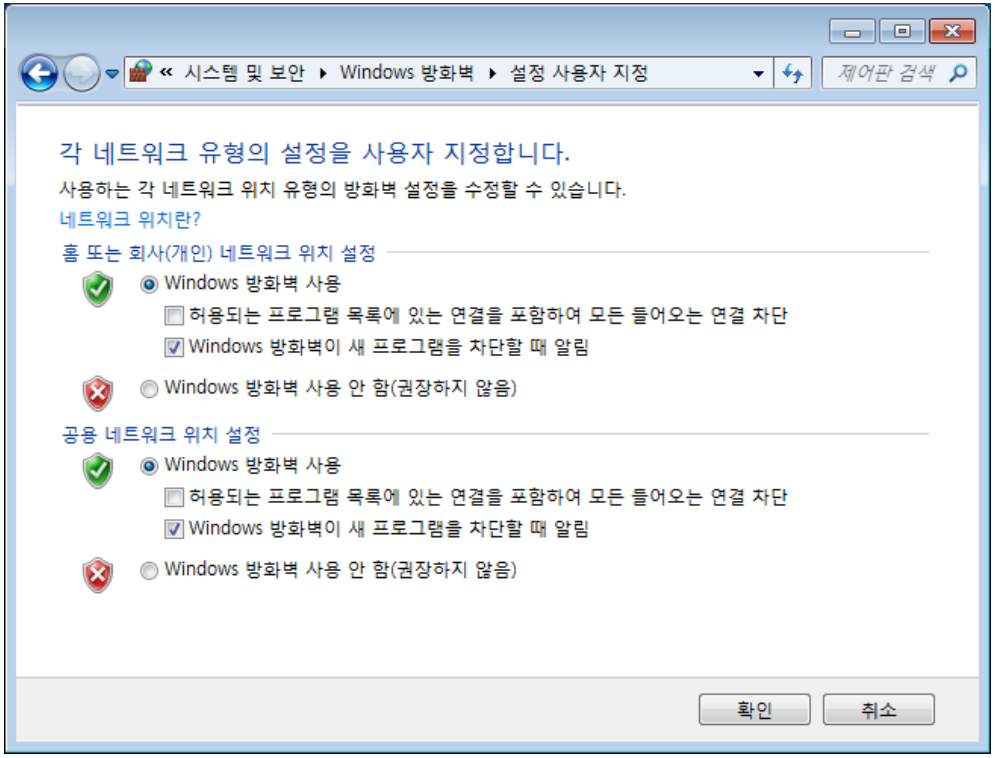
- 방화벽은 바이러스나 악성코드가 네트워크를 통해 사용자 컴퓨터에 액세스하는 것을 방지해 준다.
- 개인 컴퓨터의 방화벽 설정은 <제어판 → 시스템 및 보안 → Windows 방화벽>을 클릭하면 확인할 수 있다.



[그림 9-14] 방화벽 설정 확인

03. 시스템 보안 기술 : 방화벽

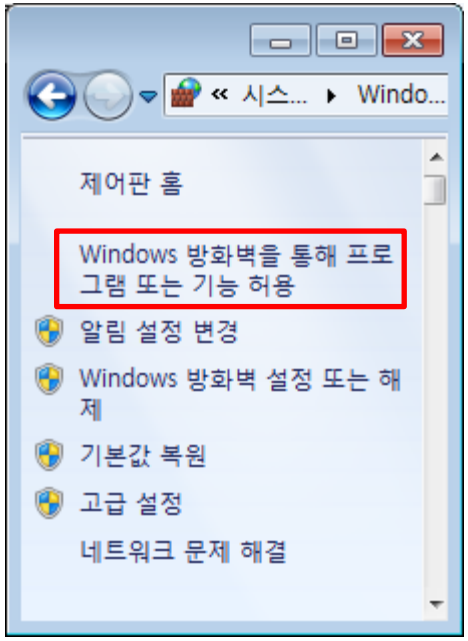
- 왼쪽 부분에서 <Windows 방화벽 설정 또는 해제>를 클릭하면 사용하는 각 네트워크의 위치 유형별로 방화벽을 설정하거나 수정할 수 있다.



[그림 9-15] 네트워크 위치 유형별 방화벽 설정

03. 시스템 보안 기술 : 방화벽

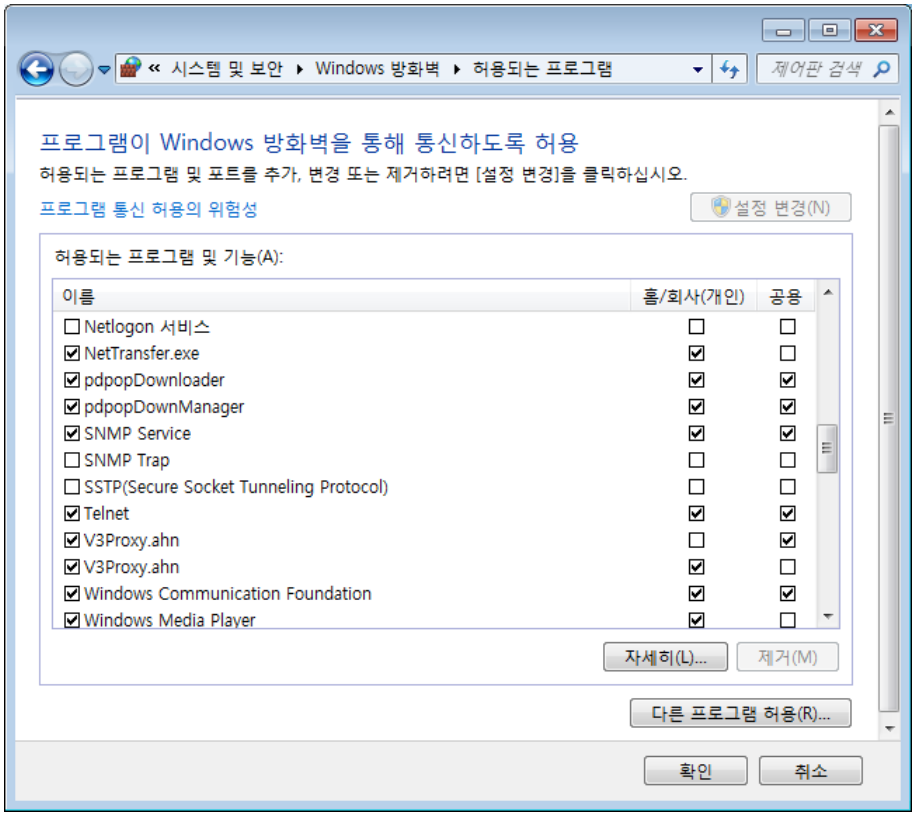
- 통신을 허용하려면 왼쪽 부분에서 <Windows 방화벽을 통해 프로그램 또는 기능 허용>을 클릭한다.



[그림 9–16] 통신을 허용할 프로그램이나 기능 허용 설정

03. 시스템 보안 기술 : 방화벽

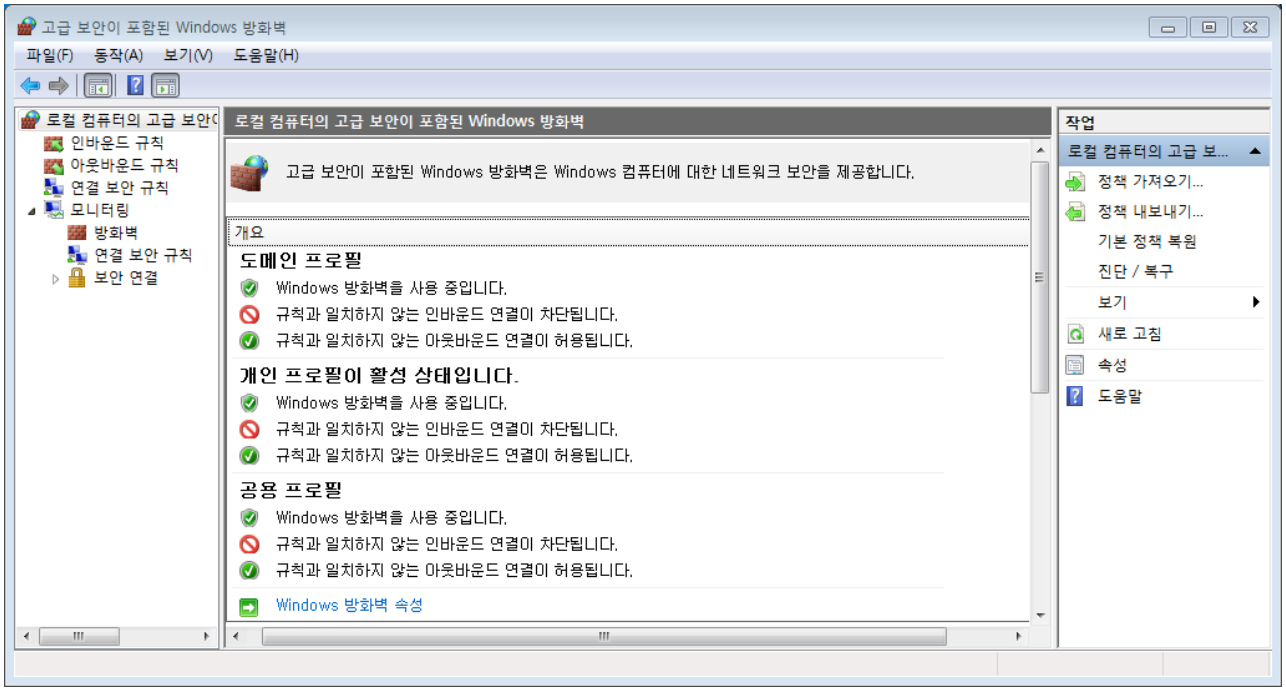
- [그림 9-17]처럼 통신을 허용하는 프로그램을 확인할 수 있으며, <설정 변경> 버튼을 누르면 허용하는 프로그램 및 포트를 추가할 수 있다.



[그림 9-17] 허용하는 프로그램 및 포트 추가

03. 시스템 보안 기술 : 방화벽

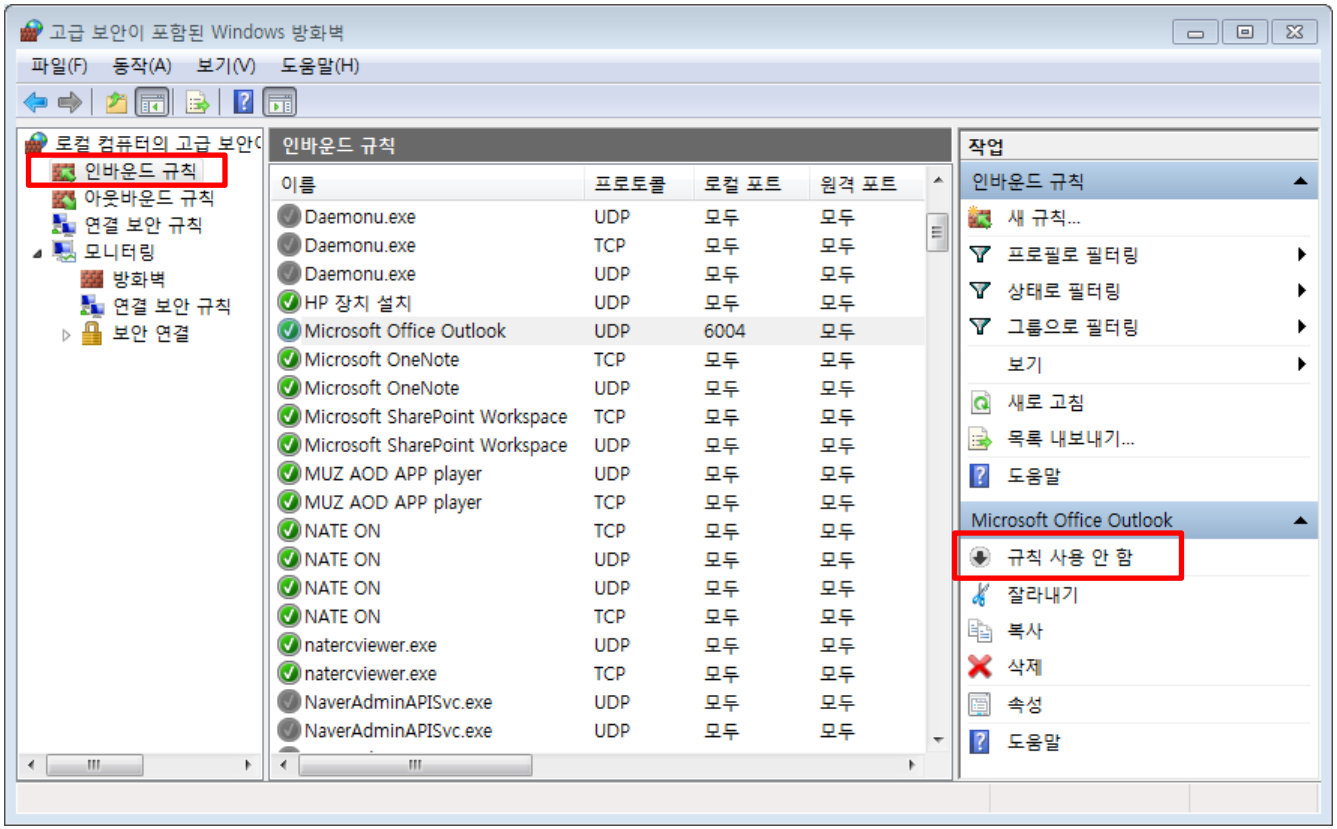
- 꼭 필요할 때만 프로그램을 허용하거나 포트를 열고, 필요하지 않을 때는 프로그램을 제거하거나 포트를 닫는 것이 보안 위험을 줄이는 데 도움이 된다.
- 방화벽 포트를 닫으려면 [그림 9-16]의 Windows 방화벽 창에서 <고급 설정>을 클릭하거나 고급 보안이 포함된 Windows 방화벽을 설정해야 한다(관리자로 로그인). 또는<제어판 → 시스템 및 보안 → 관리 도구 → 고급 보안이 포함된 Windows 방화벽>에서도 설정할 수 있다.



[그림 9-18] 고급 보안이 포함된 Windows 방화벽 1

03. 시스템 보안 기술 : 방화벽

- 왼쪽 부분에서 <인바운드 규칙>을 클릭한 후 가운데 부분에서 사용하지 않을 규칙을 선택한다. 그러고 나서 오른쪽 부분에서 <규칙 사용 안 함>을 클릭한다.



[그림 9-19] 고급 보안이 포함된 Windows 방화벽 2

03. 시스템 보안 기술 : 방화벽

방화벽 규칙과 연결 보안 규칙

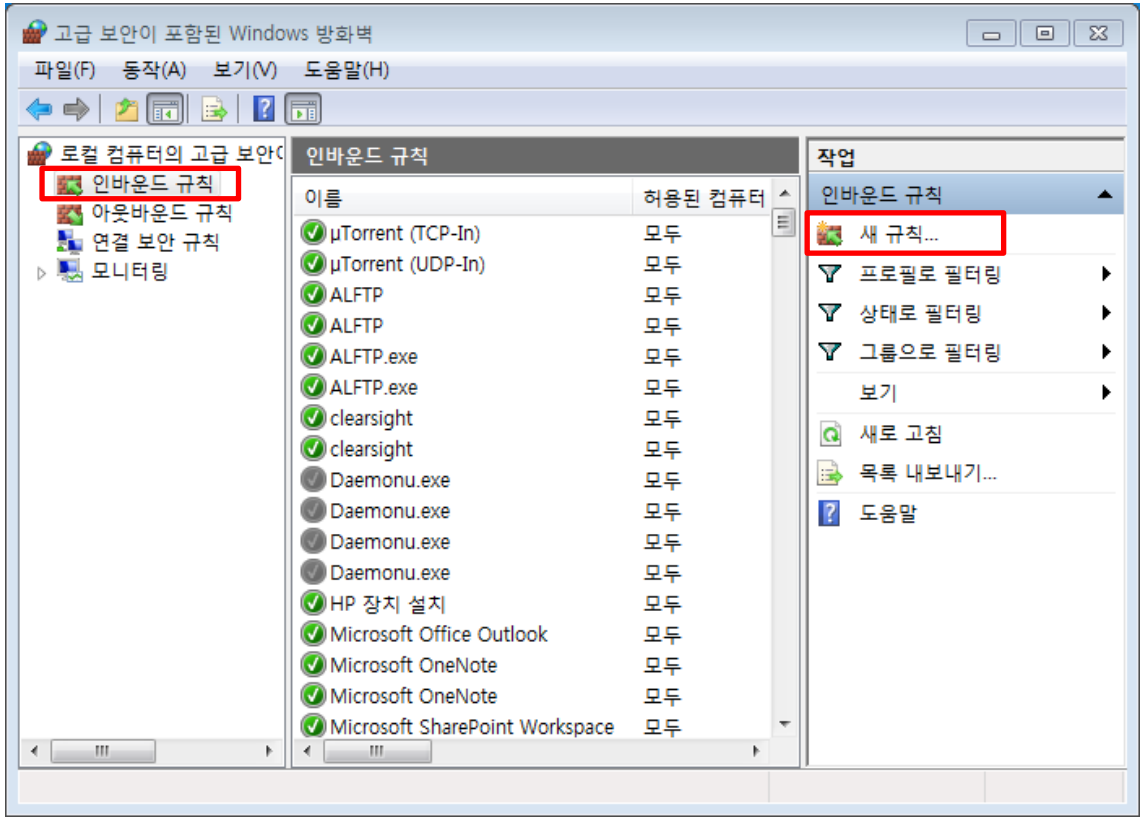
- 컴퓨터와 프로그램, 서비스, 다른 컴퓨터 간에 트래픽을 송수신할 수 있는 방화벽 규칙을 만들 수도 있다. 이 방화벽 규칙은 조건과 일치하는 모든 연결에서 연결 허용, IPsec를 사용하여 보안할 때만 연결 허용, 연결 차단 중 하나를 수행하도록 한다.
- 기본적으로 인바운드 연결은 허용 규칙과 일치하면 허용하고, 아웃바운드 연결은 차단 규칙과 일치하지 않으면 허용한다.
- 특정 프로그램의 연결을 허용하는 방화벽 규칙과 연결 보안 규칙을 만들어 보자.

인바운드 규칙

① 새 규칙 생성

- 고급 보안이 포함된 Windows 방화벽 창의 왼쪽 부분에서 <인바운드 규칙>을 클릭한 후 오른쪽 부분에서 <새 규칙>을 클릭한다

03. 시스템 보안 기술 : 방화벽

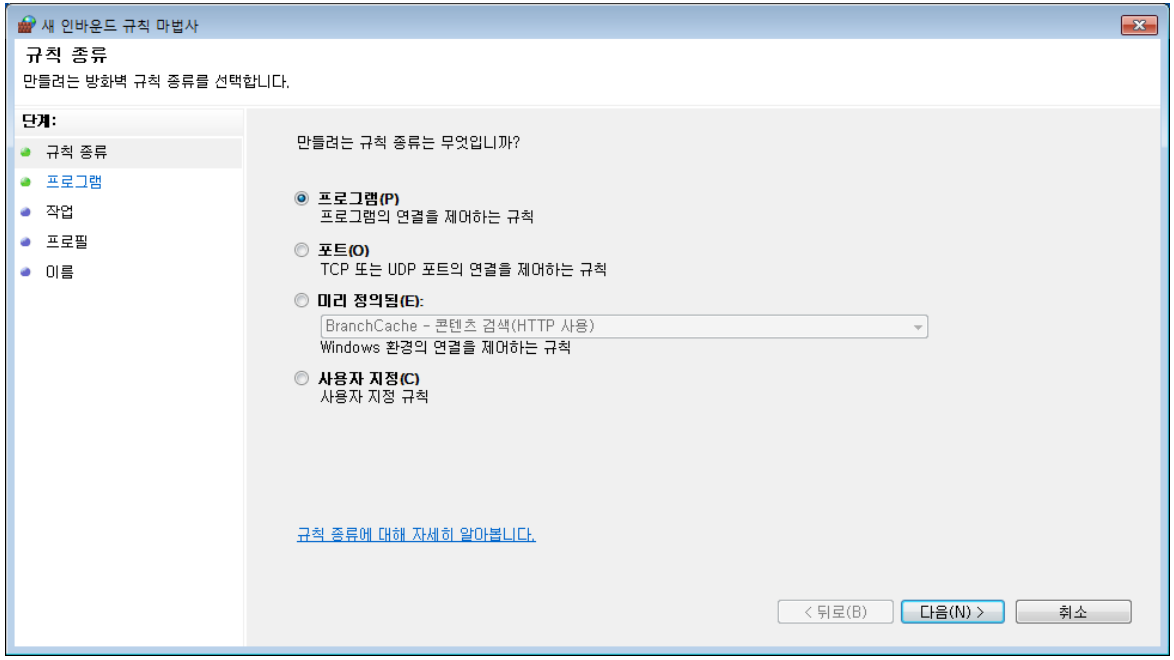


[그림 9–20] 새로운 인바운드 규칙 생성

03. 시스템 보안 기술 : 방화벽

② 규칙 종류 선택

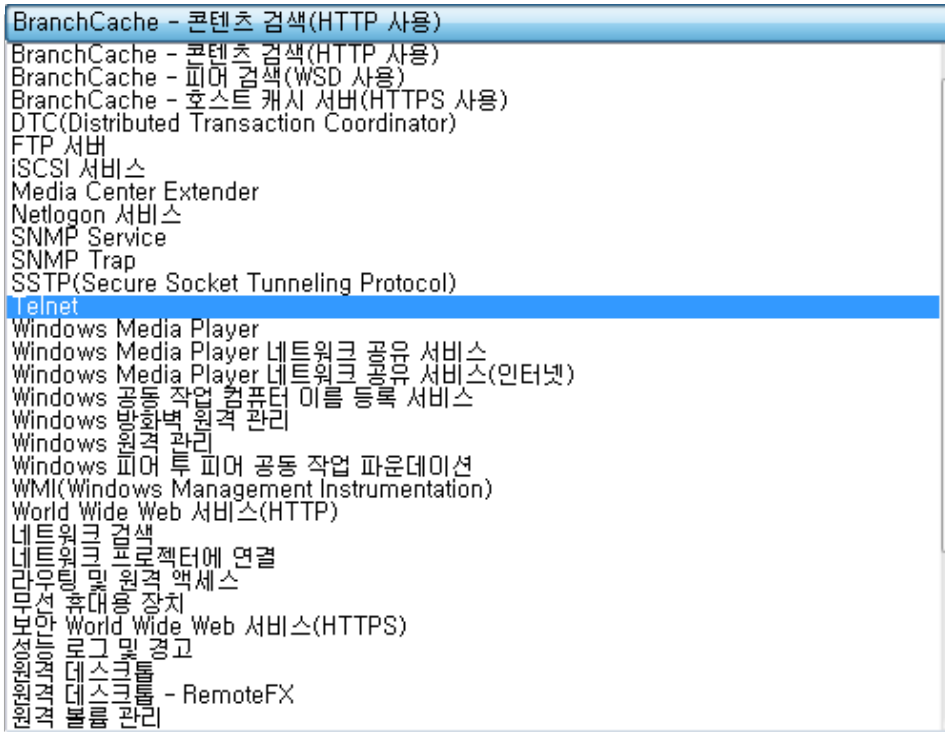
- 만들려는 방화벽의 규칙 종류를 선택한다.
- 방화벽 규칙 종류에는 네 가지가 있는데, 그 중 하나를 선택하면 방화벽을 통한 연결을 명시적으로 허용하거나 거부하는 예외 항목을 만들 수 있다.
- 인바운드 규칙과 아웃바운드 규칙을 만들 때는 동일한 마법사와 속성 페이지를 사용한다.



[그림 9-21] 규칙 종류 선택

03. 시스템 보안 기술 : 방화벽

- 프로그램 : 연결을 시도하는 프로그램에 따라 연결을 허용할 수 있다. 이렇게 하면 카카오톡 프로그램이나 기타 프로그램의 연결을 쉽게 허용할 수 있다.
- 포트 : 컴퓨터에서 연결을 시도하는 데 사용하는 프로토콜(TCP/UDP)과 로컬 포트 번호를 지정할 수 있다.
- 미리 정의됨 : 정의된 목록 또는 서비스 중 하나를 선택하여 연결을 허용할 수 있다.



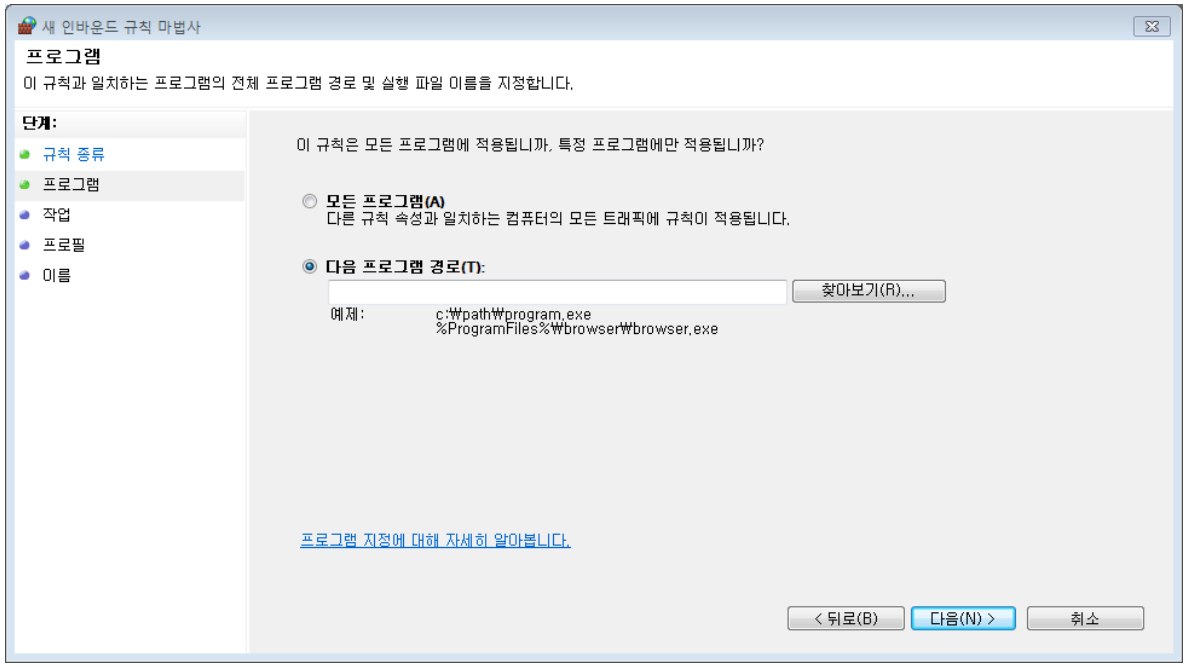
[그림 9-22] 미리 정의된 목록 또는 서비스 중 선택

03. 시스템 보안 기술 : 방화벽

- 사용자 지정 : 다른 방화벽 규칙 종류에 포함하지 않은 조건에 따라 연결을 허용하도록 구성할 수 있는 규칙을 만들 수 있다.

③ 일치시킬 프로그램 경로 및 실행 파일 이름 지정

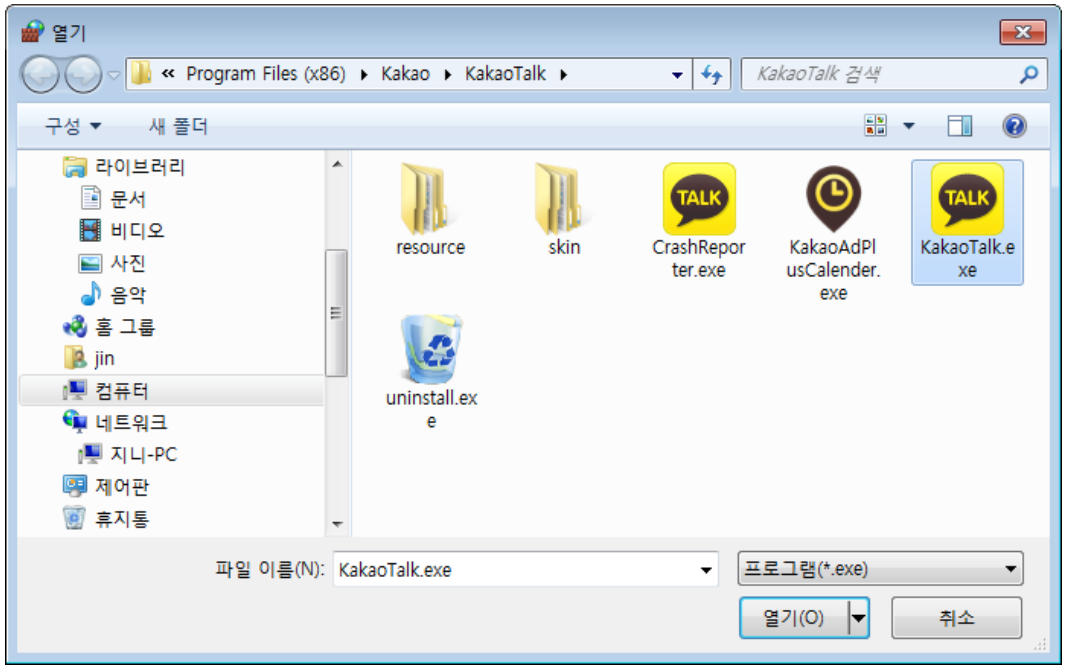
- 규칙과 일치하는 프로그램의 전체 프로그램 경로 및 실행 파일 이름을 지정한다. 방화벽이 네트워크 패킷을 일치시키는 방식 중 하나를 선택할 수 있다.



[그림 9-23] 일치시킬 프로그램 경로 및 실행 파일 이름 지정

03. 시스템 보안 기술 : 방화벽

- 모든 프로그램 : 다른 규칙 속성과 일치하는 컴퓨터의 모든 트래픽에 규칙이 적용된다.
- 다음 프로그램 경로 : 지정한 프로그램에서 보내는 패킷을 일치시키려면 이 옵션을 선택한다. 프로그램 전체 경로를 입력하거나 <찾아보기>를 클릭하여 디렉터리에서 프로그램을 찾는다.

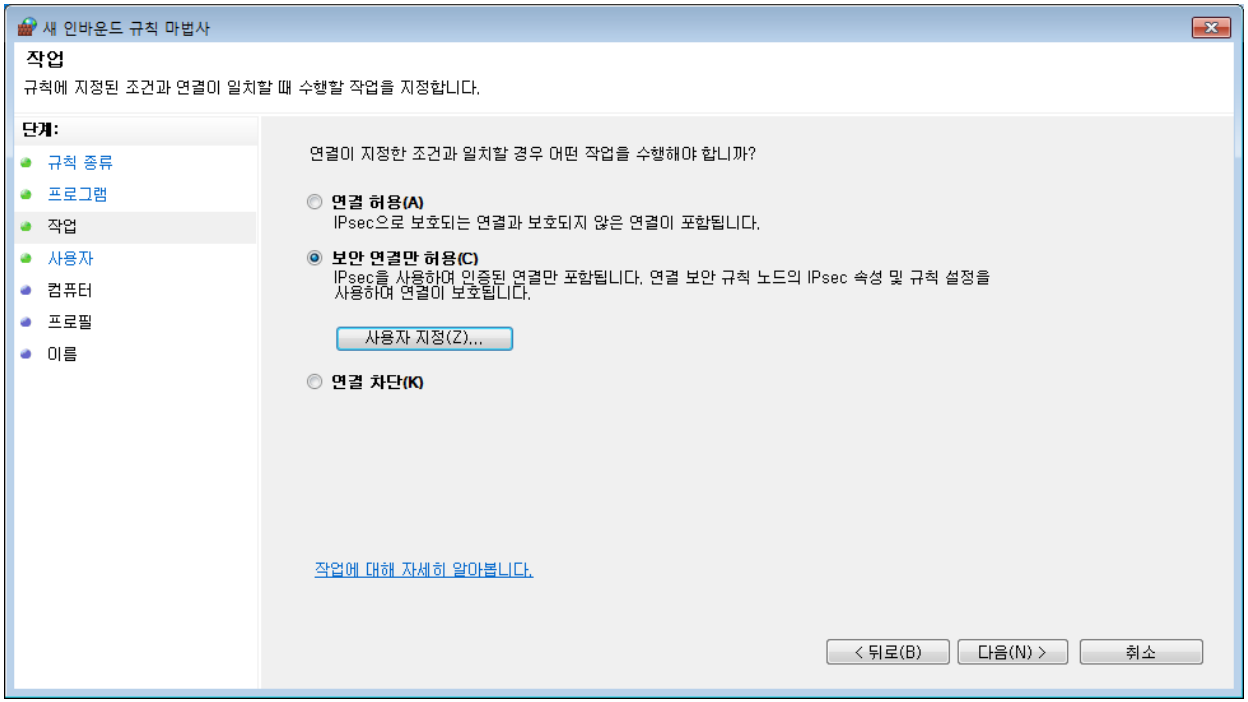


[그림 9-24] 일치시킬 프로그램 지정

03. 시스템 보안 기술 : 방화벽

④ 일치할 때 수행할 작업 지정

- 규칙에 지정한 조건과 연결이 일치할 때 수행할 작업을 지정한다. 방화벽에서 방화벽 규칙조건과 일치하는 송수신 패킷이 들어오면 실행할 동작을 선택할 수 있다.

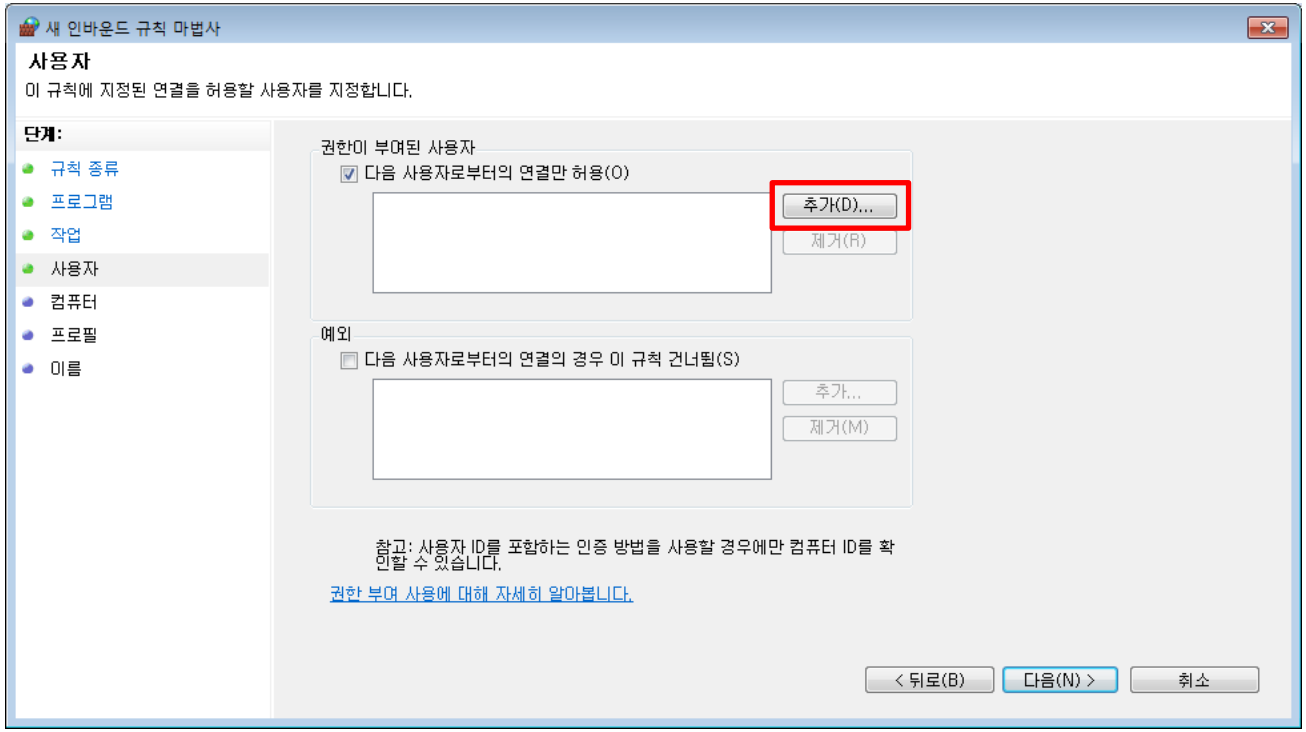


[그림 9-25] 일치할 때 수행할 작업 지정

03. 시스템 보안 기술 : 방화벽

⑤ 사용자 지정

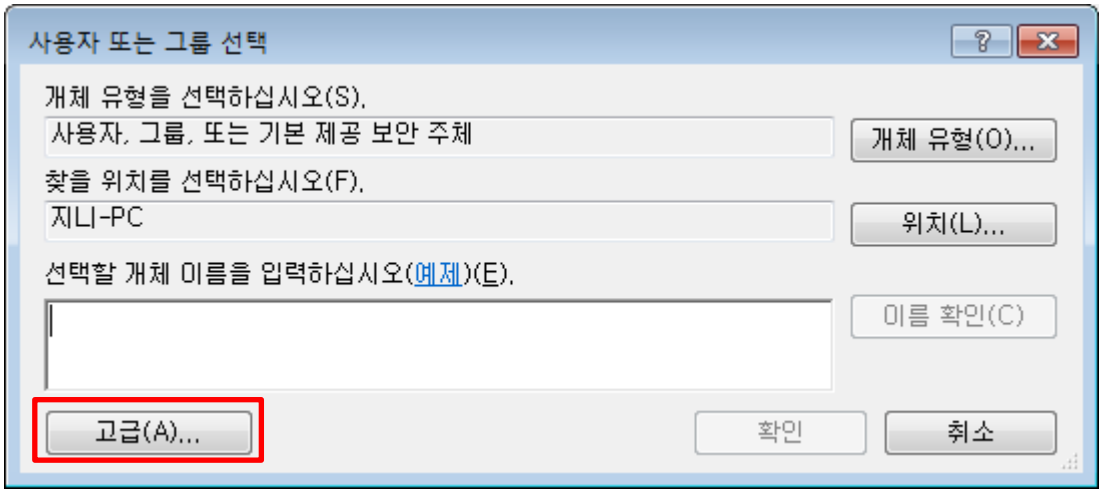
- 규칙에 지정된 연결을 허용할 사용자를 지정한다. 로컬 컴퓨터에 연결할 수 있는 사용자와 그룹을 선택할 수 있다.



[그림 9-26] 사용자 지정

03. 시스템 보안 기술 : 방화벽

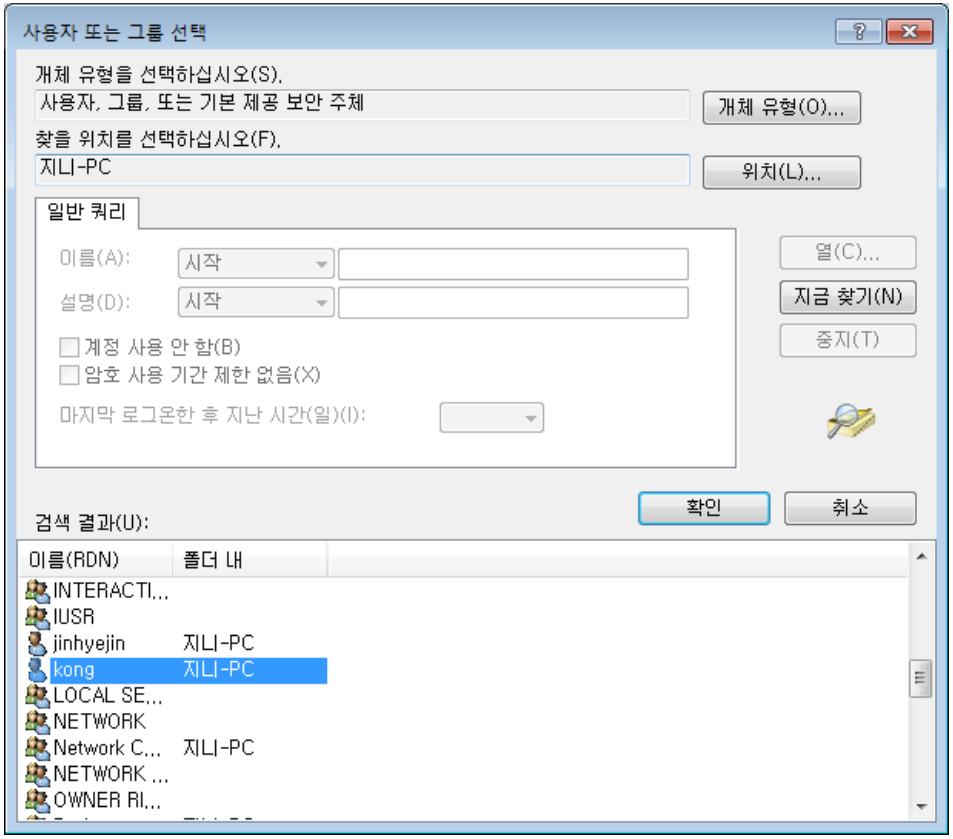
- 이 옵션을 사용하려면 방화벽 규칙 동작을 '보안 연결만 허용'으로 설정해야 한다.
- 사용자 또는 그룹 선택 화면에서 선택할 개체 이름을 입력한다. 개체 이름을 모를 때는 <고급> 버튼을 누른다.



[그림 9-27] 사용자 추가

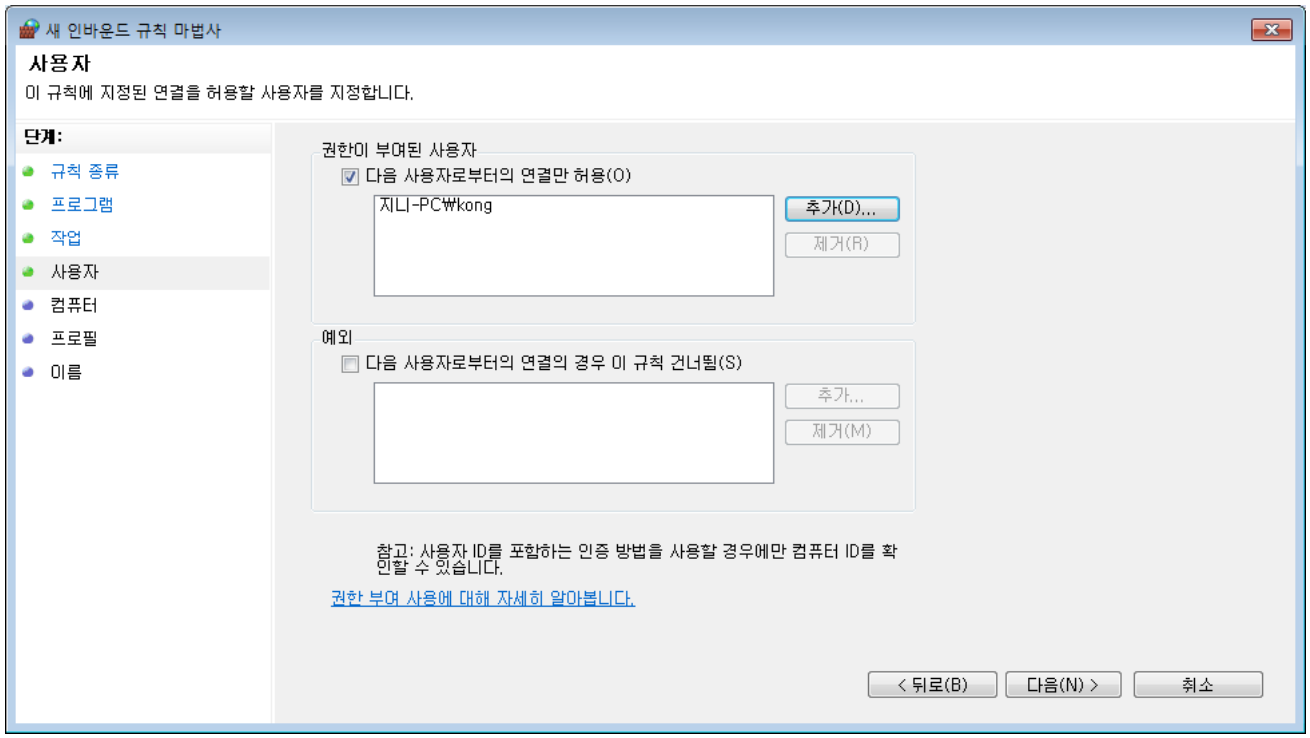
03. 시스템 보안 기술 : 방화벽

- 개체 유형과 찾을 위치를 선택한 후 <지금 찾기> 버튼을 누르면 대화상자 아래쪽에 검색 결과를 표시한다.
  - 목록 중에서 선택할 개체를 클릭하면 된다.



[그림 9-28] 사용자 검색 결과

03. 시스템 보안 기술 : 방화벽

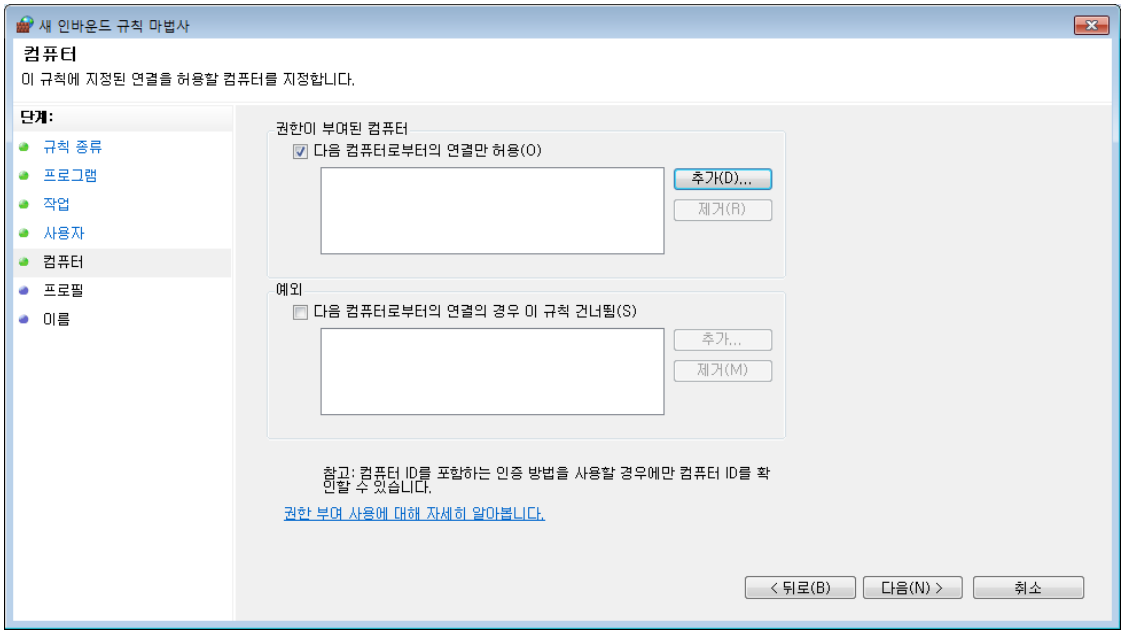


[그림 9-29] 사용자 지정 완료 화면

03. 시스템 보안 기술 : 방화벽

⑥ 연결을 허용할 컴퓨터 지정

- 규칙에 지정한 연결을 허용할 컴퓨터를 선택한다.

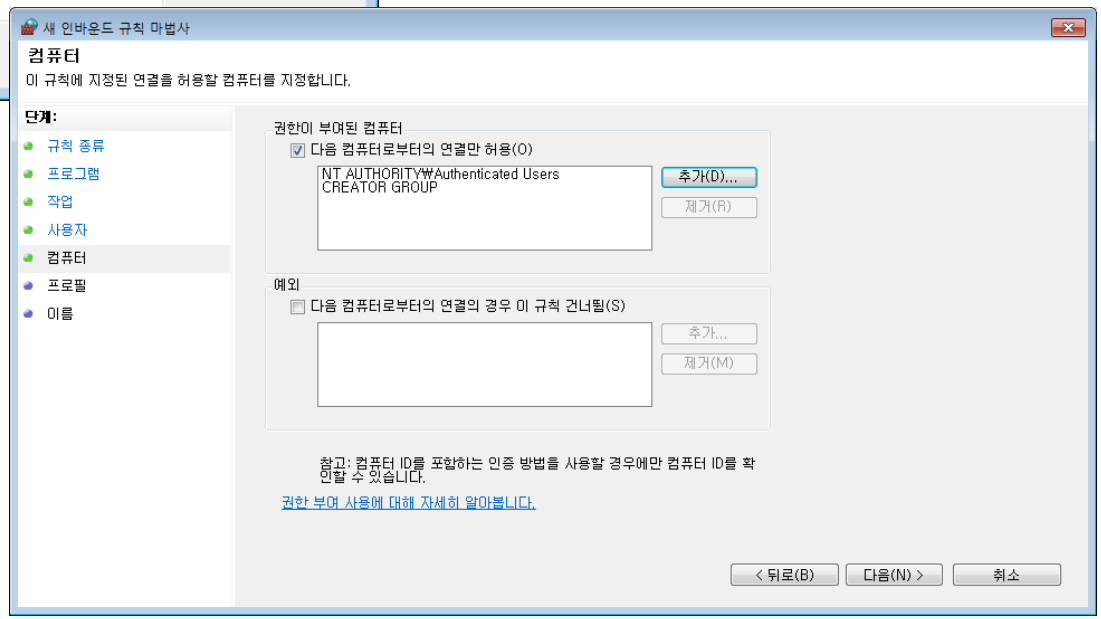


[그림 9-30] 연결을 허용할 컴퓨터 지정

03. 시스템 보안 기술 : 방화벽

- <추가> 버튼을 눌러 선택할 개체 이름을 입력한다.

[그림 9-31] 컴퓨터 추가

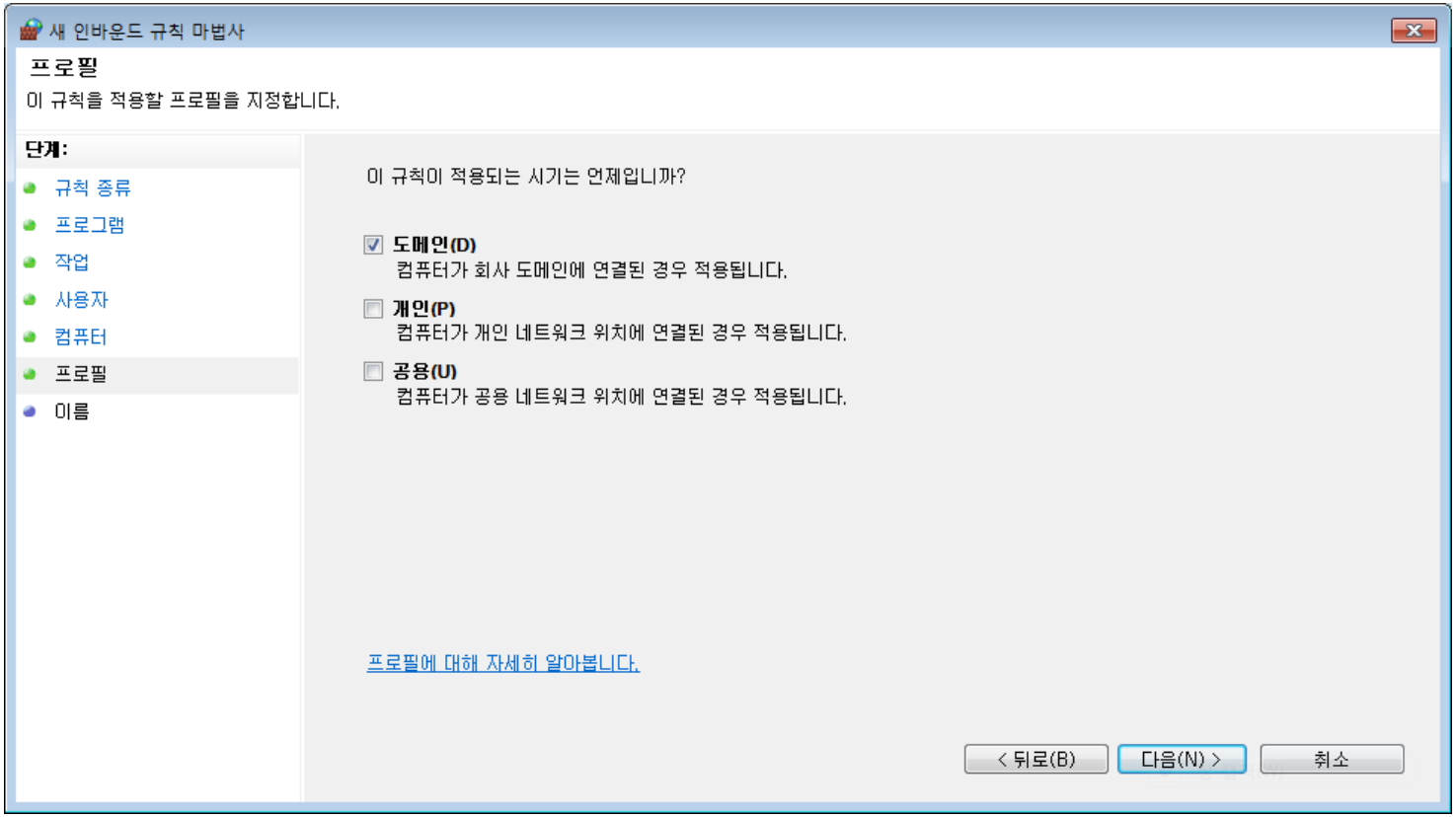


[그림 9-32] 컴퓨터 지정 완료 화면

03. 시스템 보안 기술 : 방화벽

⑦ 프로필 지정

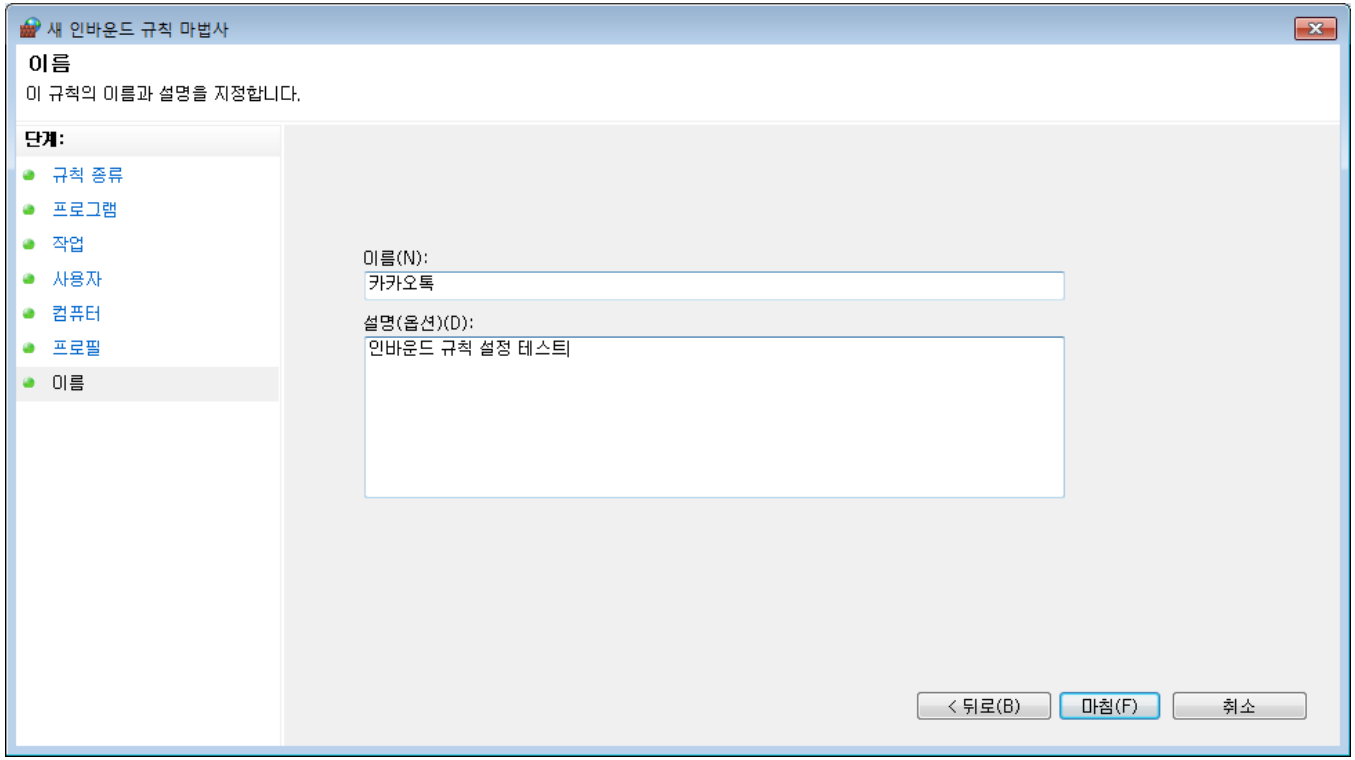
- 규칙을 적용할 프로필을 지정한다. 네트워크에 연결된 각 컴퓨터의 LAN 카드는 연결된 네트워크에서 검색된 프로필에 따라 프로필 중 하나를 할당 받는다.



03. 시스템 보안 기술 : 방화벽

⑧ 규칙의 이름과 설명 지정

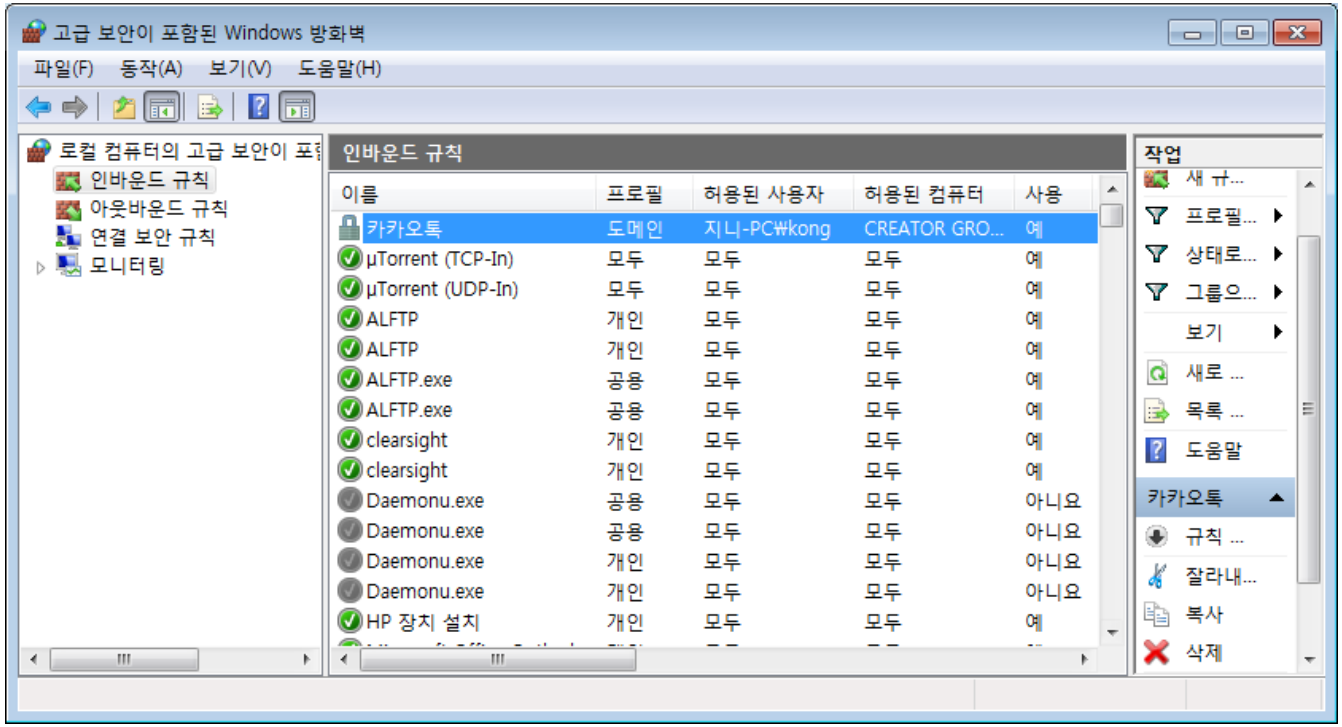
- 새로운 규칙의 이름과 설명을 지정한다.



[그림 9-34] 규칙의 이름과 설명 지정

03. 시스템 보안 기술 : 방화벽

- 이제 고급 보안이 포함된 Windows 방화벽의 인바운드 규칙에 카카오톡 프로그램이 추가된 것을 확인할 수 있다.



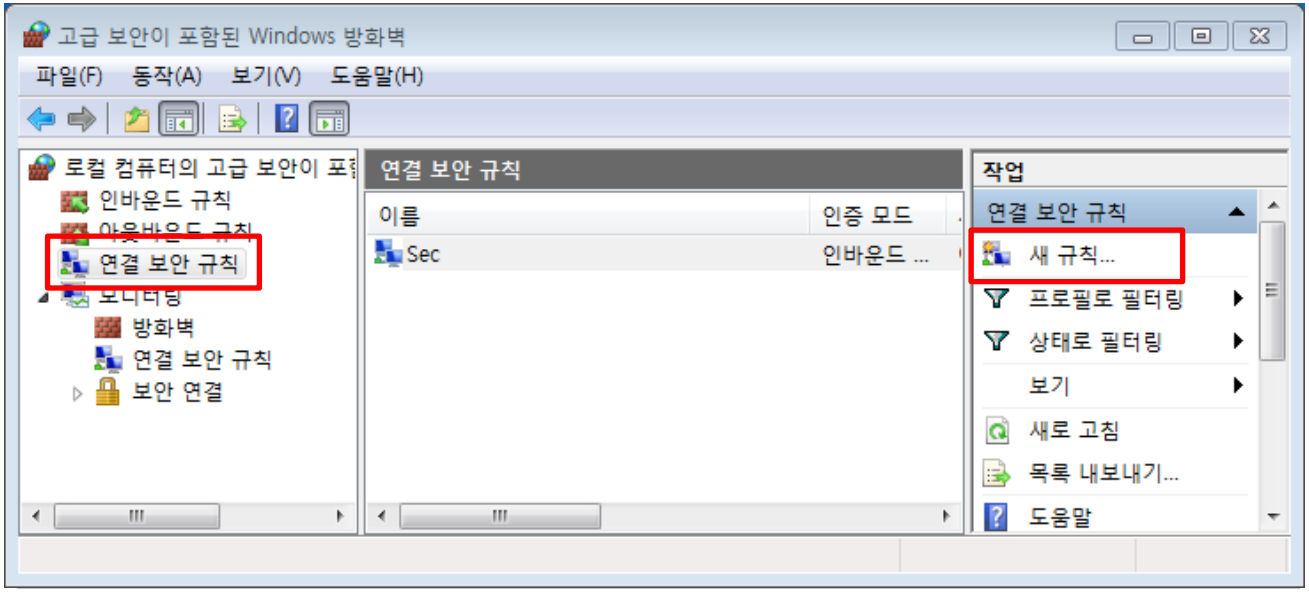
[그림 9-35] 새로운 인바운드 규칙 확인

03. 시스템 보안 기술 : 방화벽

■ 연결 보안 규칙

① 새로운 연결 보안 규칙 생성

- 고급 보안이 포함된 Windows 방화벽 창의 왼쪽 부분에서 <연결 보안 규칙>을 클릭한 후 오른쪽 부분에서 <새 규칙>을 클릭한다.

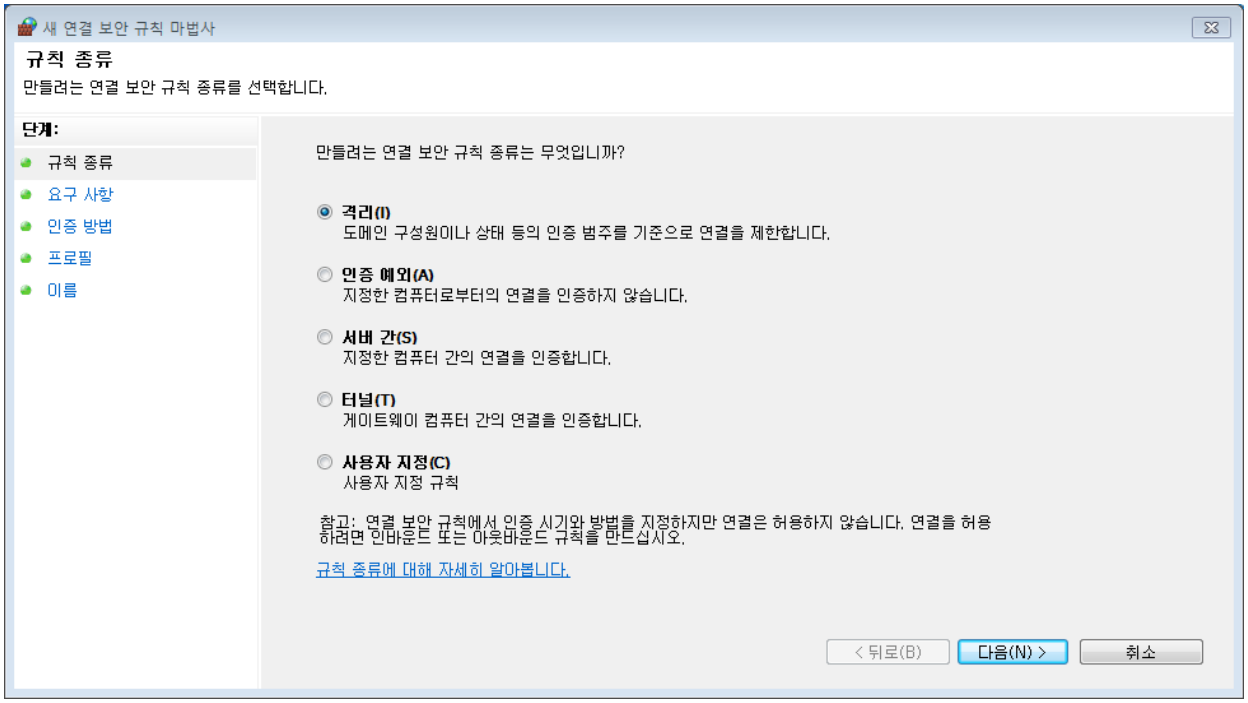


[그림 9-36] 새로운 연결 보안 규칙 생성

03. 시스템 보안 기술 : 방화벽

② 연결 보안 규칙 종류 선택

- [새 연결 보안 규칙 마법사] 대화상자에서 만들려는 연결 보안 규칙 종류를 선택한다.
  - 다양한 네트워크 보안 목적에 맞는 IPsec 규칙을 만들 수 있다.

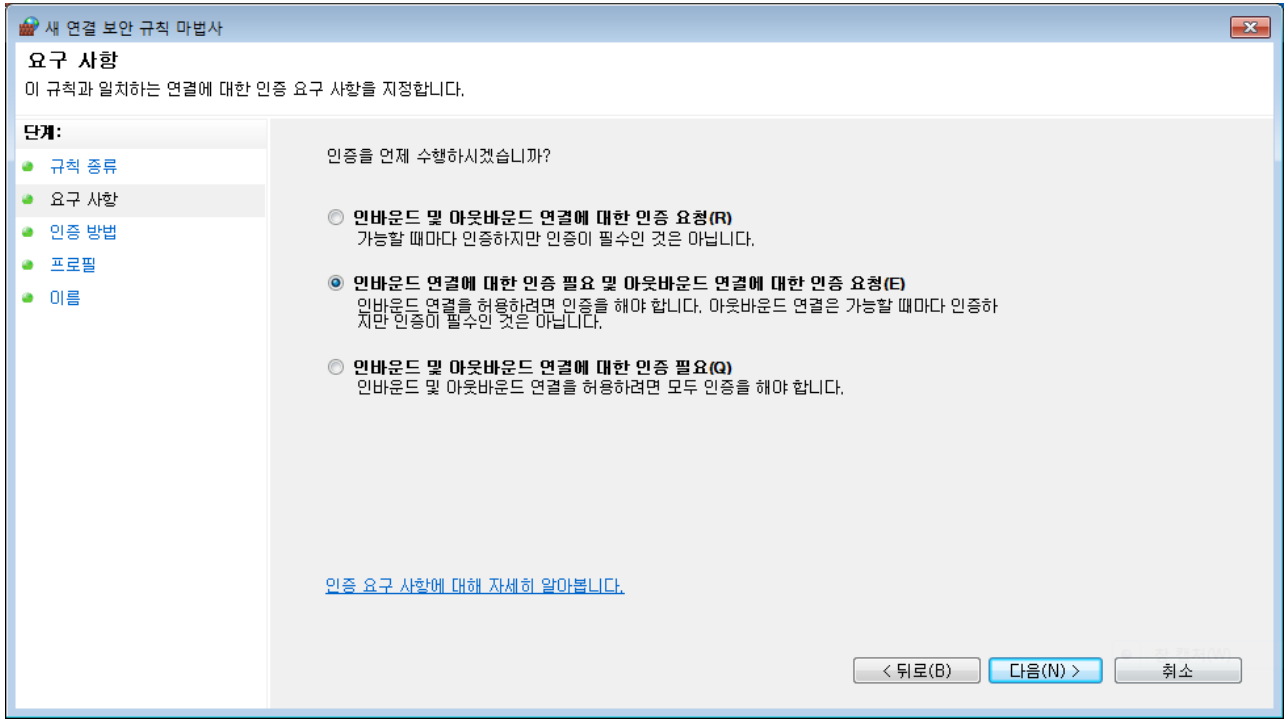


[그림 9-37] 연결 보안 규칙 종류 선택

03. 시스템 보안 기술 : 방화벽

③ 요구 사항 지정

- 규칙과 일치하는 연결에 대한 인증 요구 사항을 지정한다.
  - 연결 보안 규칙과 일치하는 인바운드 및 아웃바운드 연결에 인증이 적용되는 방식을 선택할 수 있다. 인증 필요를 선택하면 인증에 실패했을 때 연결이 끊어지지만, 인증 요청을 선택하면 인증에 실패하더라도 연결이 허용된다.

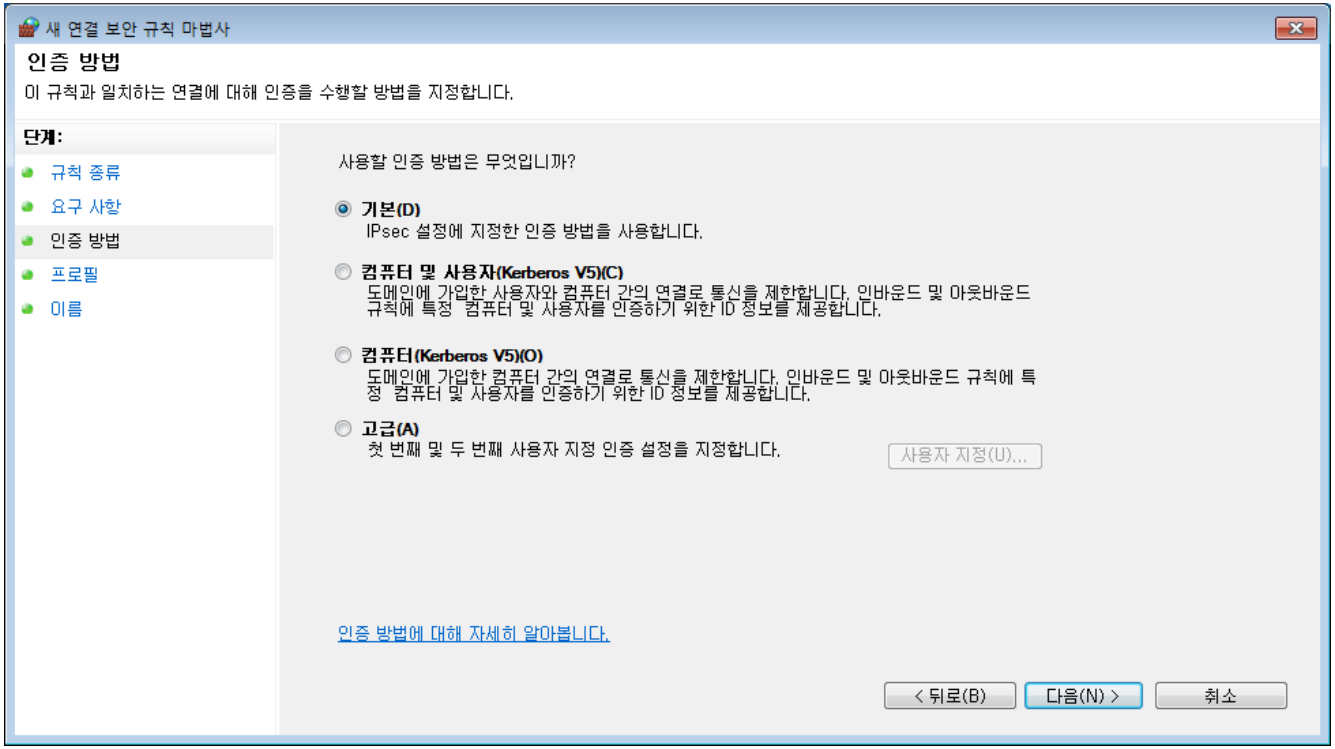


[그림 9-38] 규칙과 일치하는 연결에 대한 인증 요구 사항 지정

03. 시스템 보안 기술 : 방화벽

④ 인증 방법 지정

- 규칙과 일치하는 연결에서 인증을 수행할 방법을 지정한다. 연결 보안 규칙에서 사용하는 인증 유형을 선택할 수 있다.

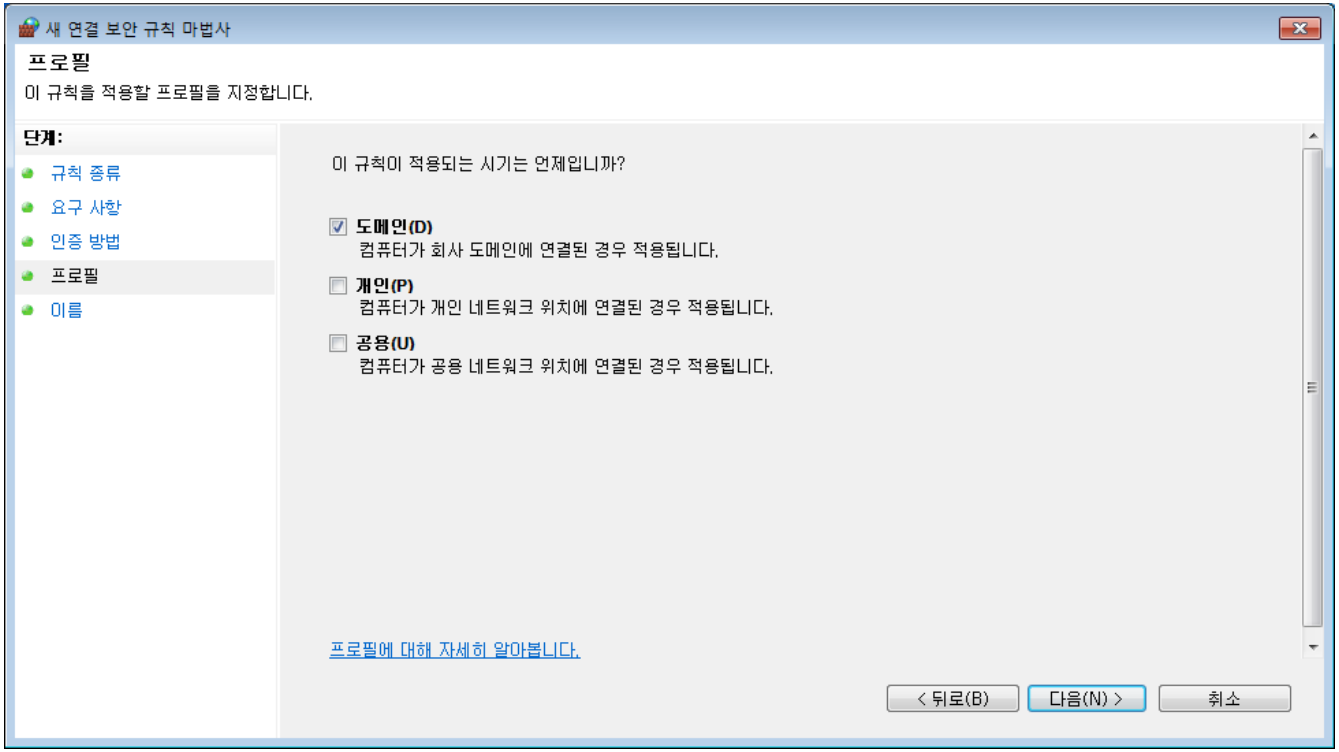


[그림 9-39] 인증을 수행할 방법 지정

03. 시스템 보안 기술 : 방화벽

⑤ 프로필 지정

- 이 규칙에 적용할 프로필을 지정한다.

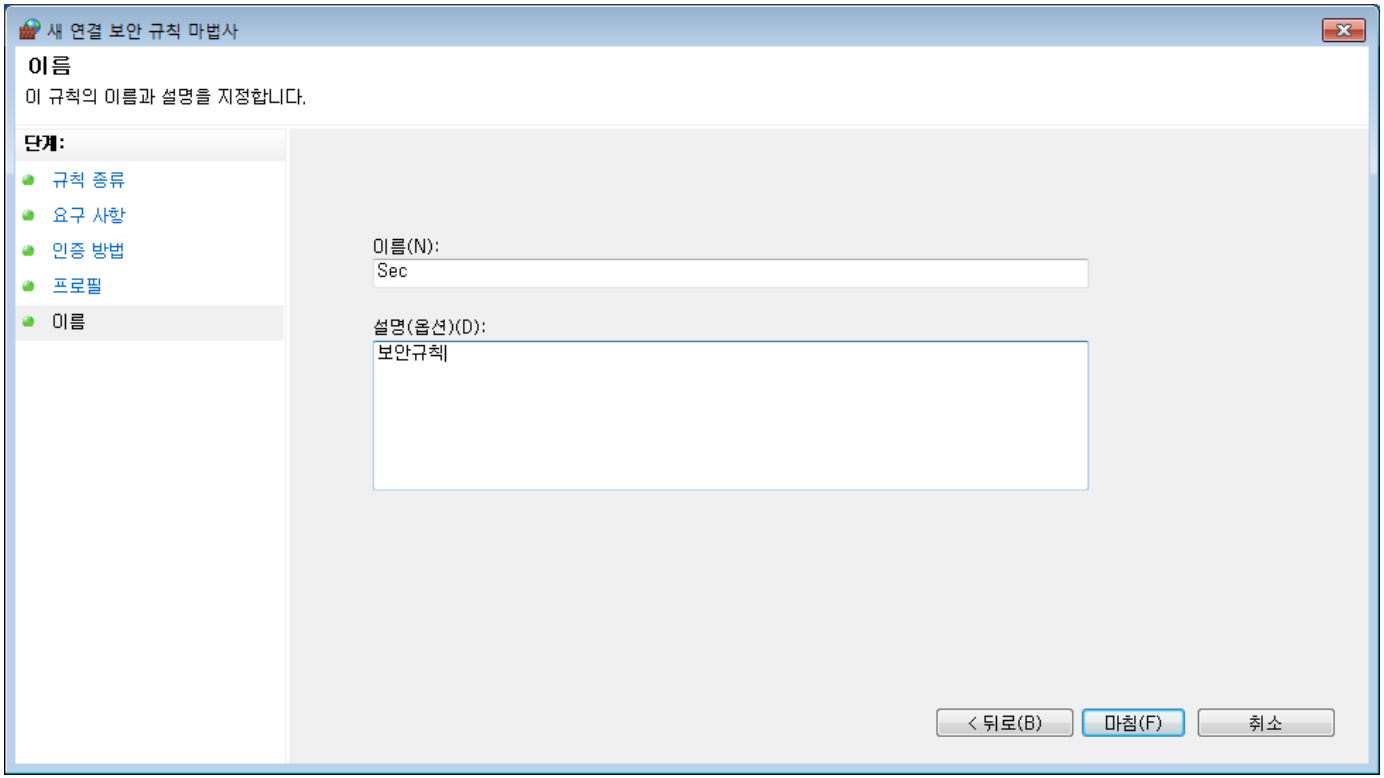


[그림 9-40] 규칙에 적용할 프로필 지정

03. 시스템 보안 기술 : 방화벽

⑥ 이름과 설명 지정

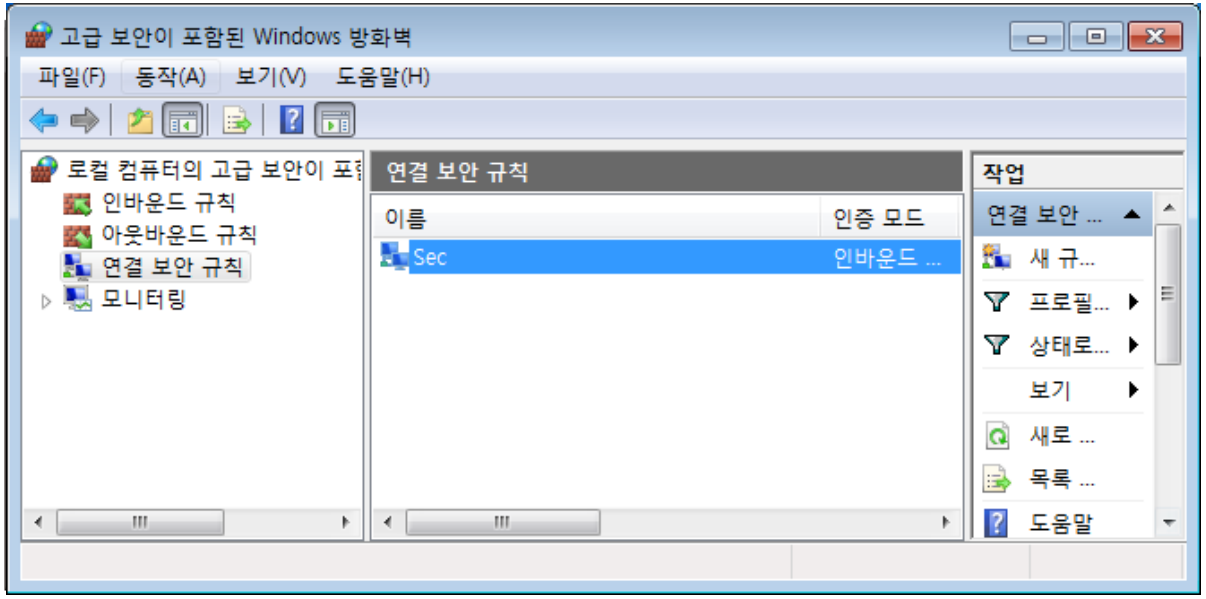
- 연결 보안 규칙의 이름과 설명을 지정한다.



[그림 9-41] 연결 보안 규칙의 이름과 설명 지정

03. 시스템 보안 기술 : 방화벽

- 이제 고급 보안이 포함된 Windows 방화벽에 새로운 연결 보안 규칙이 추가된 것을 확인할 수 있다.



[그림 9-42] 새로운 연결 보안 규칙 확인

03. 시스템 보안 기술 : 침입 탐지 시스템

침입 탐지 시스템(IDS)

- 방화벽 등 네트워크 보안 시스템은 인증 받은 사용자나 네트워크, 응용 프로그램만 네트워크 자원에 접근하는 것을 허용한다.
- 방화벽처럼 단순한 접근 제어 수준의 통제만으로는 악의적인 공격에 효과적으로 대처하는 것이 불가능하다.
- 따라서 네트워크와 시스템의 사용을 실시간으로 모니터링하고 침입을 탐지하는 침입 탐지 시스템이 등장하게 되었다.
- H-IDS는 컴퓨터에 탑재되며, N-IDS는 네트워크에 설치된다.
  - 보통 국내에서는 N-IDS를 IDS라고 부른다.

[그림 9-43] 침입 탐지 시스템

03. 시스템 보안 기술 : 침입 탐지 시스템

침입 탐지 시스템의 분류

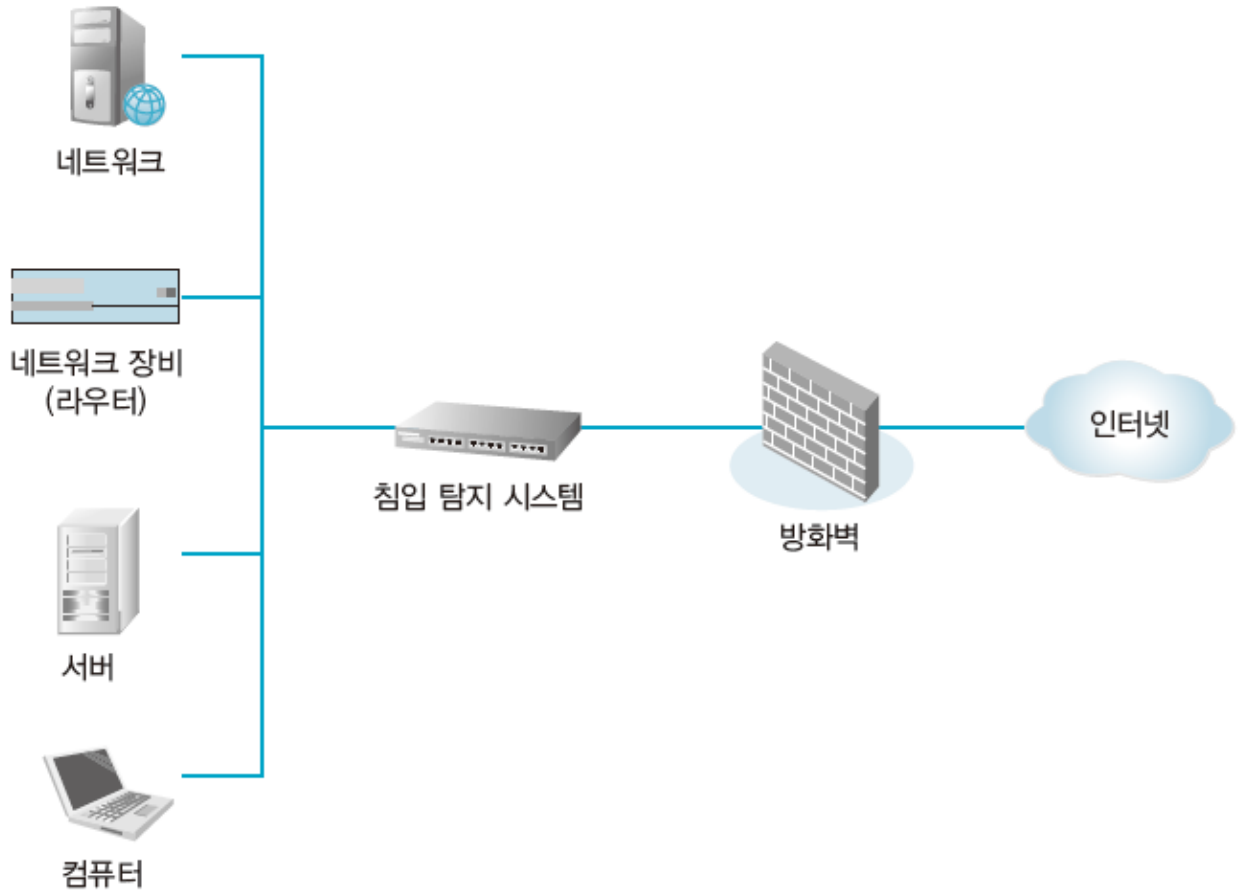
① 기초 자료의 종류에 따른 분류

- 단일 호스트 기반 : 침입 탐지 시스템을 설치한 단일 호스트에서 생성되고, 수집된 감사 자료를 침입 탐지에 활용하는 방식이다.
- 다중 호스트 기반 : 단일 호스트 기반과 동일한 방식이지만, 여러 호스트의 자료를 활용한다.
- 네트워크 기반 : 해당 네트워크 전체의 패킷 관련 자료를 수집하여 침입 탐지에 활용하는 방식이다.

② 침입 행위의 기준에 따른 분류

- 정상적인 행위의 탐지 : 정상적으로 시스템을 사용한 행위의 프로파일을 보유하고 있다가 프로파일의 기준에서 벗어나면 즉시 탐지 작업을 수행하는 방식이다.
- 잘못된 행위의 탐지 : 시스템의 잘 알려진 취약점을 공격하는 행위의 프로파일을 보유하고 있다가 해당 공격이 취해지면 즉시 탐지 작업에 들어가는 방식이다.

03. 시스템 보안 기술 : 침입 탐지 시스템



[그림 9-44] 침입 탐지 시스템의 구조

03. 시스템 보안 기술 : 침입 방지 시스템

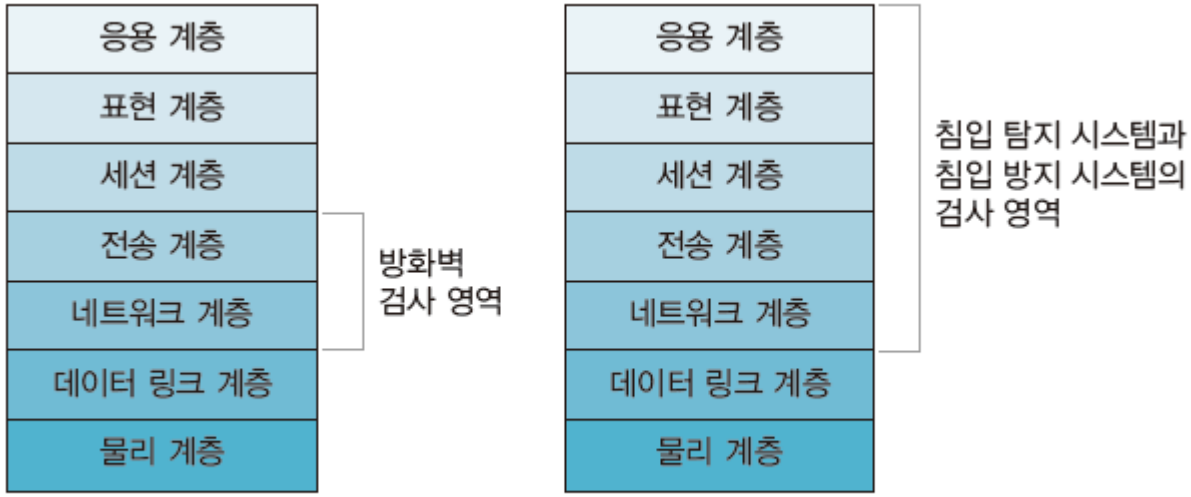
침입 방지 시스템(IPS)

- 최근 방화벽과 침입 탐지 시스템을 이용한 보안 관리의 한계를 극복하려고 침입 방지 시스템(IPS,Intrusion Prevention System)의 도입에 관심이 높아졌다.
- 차세대 능동형 네트워크 보안 솔루션인 침입 방지 시스템은 네트워크에 상주하면서 트래픽을 모니터링하여 악성코드 및 해킹 등의 유해 트래픽을 차단하고, 의심스러운 세션들을 종료시키거나공격에 대처하는 등 다양한 조치를 취하여 적극적으로 네트워크를 보호한다.

[그림 9-45] 침입 방지 시스템

03. 시스템 보안 기술

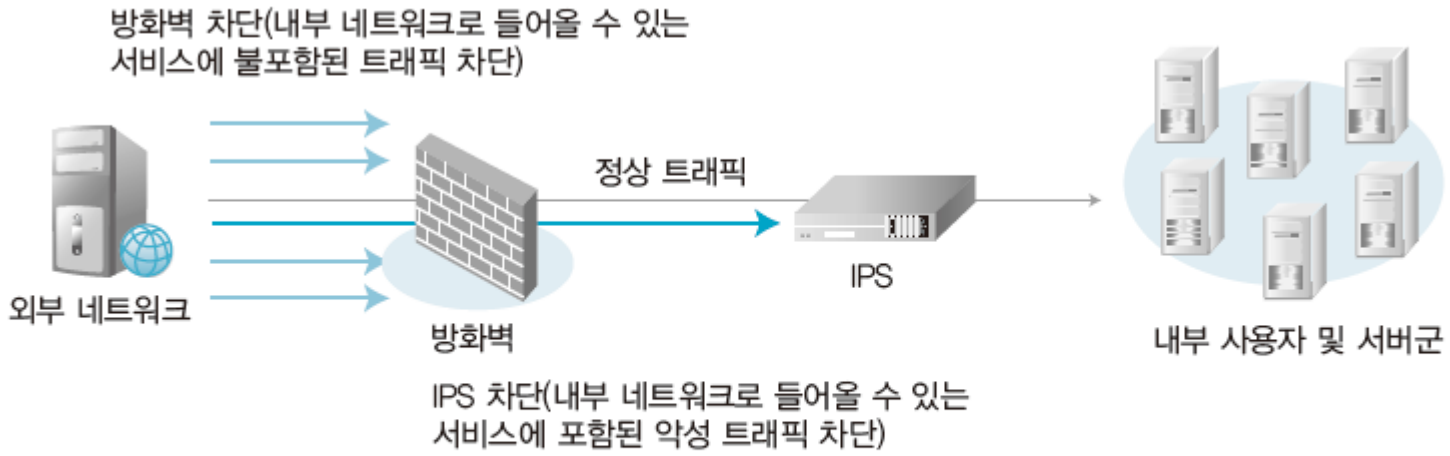
- 방화벽, 침입 탐지 시스템, 침입 방지 시스템의 비교
  - 방화벽은 전송 계층과 네트워크 계층의 IP/Port 데이터를 기반으로 동작한다.
  - 반면, 침입방지 시스템은 방화벽이 검사할 수 없는 응용 계층 데이터까지 검사할 수 있다.
  - 침입 탐지 시스템과 침입 방지 시스템 등 네트워크 보안 시스템에서 비정상 트래픽을 탐지하려고 네트워크 패킷의 헤더뿐만 아니라 헤더를 제외한 페이로드에 포함된 데이터까지 심층적으로 분석하는 기술로 DPI(Deep Packet Inspection)를 사용한다.



[그림 9-46] 방화벽, 침입 탐지 시스템, 침입 방지 시스템의 검사 영역

03. 시스템 보안 기술

- 침입 탐지 시스템과 침입 방지 시스템은 IP 변경 없이 네트워크 구성을 설치하므로, 설치하는 구간의 제약은 없다. 보통 인터넷 구간의 방화벽 뒤편에 설치하여 방화벽으로 필터링할 수 없는 트래픽을 차단하는 형식으로 설치된다.



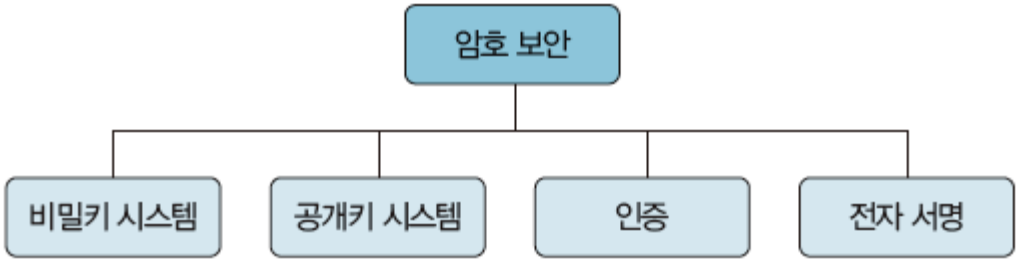
[그림 9-47] 방화벽과 IPS의 설치 위치

04. 암호 보안 기술

암호 보안 기술

암호화 방식

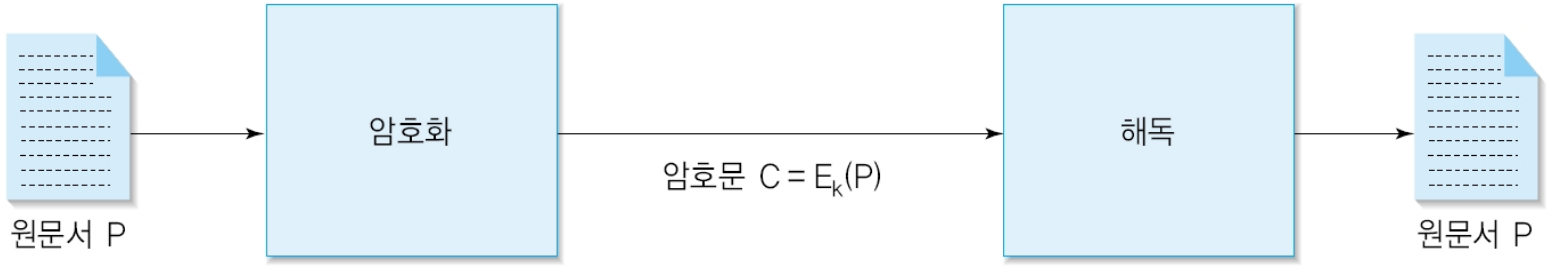
- 암호화는 키와 알고리즘으로 구성되며, 키의 값에 따라 알고리즘의 출력이 바뀐다.
- 키는 매우 큰 숫자 중 하나이며, 키가 가질 수 있는 가능한 값의 범위를 '키스페이스(Keyspace)'라고 한다.
- 이 키를 이용하여 암호화 및 복호화되며, 키의값을 제외하고는 모든 사용자가 동일한 암호화 및 복호화 알고리즘(Algorithm)을 사용한다.
- 암호를 사용하려면 송신자와 수신자가 메시지를 암호문으로 바꿀 때 사용한 규칙이 어떤 것인지 알아야 한다.



[그림 9-48] 암호 보안 기술

1절. 암호화의 이해

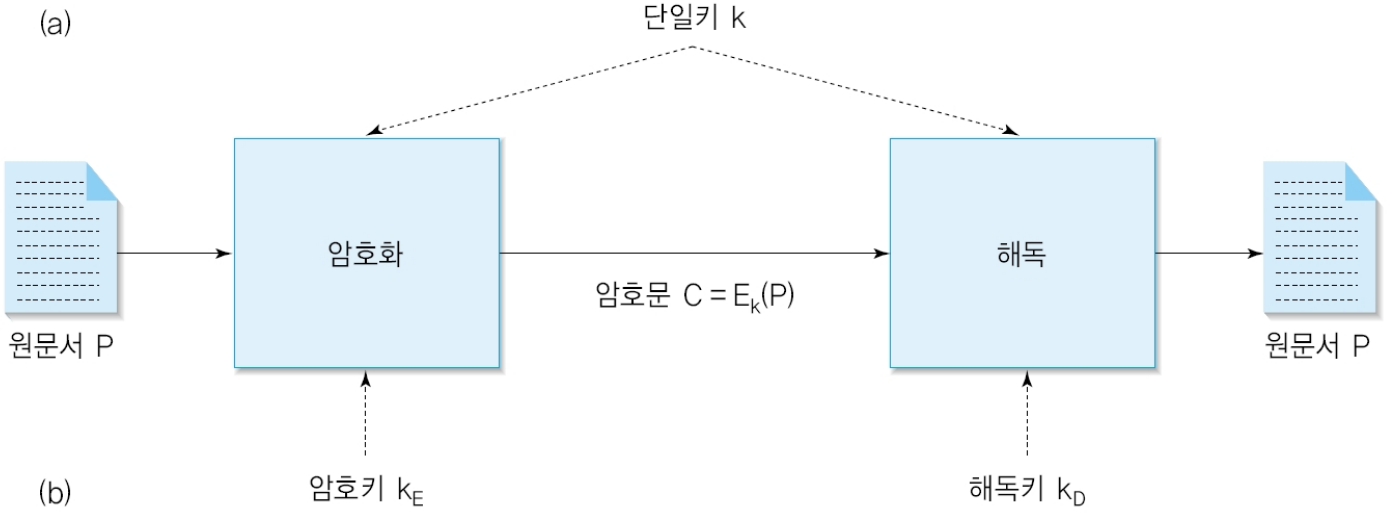
- 암호화 관련 용어
  - 암호화 용어 [그림 13-1]
    - 암호화: 메시지의 내용을 변형하여 원래의 의미를 알 수 없도록 변형
    - 해독: 암호화된 문서를 원래의 원어로 복원
    - 원문서(P): 암호화되기 전의 원본 문서
    - 암호문(C): 암호화된 문서



[그림 13-1] 암호화 과정과 용어

1절. 암호화의 이해

- 암호화 관련 용어
  - 암호화 알고리즘
    - 암호키(k_E): 암호화 과정에서 사용하는 키
    - 해독키(k_D): 해독 과정에서 사용하는 키
    - 대칭키 방식: 암호키 = 해독키 [그림 13-2(a)]



[그림 13-2] 키의 종류

암호화의 이해

- 대체 암호화
  - 특정 문자를 다른 문자로 1:1 대응

  – 시저 암호화
    - 알파벳 문자를 순차적으로 세 문자씩 오른쪽으로 이동
    - 암호키

원문 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

암호문 d e f g h i j k l m n o p q r s t u v w x y z a b c

- 예

N E T W O R K T E C H N O L O G Y

q h w z r u n w h f k q r o r j b

암호화의 이해

- 대체 암호화
  - 키워드 암호화
    - 키워드로 지정된 단어의 문자를 먼저 적고 나머지 문자를 알파벳 순으

원문 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

암호문 s e o u l a b c d f g h i j k m n p q r t v w x y z

키워드 s, e, o, u, l을 제외한 문자를 알파벳 순서로 배치

암호화의 이해

- 대체 암호화
  - 복수개의 문자표
    - 둘 이상의 문자표를 사용

홀수 위치에 있는 문자

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

짝수 위치에 있는 문자

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	s	e	o	u	l	a	b	c	d	f	g	h	i	j	k	m	n	p	q	r	t	v	w	x	y	z

암호화의 이해

- 대체 암호화
  - 복수개의 문자표
    - 예

1	2	3	4	5	6	7		8	9	10	11	12	13	14	15	16	17
N	E	T	W	O	R	K		T	E	C	H	N	O	L	O	G	Y
q	l	w	w	r	p	n		r	h	u	k	j	r	h	r	b	b

홀수 위치에 있는 문자

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

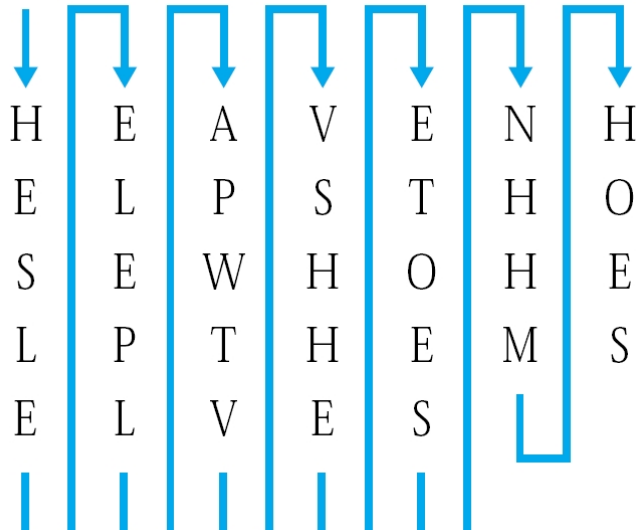
짝수 위치에 있는 문자

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	s	e	o	u	l	a	b	c	d	f	g	h	i	j	k	m	n	p	q	r	t	v	w	x	y	z

암호화의 이해

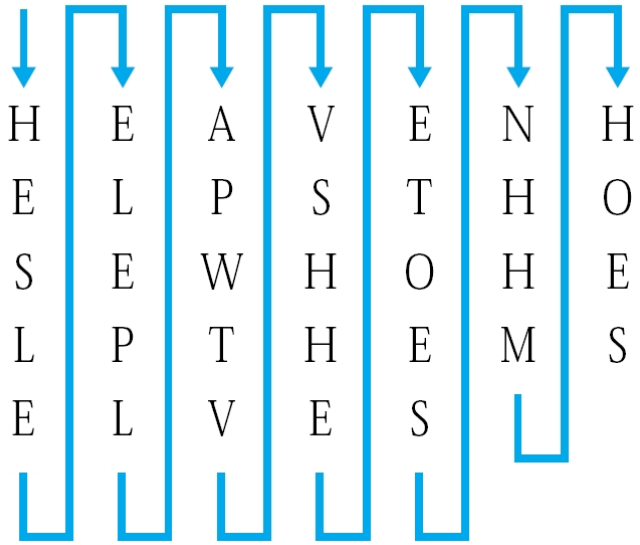
- 위치 암호화
  - 문자들의 배열 순서를 변경

  – 컬럼 암호화
    - 전체 문장을 컬럼(열)을 기준으로 다시 배치
    - 예: 컬럼의 길이가 7 인 경우
      – 원문서: HEAVEN HELPS THOSE WHO HELP THEMSELVES
      – 암호문1: hesle elepl apwtv vshhe etoes nhhm hoes



암호화의 이해

- 위치 암호화
  - 컬럼 암호화
    - 예: 컬럼의 길이가 7이며, 공백에 Z 문자를 강제로 채운 경우
      - 원문서: HEAVEN HELPS THOSE WHO HELP THEMSELVES
      - 암호문2: hesle elepl apwtv vshhe etoes nhhmz heosz



암호화의 이해

- 위치 암호화
  - 키워드 암호화
    - 임의의 단어를 이용하여 컬럼의 순서를 결정
    - 예: NETWORK

키워드	N	E	T	W	O	R	K
순서	3	1	6	7	4	5	2
	H	E	A	V	E	N	H
	E	L	P	S	T	H	O
	S	E	W	H	O	H	E
	L	P	T	H	E	M	S
	E	L	V	E	S	Z	Z

THEMSELVES
tv vshhe

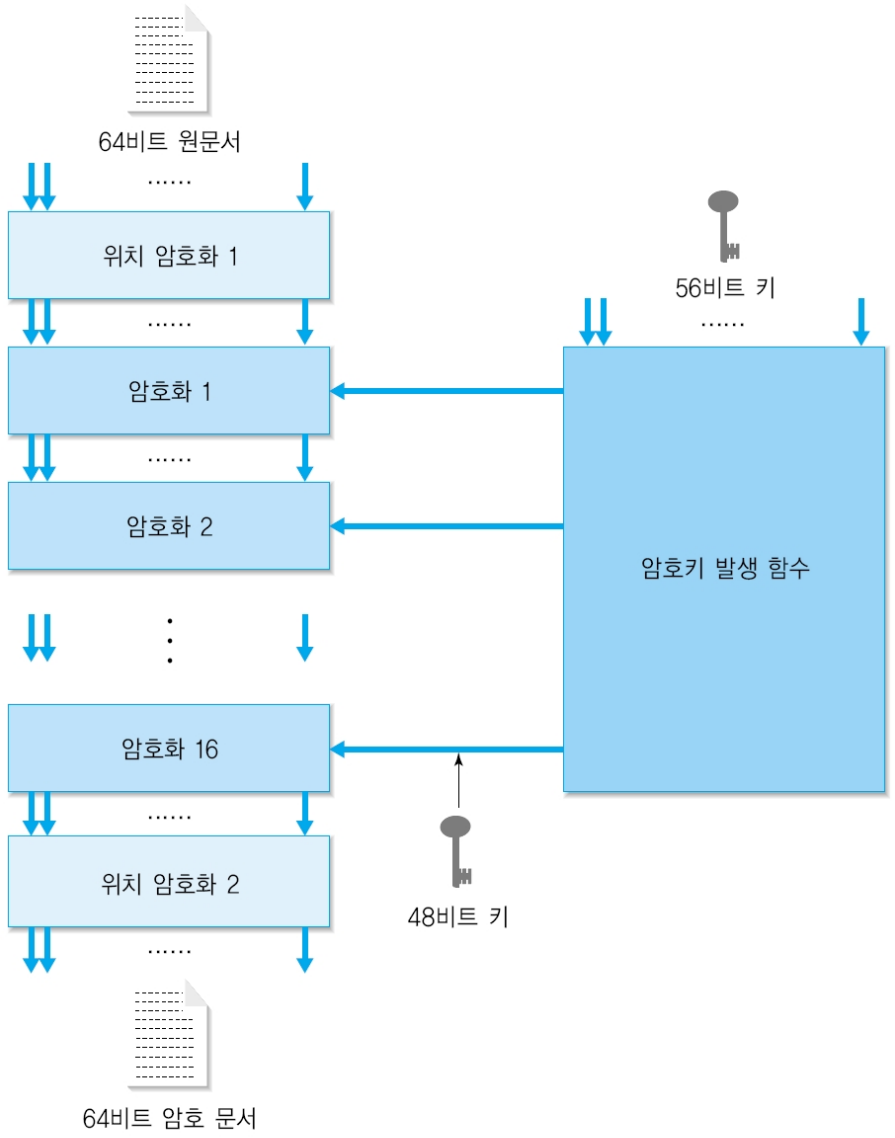
암호화 시스템

- 컴퓨터 보급 전: 수작업을 위해 알고리즘은 간단하고 암호키가 복잡하게 구성
- 컴퓨터 보급 후: 알고리즘의 복잡도가 증가됨

- DES 알고리즘
  - 대칭키의 비공개키 알고리즘
  - 동작 방식
    - 암호키: 56 비트
    - 64 비트 단위로 암호화
    - 16 단계의 암호화 과정을 수행: 16 + 2 단계

암호화 시스템

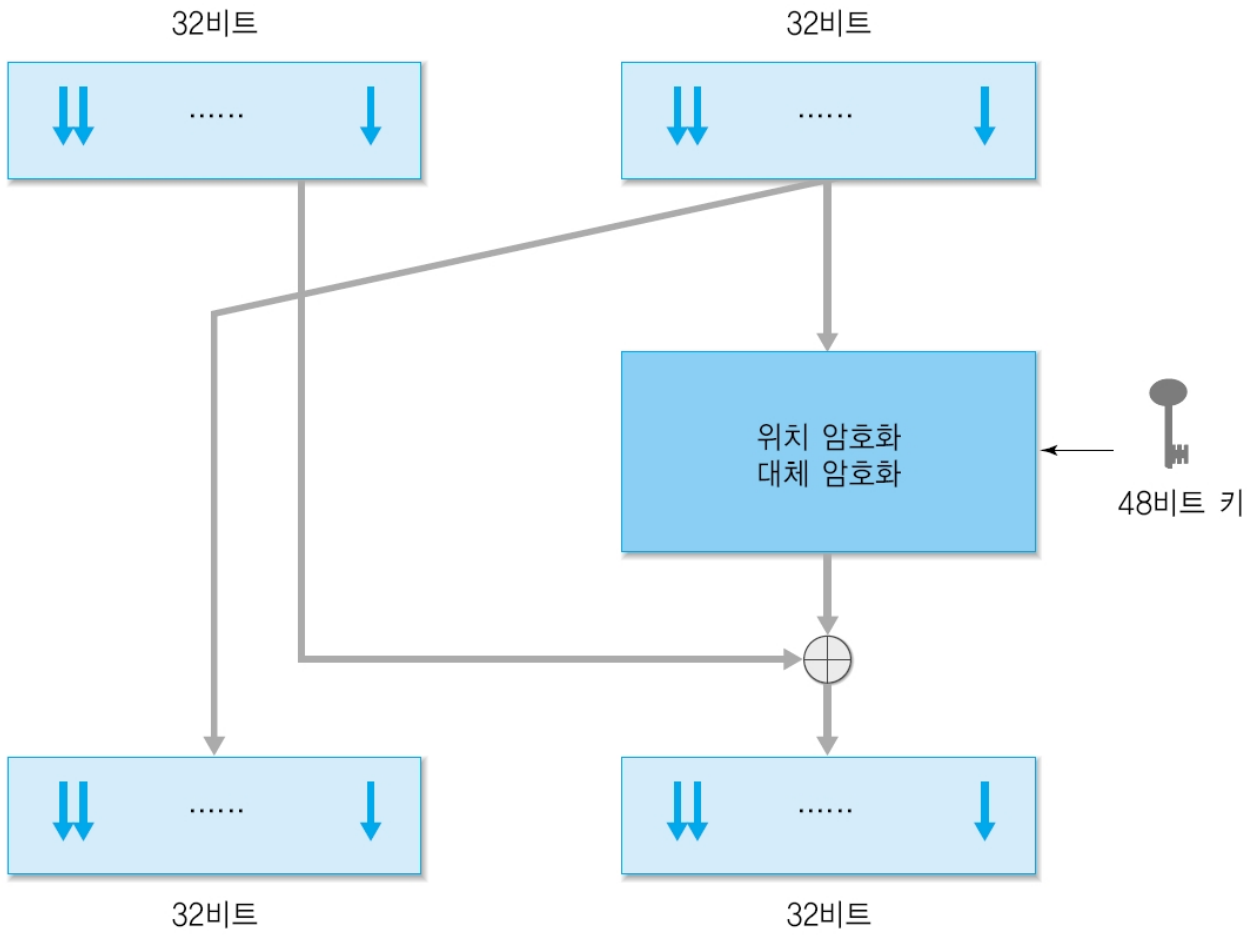
- DES 알고리즘
  - 동작 방식 [그림 13-3]



[그림 13-3] DES 알고리즘 동작 과정

암호화 시스템

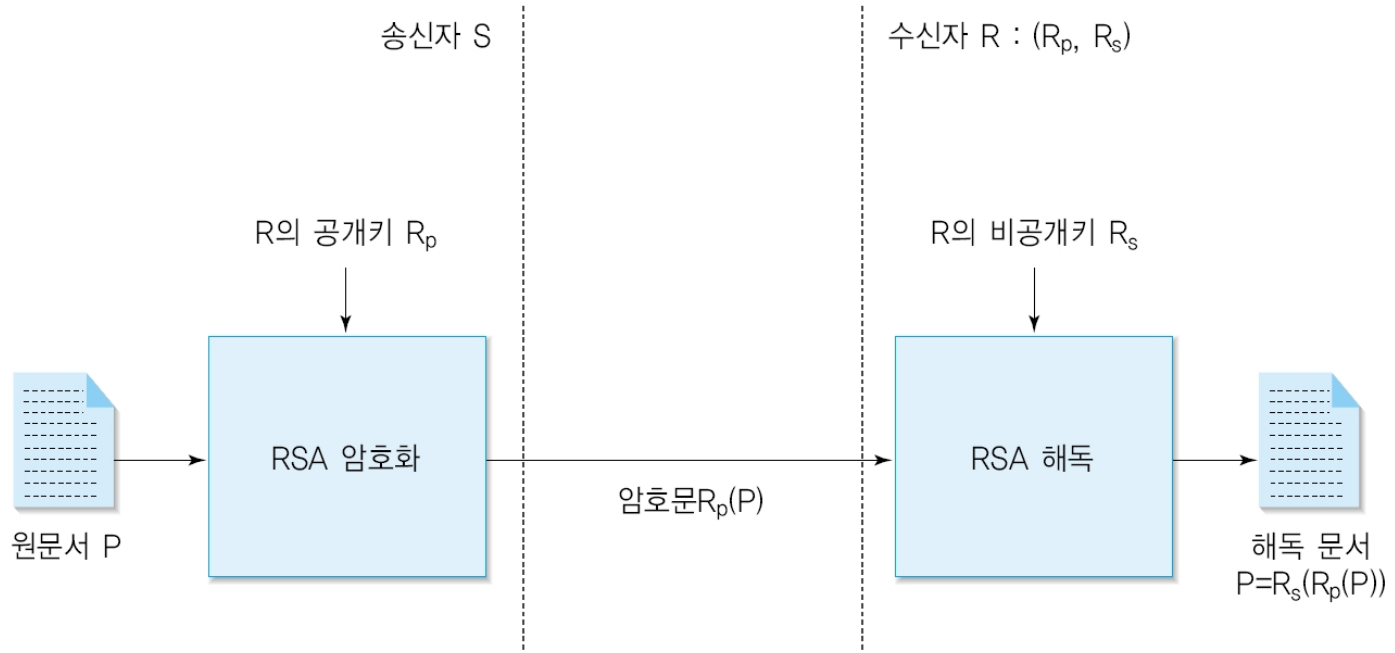
- DES 알고리즘
  - 16 단계의 암호화 [그림 13-4]



[그림 13-4] [그림 13-3]의 16단계 암호화 알고리즘

암호화 시스템

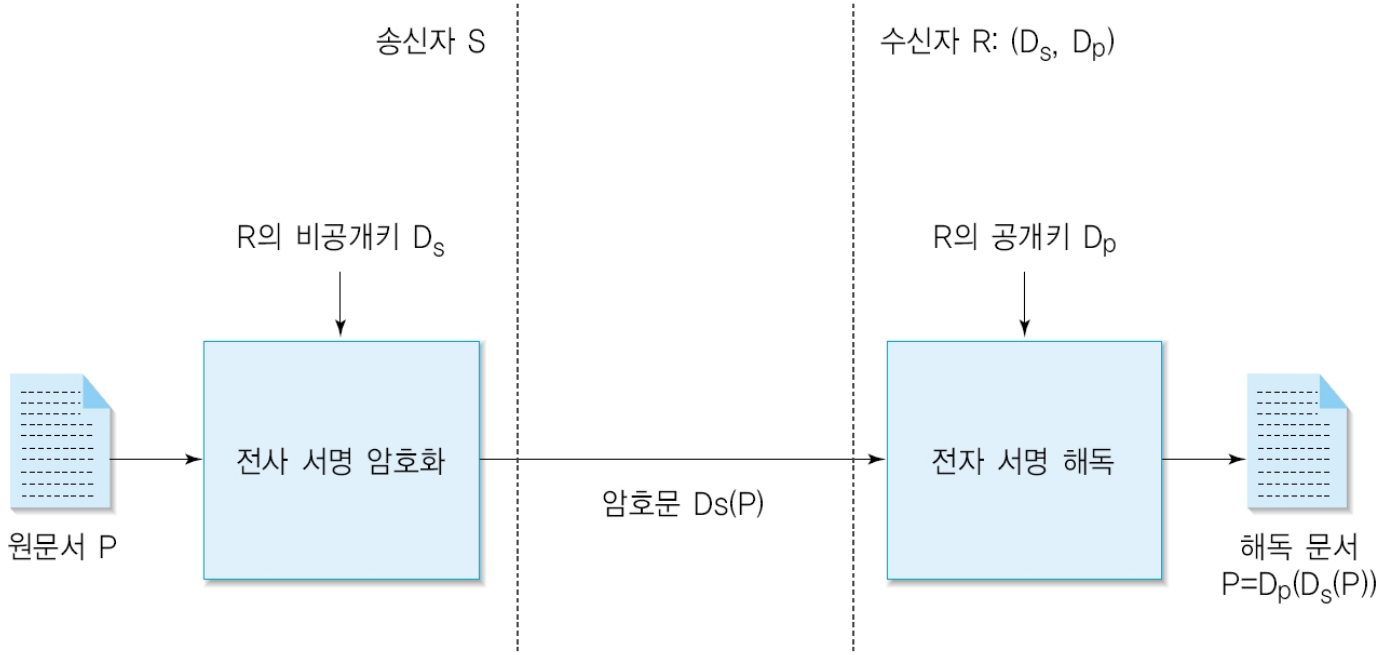
- RSA 알고리즘
  - 비대칭키의 공개키 알고리즘
    - 공개키: 원문서를 암호화하는 용도로 사용 (모든 사람이 암호화 과정 수행)
    - 비공개키: 암호문을 해독하는 용도로 사용 (특정인만 해독 과정 수행)
  - RSA 알고리즘 [그림 13-5]
    - (공개키, 비공개키) 조합을 생성



[그림 13-5] RSA 알고리즘

암호화 시스템

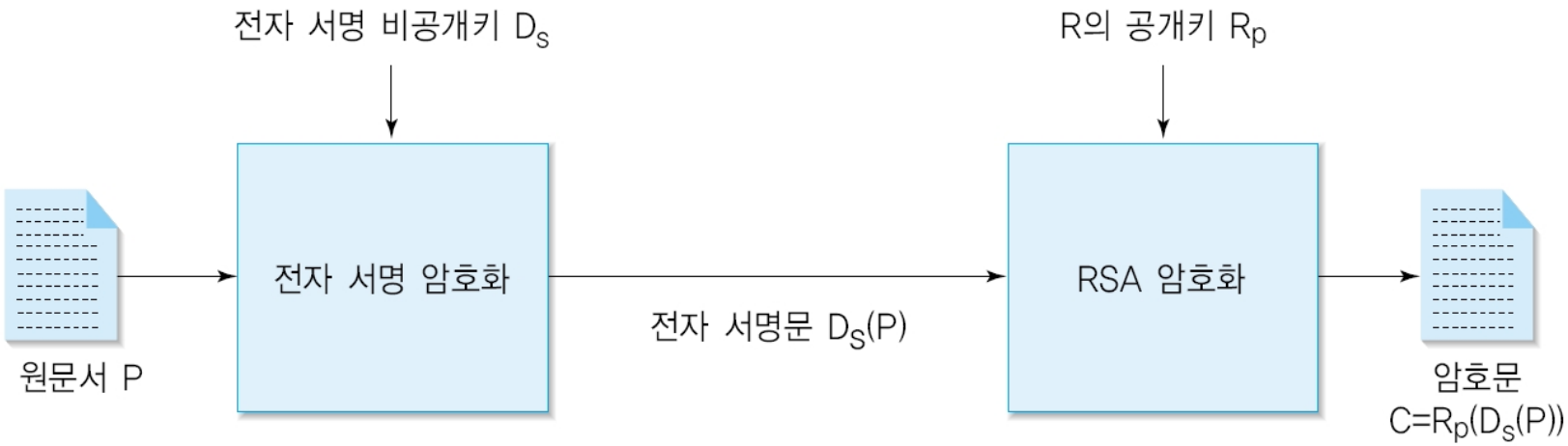
- 전자 서명
  - 사용자의 인증 기능 제공
  - RSA 알고리즘과 반대 원리로 동작 [그림 13-6]
    - 비공개키: 원문서를 암호화하는 용도로 사용 (특정인만 암호화 과정 수행)
    - 공개키: 암호문을 해독하는 용도로 사용 (모든 사람이 해독 과정 수행)



[그림 13-6] 전자 서명의 원리

암호화 시스템

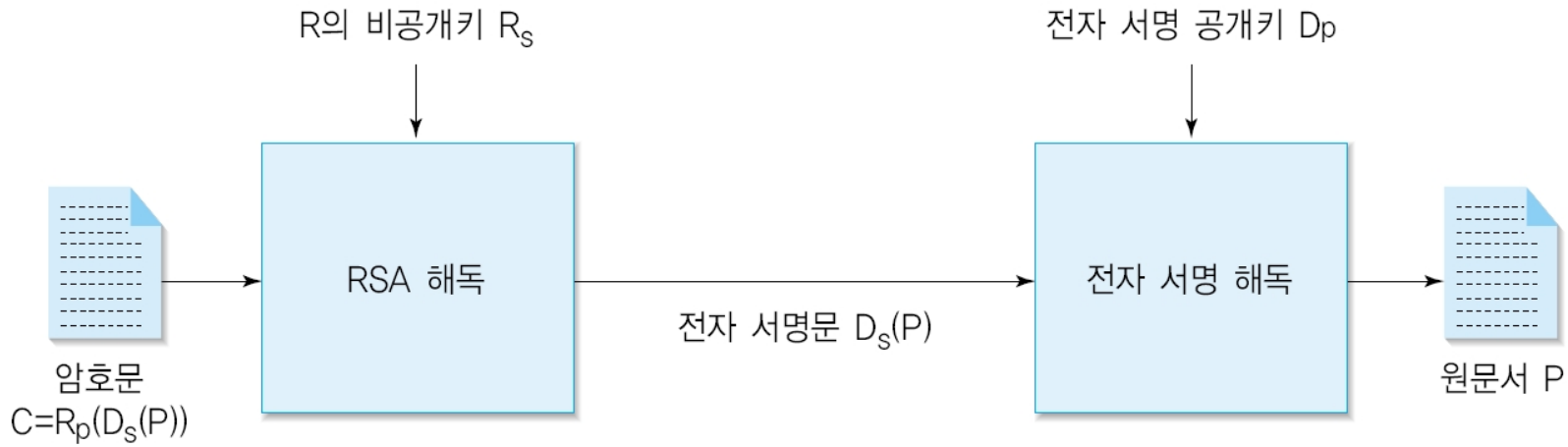
- 전자 서명
  - 암호화 과정 [그림 13-7]
    - 1단계: 전자 서명 알고리즘으로 인증 정보를 암호화 (사용자 인증)
    - 2단계: RSA 알고리즘으로 전자 서명 정보를 암호화 (전송 보안)



[그림 13-7] 전자 서명 암호화

암호화 시스템

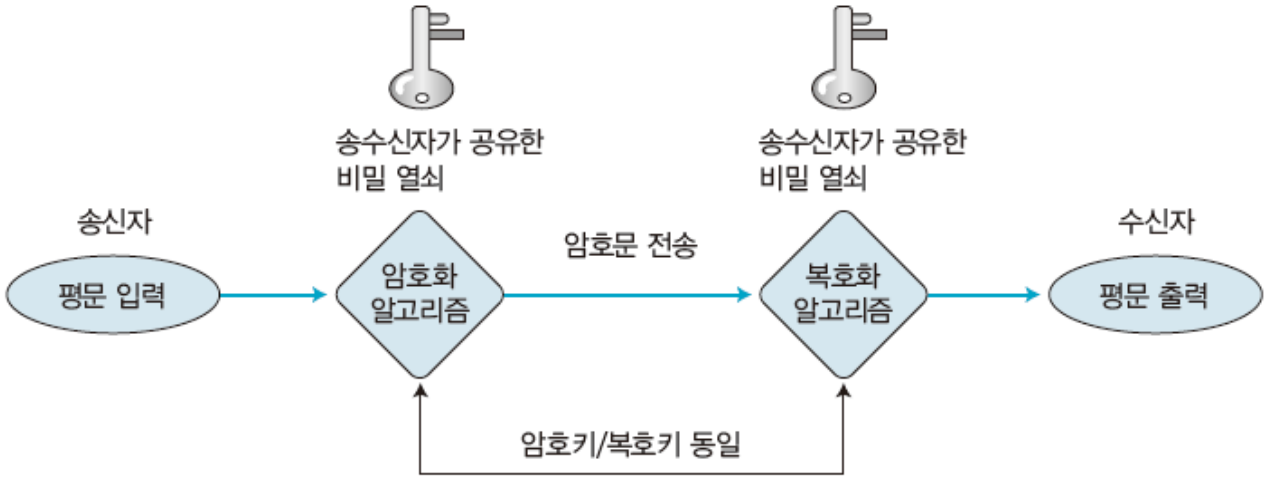
- 전자 서명
  - 해독 과정 [그림 13-8]
    - 1단계: RSA 알고리즘으로 전자 서명 정보를 해독
    - 2단계: 전자 서명 알고리즘으로 인증 정보 해독



[그림 13-8] 전자 서명 해독

04. 암호 보안 기술

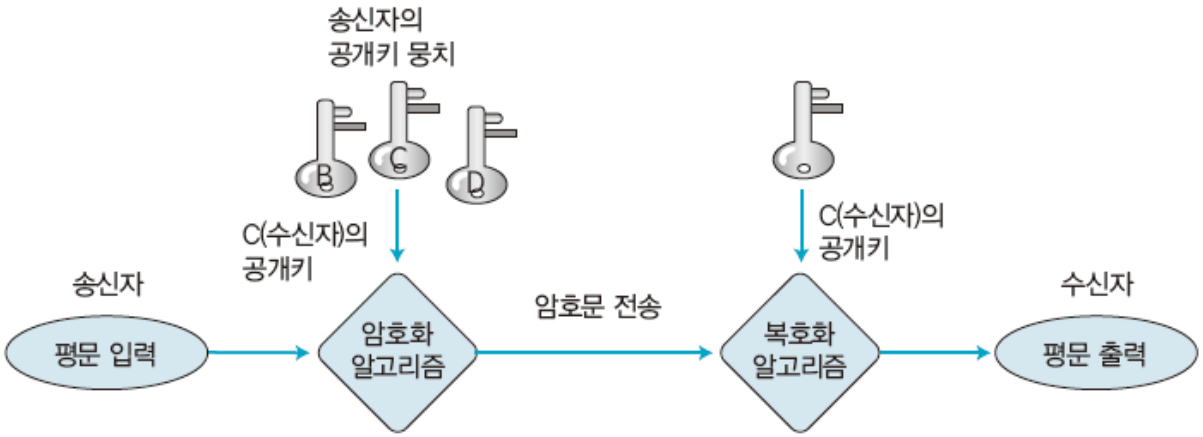
- 비밀키 암호화 방식
  - 비밀키 암호화 방식(Secret-key Algorithm, Symmetric Algorithm)은 암호키와 복호키가 동일하므로 두 개체가 같은 키를 공유하면서 하나의 키를 사용하여 암호화하고 복호화한다.
  - 암호키에서 복호키를 계산하거나 복호키에서 암호키를 계산할 수 있을 때 비밀키 암호화 방식이라고 한다.
  - 비밀키 암호화 과정을 보여준다. 암호문을 만들어 전송한 후 같은 키로 해독하여 평문으로 바꿀 수 있다.



[그림 9-49] 비밀키 암호화 방식

04. 암호 보안 기술

- 공개키 암호화 방식
  - 공개키 암호화 방식(Public-key Algorithm, Asymmetric Algorithm)은 암호키와 복호키가 서로 다르며, 암호키에서 복호키를 계산할 수 없다.
  - 암호키가 공개되어 있어 누구나 원하는 내용을 암호화할 수 있지만, 해당 복호키(개인키)를 가진 사람만 그 암호문을 복호화할 수 있기 때문에 이 알고리즘에서는 암호키를 '공개키'라 하고, 복호키를 '개인키(Private Key)'라고 한다.
  - 이 방식은 전송 도중 메시지가 도청당하더라도 개인키가 있어야만 메시지를 볼 수 있기 때문에 안전할 뿐만 아니라 개인키를 공개할 필요가 없어 외부에 알려질 위험도 없다.



[그림 9-50] 공개키 암호화 방식

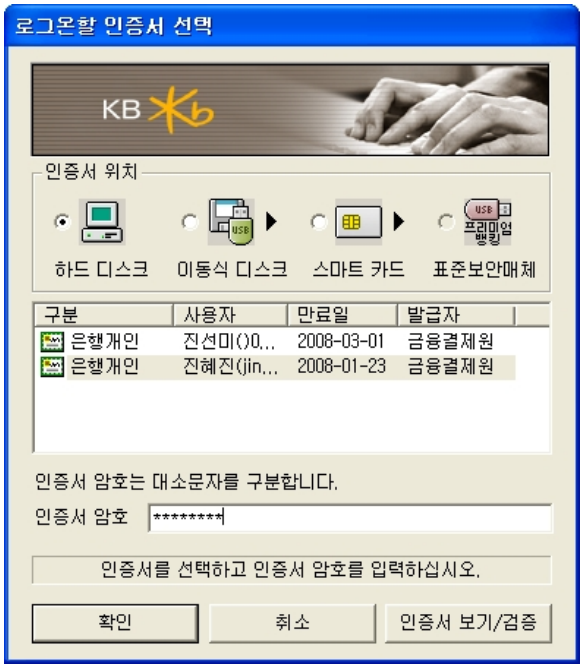
04. 암호 보안 기술

- 인증
  - 네트워크 보안의 중요한 내용 중 하나는 권한이 있는 사용자만 정보에 접근할 수 있도록 하는 것이다.
  - 이를 위해 시스템에 접근하는 각 사용자가 권한이 있는 사용자인지 구분해야 하고, 각 사용자가 본인 여부를 확인하는 과정도 필요하다.
- 생체 인식
  - 생체 인식은 개인의 독특한 생체 정보(지문, 목소리, 홍채 등 개인의 신체적·행동적 특징)를 패스워드로 활용하여 인증하는 방식이다.
  - 생체 인식과 공개키 암호화 방식은 네트워크를 보안할 수 있는 좋은 방법이나, 두 기술의 장점을 통합한다면 좀 더 안전하고 신뢰성 있는 보안도 가능할 것이다.
  - 공개키 암호화 방식은 온라인에서 데이터 보안을 위해 사용할 수 있고, 키가 중요한 정보를 포함하지 않으므로 정보 누설의 위험이 없다는 장점이 있다.
- 전자 서명
  - 신원을 확인하기 어려운 사이버 공간에서 한쌍의 키(개인키+공개키)를 사용하여 자신을 증명하는 것이 전자 서명의 원리다.

04. 암호 보안 기술

- 전자 서명은 송신자가 작성한 전자 문서 자체를 암호화하는 것이 아니므로 제3자가 문서 내용을 열람하는 데는 아무런 지장이 없다.
- 다만, 전자 서명에는 작성자로 기재된 자가 전자문서를 작성했다는 사실과 작성 내용이 송수신 과정에서 위조 또는 변조되지 않았음을 증명하고, 작성자가 나중에 작성 사실을 부인할 수 없도록 하는 정보가 들어 있어야 한다.

[그림 9-51] 공인 인증서 사용 예(안전 결제)



[그림 9-52] 공인 인증서

05. 메일 보안 기술

PGP

- PGP(Pretty Good Privacy)는 인터넷을 이용하여 전송하는 이메일을 암호화하거나 복호화하여 제3자가 알아볼 수 없도록 만드는 보안 프로그램이다.
- 일반 편지봉투는 뜯어서 내용을 보거나 바꿀 수 있지만, 이 프로그램은 암호 알고리즘을 이용하여 이메일 내용을 암호화하기 때문에 특정키가 있어야만 내용을 확인할 수 있다.

PEM

- 인터넷 이메일 전송 프로토콜인 SMTP에는 메시지를 암호화하거나 메시지가 중간에 수정되는 것을 검증하는 보안 기능이 포함되지 않았다.
- 기존의 메시지 전송 시스템을 그대로 이용하여 전송하는 이메일의 보안을 강화한 것이 바로 인터넷 표준으로 제안된 PEM(Privacy Enhanced Mail)이다.
  - SMTP와 달리 이메일을 암호화하여 보내므로 전송 도중 데이터가 유출되면 내용을 알아보기 힘들다.
  - 인터넷 표준안이며 군사용 및 은행 시스템용으로 많이 사용한다.

05. 메일 보안 기술

PGP vs PEM

- PEM은 IETF에서 인터넷 드래프트로 채택되었다. 높은 보안성이 있지만, 구현이 복잡하여 널리 사용하지 않는다.
- 반면, PGP는 PEM에 비해 보안성은 조금 취약하나, 구현이 비교적 쉽고 키 인증 등 권한을 한곳에 집중시키지 않고 사용자 스스로가 가질 수 있어 현재 가장 많이 사용한다.

[표 9-4] PGP와 PEM 비교

구분	PGP	PEM
개발자	필 짐버맨	IETF
키 인증 방식	분산화된 키 인증	중앙집중화된 키 인증
특징	• 응용 프로그램 • 구현이 쉬움 • 익명의 메시지 허용 • PEM에 비해 낮은 보안성 • 현재 많이 사용	• 인터넷 표준안 • 구현이 어려움 • 익명의 메시지 허용하지 않음 • 높은 보안성(금융계, 군사용) • 현재 많이 사용하지 않음