Windows NT용 IBM eNetwork Firewall

# 사용자 안내서

*버전 3 릴리스 2.1.1*

GC31-8658-01

Windows NT용 IBM eNetwork Firewall

# 사용자 안내서

*버전 3 릴리스 2.1.1*

GC31-8658-01

주

이 책과 이 책에서 지원하는 제품을 사용하기 전에 129페이지의 『부록. 주의사항』을 읽으십니다.

**재판 (1998 6월)**

이 책은 Windows NT용 IBM eNetwork Firewall 버전 3 릴리스 2.1.1 (제품 번호 5765-C16)에 적용됩니다. GC31-8658-00 대신 이 책이 사용됩니다.

# 목차

# 이 책에 관하여

이 책에는 보안 네트워크 내부 또는 외부로 원하지 않거나 허가되지 않은 통신을 금지할 수 있도록 Windows NT** 시스템상의 IBM eNetwork Firewall을 구성하고 관리하는 방법에 대해 설명되어 있습니다.

이 책은 IBM Firewall을 설치, 관리 및 사용하는 네트워크 또는 시스템 보안 관리자를 위한 것입니다. 비록 클라이언트 프로그램으로 Firewall을 액세스하는 방법을 설명하고 있어도 이는 클라이언트 프로그램을 위한 사용자 안내서는 아닙니다. 텔넷 또는 FTP와 같은 클라이언트 프로그램을 사용하려면, TCP/IP 클라이언트 프로그램에 대한 사용자 안내서를 참조하십시오.

**이 책을 사용하기 전에 CDROM 케이스에 부착된 설치 지침을 사용하여 제품을 설치하십시오.**

구성 클라이언트를 시작하고 난 후, 온라인 도움말 정보는 구성 클라이언트 필드를 채우고 대화 상자 사이에서 이동하는 것을 도와줍니다.

## 사전 지식

IBM Firewall을 설치하기 전에 TCP/IP 주소지정, 마스크 및 네트워크 관리에 대한 사전 지식을 가지고 있는 것이 필요합니다. 네트워크 안밖으로 액세스를 제어하는 Firewall을 설정하고 구성해야 하기 때문에 네트워크의 연산 방법을 먼저 알아 두어야 합니다. 특히, IP 주소, 완전히 규정된 이름, 그리고 서브네트 마스크의 기본에 대해 이해해야 합니다.

netstat, arp, ifconfig, ping, nslookup, DNS, sendmail, routing 및 그 이상을 다루는 TCP/IP에 대한 우수한 책은 *TCP/IP Network Administration*입니다. 더 자세한 것은 *참고 문헌*을 보십시오.

TCP/IP 및 경로지정, 네트워크 하드웨어, DNS 및 sendmail의 개요가 나와 있는 UNIX 관리 수행을 위한 우수한 책은 *UNIX System Administration Handbook* 입니다. 자세한 내용은 참고 문헌을 참조하십시오.

## 이 릴리스에 포함된 기능

Windows NT용 IBM eNetwork Firewall에서는 풍부하고 다양한 기능을 제공하며, 모두 3가지의 Firewall 구조를 포함합니다.

1. 응용 프로그램 프록시
   - FTP
   - Gopher 및 WAIS를 포함한 HTTP
   - 텔넷
   - SafeMail

   HTTP, 텔넷 및 FTP는 사용자 확인 기능을 가집니다.

2. Socks 프로토콜을 통한 회선 레벨 게이트웨이, 인터넷 표준
3. 필터링—통신량의 허용 또는 거부를 결정짓는 광범위하고 강력한 기준 세트. 기준에는 TCP/IP 주소, 포트, 프로토콜, 방향, 어댑터(보안/비보안) 등이 포함됩니다.

   다수의 사전정의된 서비스는 설정을 신속하게 만듭니다.

## Socks 프로토콜 버전 5

SOCKS 프로토콜 버전 5는 그 간편성이나 융통성과 더불어 다음과 같은 장점을 제공합니다.

- 사용자 확인 및 암호화 방법의 쉬운 전개
- UDP 기반 프록시 회선을 가로지르기 위한 가상 프록시 회선을 작성하는 UDP 연결.
- 실시간 socks 성능 정보를 표시하는 Socks V5 감시자

## 네트워크 주소 변환

인터넷 사용이 폭발적으로 성장함에 따라 IP 주소의 부족은 중요한 문제로 대두되었습니다. 네트워크 주소 변환 (NAT)은 주소 재사용을 기초로 IP 주소 부족 문제 해결책을 제공합니다.

개인 또는 위법의 주소를 사용하는 네트워크가 NAT를 통해 인터넷의 호스트와 통신하여 더 많은 공간을 개인 네트워크에 효과적으로 제공할 수 있는 점이 NAT의 장점입니다.더군다나, NAT를 사용하면, 개인 네트워크에서 주소를 외부로부터 숨길 수 있으므로 보안 레벨을 하나 더 추가할 수 있습니다.

## 단순 관리

원격 시스템에서 관리할 수 있는 Java** 응용 프로그램을 사용하여, Firewall 구성을 쉽게 갱신할 수 있습니다. 그러면, 다른 관리자에게 Firewall으로의 액세스를 더 제어할 수 있는 다른 레벨의 권한이 지정될 수 있습니다. 이러한 이해하기 쉬운 단일 그래픽 사용자 인터페이스(GUI)가 NT Firewall과 AIX Firewall 모두를 관리하는 데 사용될 수 있습니다.

## NT 강화

Firewall이 설치되면, 비 TCP/IP 프로토콜을 사용할 수 없으며, 불필요한 시스템 서비스를 사용할 수 없고 비관리자 계정의 로컬 로그인을 사용할 수 없습니다.

## 강력한 사용자 확인

SecurID, SecureNet 키 등과 같이 일반적인 모든 토큰 기반의 사용자 확인 메카니즘에 대한 지원이 제공됩니다.

### 보고서 유틸리티

보고서 유틸리티를 사용하여 일단 데이터베이스 엔진으로 반출되면 시스템 로그에 대해 다시 SQL 조회를 실행할 수 있습니다.

### 경보, 모니터 및 기록

확장된 자세한 로깅에는 TCP/IP 주소, 사용자 ID, TOD, 파일명, 포트 번호 등과 함께 모든 Firewall 활동이 포함됩니다. 의심스러운 활동을 감시하고 임계값이 초과될 때 경보를 보내기 위해 로그 모니터가 포함되어 있습니다.

### 다중 네트워크 분리

Firewall에서 복수의 네트워크 인터페이스 카드(NIC)를 사용하여, 여러 개의 서브네트워크를 분리할 수 있습니다.

### 자국어 지원

자국어 지원은 영어, 일본어, 한국어, 프랑스어, 간체 중국어, 정체 중국어, 이탈리아어, 스페인어 및 브라질 포르투갈어에 대해 제공됩니다.

## IP 주소 입력

Firewall을 구성할 때 IP 주소를 입력해야 합니다. 형식에 4개의 8진수가 있는 점분리 십진수 IP 주소를 입력해야 합니다.

```
nnn.nnn.nnn.nnn
```

여기서 각 nnn은 범위 000–255 사이에 오는 3 숫자 세트입니다.

## IBM으로부터 서비스 호출 방법

IBM 지원 센터는 문제점 진단과 해결에 있어서 전화 지원을 제공합니다. 언제든지 IBM 지원 센터로 연락하실 수 있습니다. 여러분은 8시간내에 확인 전화를 받게 됩니다 (월요일–금요일, 8:00 a.m.–5:00 p.m., 해당 지역 고객 시간).

미국이나 또는 푸에르토리코 밖에 있을 때는 IBM 영업 대표부나 허가받은 IBM 공급자에게 문의하십시오.

# 제1장 IBM Firewall 소개

IBM eNetwork Firewall은 AIX 및 Windows NT**용 네트워크 보안 프로그램입니다. 본질적으로 Firewall은 하나 이상의 보안, 내부 개인 네트워크와 다른 (비보안) 네트워크 또는 인터넷 사이의 차단물에 해당합니다. Firewall의 목적은 보안 네트워크의 내부 또는 외부에서 원하지 않거나 권한이 없는 통신을 금지하기 위한 것입니다. Firewall에는 다음의 세 가지 작업이 있습니다.

- 인터넷 보안 규정을 강화합니다.
- 네트워크 데이터와 기타 자원을 손상하지 않고 사용자의 고유 네트워크 사용자가 외부 네트워크에서 허가된 자원을 사용할 수 있게 합니다.
- 허가되지 않은 사용자를 네트워크에 들어 오지 못하게 합니다.

## Firewall 개념

인터넷의 어떤 것들 사이의 연결성은 다수의 보안 위험을 초래할 수 있습니다. 사용자는 자신의 개인용 데이터를 보호하고, 개인용 네트워크 내의 시스템을 외부에서 악용하지 못하도록 이에 대한 액세스도 보호해야 합니다. 이러한 보호를 성취하기 위한 첫번째 단계는 개인용 네트워크가 인터넷에 연결되어 있는 지점의 수를 제한하는 것입니다. 개인용 네트워크가 단 하나의 게이트웨이에 의해 인터넷에 연결된 구성에서는 인터넷 내부 및 외부에 허용되는 통신량을 조절할 수 있습니다. 이 게이트웨이를 Firewall이라고 합니다.

Firewall이 작업하는 방법을 이해하려면, 다음 예제를 고려해 보십시오. 출입을 제한하고 들어 가는 사람을 통제하기 원하는 빌딩이 있다고 가정합시다. 빌딩에는 한 개의 로비가 있으며, 이는 유일한 입구가 됩니다. 이 로비에서는 빌딩을 들어 가는 사람을 환영하는 몇 명의 프런트, 이들을 감시하는 몇 명의 보안 요원, 이들의 행동을 녹화할 몇 개의 비디오 카메라 및 신원을 확인할 몇 개의 배지 리더가 있습니다.

이는 개인 빌딩으로 들어 오는 사람들을 통제하기 위한 좋은 방법입니다. 그러나 만일 허가 받지 않은 사람이 로비를 지나는 데 성공한다면, 이 사람의 행동으로부터 빌딩을 보호할 수 있는 방법은 없습니다. 그러나, 이 사람의 행동을 감독할 수 있다면, 의심이 가는 행동을 감지할 수 있게 될 것입니다.

Firewall 전략을 정의하는 경우에는 조직에 위험이 되는 모든 것을 방지하고 나머지는 허용하는 것으로 충분하다고 생각할 것입니다. 그러나 새로운 시스템 공격 방법 때문에 이런 공격을 막는 방법을 미리 예측하고 빌딩의 경우에는 보호막에 금이 갔다는 조짐을 모니터해야 합니다. 일반적으로, 침입으로부터 복구하는 것이 이를 원천 봉쇄하는 것보다 훨씬 더 피해를 입히고 더 많은 비용이 듭니다.

## IBM Firewall 툴

IBM Firewall은 다른 Firewall 구조를 구현하는 데 사용하는 툴 박스와 같은 것입니다. 일단, 구조 및 보안 전략을 선택하면, 필요한 IBM Firewall 툴을 선택합니다. IBM Firewall 구성 클라이언트는 사용자에게 친숙한 관리용 그래픽 사용자 인터페이스를 제공합니다. IBM Firewall은 관리 변경과 보안을 흐트러 놓을 시도와 같은 모든 중요한 이벤트의 포괄적인 기록을 제공합니다.

IBM Firewall이 실제로는 IP 게이트웨이이므로, 이것은 월드를 둘 이상의 네트워크 즉, 하나 이상의 비보안 네트워크와 하나 이상의 보안 네트워크로 나눕니다. 예를 들어, 비보안 네트워크는 인터넷입니다. 보안 네트워크는 일반적으로 조직 IP 네트워크입니다. IBM Firewall이 제공하는 일부 툴은 다음과 같습니다.

- Expert 필터
- 프록시 서버
- Socks 서버
- 도메인 이름 서비스(DNS) 및 SafeMail과 같은 특정 서비스

## Expert 필터

Expert 필더는 시각, IP 주소 및 서브네트와 같은 여러 기준에 따라 세션 레벨에서 패킷을 검사하는 툴입니다. 필터 규칙은 IP 게이트웨이와 함께 작동하여 시스템에서 별도의 IP 네트워크 또는 서브네트워크 각각에 두 개 이상의 네트워크 인터페이스를 갖추어야 합니다. 한 세트의 인터페이스는 비보안으로 선언되고, 기타 세트는 보안으로 선언됩니다. 필터는 2페이지의 그림 1에서와 같이 이들 두 세트의 인터페이스 사이에서 작동합니다.

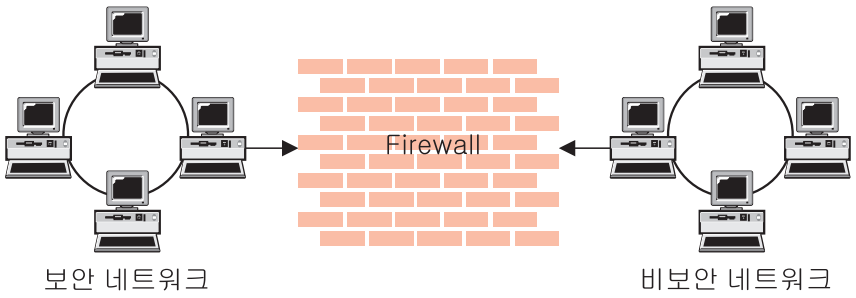


*그림 1. Expert 필터링이 있는 Firewall*

### Expert 필터의 목적

Expert 필터링은 Firewall에 대한 기본적인 보호 메카니즘을 제공합니다. 필터를 사용하여 IP 세션 세부사항에 따라 Firewall에 걸쳐 전달되는 통신량을 결정할 수 있으며, 그것에 의해 보안 서버 스캐닝 또는 IP 주소 속이기와 같

은 외부 처리로부터 보안 네트워크가 보호됩니다. 필터링 기능을 기타 툴이 구성되는 기본으로 생각하십시오.

## 프록시 서버

단지 통과된 패킷을 검사하는 필터링과는 달리, 프록시 서버는 Firewall의 일부인 응용 프로그램이며, 네트워크 사용자 대신에 특정 TCP/IP 기능을 수행합니다. 사용자는 TCP/IP 응용 프로그램(텔넷 또는 FTP) 중 하나를 사용하여 프록시 서버에 접촉합니다. 프록시 서버는 사용자를 대신하여 원격 호스트와 접촉하여 외부 사용자로부터 네트워크 구조를 감추면서 액세스를 제어하게 됩니다. 3페이지의 그림 2는 외부 사용자로부터의 요청을 가로채는 프록시 텔넷 서버를 보여줍니다.

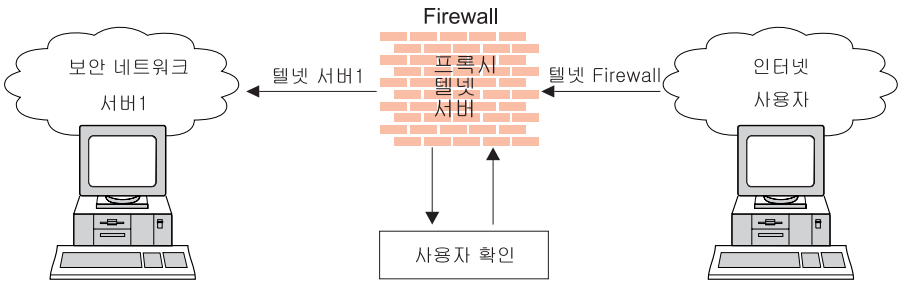


*그림 2. 프록시 서버를 갖춘 Firewall*

사용 가능한 프록시 서비스로는 텔넷, FTP, HTTP, WAIS, GOPHER 및 HTTPS, SafeMail이 있습니다.

IBM Firewall 프록시 서버는 다양한 사용자 확인 방법으로 사용자를 확인할 수 있습니다. 사용자는 자신의 내부 네트워크의 보안을 손상시키지 않고 인터넷의 유용한 정보를 액세스할 수 있습니다.

### 프록시 서버의 목적

프록시 서버를 통해 연결할 때 TCP/IP 연결은 Firewall에서 단절되므로 보안 네트워크를 손상시킬 가능성이 줄어듭니다. 사용자들에게는 많은 사용자 확인 방법 중 하나를 사용하여 스스로를 확인하도록 요구됩니다.

프록시 서버의 한 가지 주된 이점은 주소 감추기입니다. 모든 아웃바운드 프록시 연결은 Firewall 주소를 사용합니다. 프록시 서버의 또다른 주요 이점은 보안입니다. IBM 전문가들은 클라이언트 시스템에서 나타날 수 있는 보안 약점을 보완하기 위해 이러한 프록시 서버를 개발했습니다.

프록시 서버의 또다른 이점은 클라이언트 시스템에서 특정 버전의 클라이언트 프로그램을 사용해야 할 필요가 없다는 것입니다. 따라서, 일단 Firewall을 설치했으면, Firewall에 기록된 모든 사용자는 추가 소프트웨어를 설치하지 않고도 비보안 네트워크에 액세스할 수 있습니다.

## Socks 서버

Socks는 주소 숨김을 제공하지만 좀더 상용적인 프록시 서버에 드는 비용이 필요하지 않은 회선 레벨 게이트웨이에 대한 표준입니다.

Socks 서버는 세션이 Firewall에서 끊어진다는 점에서 프록시 서버와 유사합니다. 두 서버의 차이점은 SOCKS는 각 응용 프로그램에 대해 고유한 프록시를 요구하는 대신 모든 응용 프로그램을 지원할 수 있다는 것입니다. 가시적으로 Socks 클라이언트는 IBM Firewall 호스트에서 Windows NT Socks 서비스를 사용하여 세션을 시작한 후, 출발지 주소와 사용자 ID가 비보안 네트워크로의 전진 연결을 설정할 수 있는지에 대한 유효성을 검증한 다음, 두 번째 세션을 작성합니다. 4페이지의 그림 3은 Socks 서버를 갖춘 Firewall을 그림으로 설명합니다.

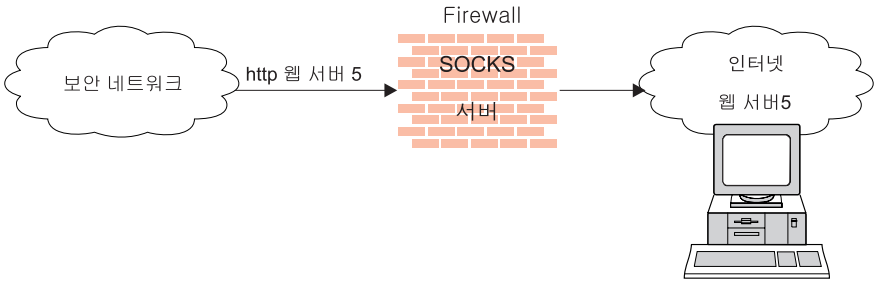


*그림 3. Socks 서버를 갖춘 Firewall*

Socksified 클라이언트 소프트웨어(Socks-준수 클라이언트라고 함)는 Netscape Navigator** 또는 Microsoft** Internet Explorer와 같은 많은 응용프로그램에서 사용할 수 있으며, Aventail** AutoSocks와 같은 TCP/IP 소프트웨어를 통해 사용할 수 있습니다.

### Socks 서버의 목적

아웃바운드 세션(보안 클라이언트에서 비보안 서버로)에 대해 Socks 서버는 프록시 서버와 같은 목적을 가집니다. 즉, 세션을 Firewall에서 차단시키고 사용자가 이를 통과하기 위해 자신의 신원을 증명해야 하는 보안 입구를 제공하는 것입니다. 이는 적은 양의 관리 추가 관리 작업으로 사용자가 간단히 작업할 수 있게 해줍니다.

## 도메인 이름 서비스

보안 네트워크에 대한 도메인 이름 레코드에 대한 액세스는 침입자에게는 대단한 도움이 됩니다. 왜냐하면, 공격할 수 있는 호스트의 리스트를 제공하기 때문입니다. 파괴된 도메인 이름 서비스는 침입자에게 액세스 경로를 제공해 줄 수도 있습니다. 외부 네트워크에서 Firewall에 있는 이름 서버는 자기 자신만 인식하고 내부 IP로 정보를 절대 제공하지 않습니다. 내

부 네트워크에서 이 이름 서버는 인터넷 네트워크를 인식하고 인터넷에서 모든 기계를 그 이름으로 액세스하는 데 매우 유용합니다.

### DNS 서버의 목적

Firewall에서 DNS 서버를 수행하는 것은 이름 분석 요청이 Firewall을 지나 흐르지 않도록 막고 보안 네트워크 호스트를 비보안 환경에서 숨기는 두 가지 장점이 있습니다.

## SafeMail

전자우편은 조직이 인터넷을 액세스하고 싶은 주요 이유가 됩니다. SafeMail은 내부 네트워크의 도메인 명을 숨기기 위해 고안된 IBM 전자우편 게이트웨이입니다. SafeMail 기능은 게이트웨이상에 전자우편을 저장하지 않으며, 루트 사용자 ID하에서 수행되지 않습니다. Firewall 게이트웨이 공용 도메인명은 전자우편이 사용자 주소 대신에 Firewall의 주소에서 나온다는 것을 나타내도록, 송신 전자우편의 개별 도메인명을 대신합니다. SafeMail에서는 Simple Mail Transfer Protocol(SMTP) 및 MIME(Multipurpose Internet Mail Extensions)를 지원합니다.

## 네트워크 보안 감사 프로그램 사용하기

네트워크 보안 감사 프로그램에서는 보안상의 헛점이나 구성 오류에 대해 네트워크를 스캔합니다. 네트워크 보안 감사 프로그램에서는 포트 열기 및 기타 노출과 같은 문제점이나 취약점에 대한 리스트를 보기 위해 서버와 Firewall을 스캔하고, 정정할 수 있도록 리스트를 컴파일합니다. 네트워크 보안 감사 프로그램은 심각한 호스트의 주기적인 스캐너나 1회용 정보 수집 툴로 사용될 수 있습니다. 네트워크 보안 감사 프로그램의 관리는 사용하기 쉬운 명령행 인터페이스를 통해 실행됩니다. 네트워크 보안 감사 프로그램으로, Firewall에서 경계를 유지합니다.

네트워크 보안 감사 프로그램의 기능은 다음과 같습니다.

- TCP 및 UDP 포트 스캐닝
- 비표준 포트에서 서버 인식
- 위험한 서비스, 알려진 취약점, 쓸모 없는 서버 버전 및 조정된 사이트 규정을 위반한 서버나 서비스 보고
- 쉽게 열람하기 위해 HTML로 보고서 작성

# 제2장 계획

IBM Firewall을 구성하기 전에 네트워클 구성을 이해하는 데 도움이 되는 체크리스트와 계획 워크시트를 사용하십시오.

## 계획 검사리스트

1. 목적을 정의하십시오. 다음을 실행하겠습니까 :
   - 인터넷(텔넷, 무명의 FTP등등)을 액세스하겠습니까 ? ?
   - 내부 네트워크의 부분을 구획 분할하겠습니까 ?
   - 네트워크에 대한 *외부* 액세스를 제공하겠습니까 ?
2. IP 서브네트워크 레벨에서 네트워크의 토폴로지를 평가하십시오.
   - 한 개의 보안과 한 개의 비보안 인터페이스가 올바른 구성입니까 ?
   - 주소가 규칙에 있는 서브네트 마스크를 지원할 수 있습니까 ?
3. DNS를 사용할 방법을 결정하십시오. 31페이지의 『제6장 도메인 이름 서비스 처리』를 참조하십시오.
4. safemail를 사용할 방법을 결정하십시오. 41페이지의 『제7장 SafeMail』을 참조하십시오.
5. SOCKS을 사용하려는 경우 넷스케이프 네비게이터나 Microsoft 브라우저와 같은 Socks-준수 클라이언트가 설치되어 있는지 확인하십시오. Socks 사용에 대한 정보에 대해서는 73페이지의 『제11장 Socks 서버 구성』을 참조하십시오.
6. 필요한 사용자 확인 유형
   - Security Dynamics** ACE/Server**를 사용하여 사용자를 확인할 것이라면, Firewall 호스트에 ACE/Server 클라이언트 코드를 설치하십시오. 보안 네트워크내의 다른 호스트에 ACE/Server 서버 코드를 설치하는 것이 바람직합니다.

     Security Dynamics ACE/Server 및 SecureID** 카드의 설치 및 사용에 대해서는 Security Dynamics Technologies 사에서 제공하는 정보를 참조하십시오.
   - AssureNet Pathways** SecureNetKey** 카드를 사용할 것이라면, IBM Firewall과 별도로 카드를 구매하십시오.
   - 여러분 고유의 사용자 확인 방법을 사용할 경우, *IBM eNetwork Firewall 참조서*에서 여러분 고유의 사용자 확인 방법 제공에 관한 장을 참조하십시오.
   - NETBIOS 대신에 TCP를 사용하려면, 사용자 확인용으로 위탁된 Windows NT 도메인을 탐색할 능력을 구현하는 Windows 클라이언트 코드를 구성해야 합니다. NETBIOS는 사용이 중단됩니다. 위탁된 Windows NT 서버에는 TCP/IP 호스트 이름 및 주소가 있어야 하며, 이들과 Firewall 사이에 TCP/IP 연결성이 있어야 합니다. Firewall 관리

자는 Firewall과 수탁된 NT 서버 사이에 통신이 허용될 수 있도록 이들 간의 연결을 작성해야 합니다.

다음 사전정의된 서비스를 사용하여 이 연결을 설정하십시오.

a. 도메인 제어기 사용자 확인 - 사용자 확인을 위한 도메인 제어기의 사용을 허용
b. NetBT 이름 서비스 브로드캐스트 - NetBIOS over TCP/IP 이름 서비스 브로드캐스트 허용

그런 후, NT 구성 유틸리티를 사용하여 위탁 관계를 정의하십시오.

7. 필터링을 사용할 때는 간단한 필터 규칙으로 시작해서 점점 더 제한적으로 만드십시오. 필요한 서비스에서 사용되는 포트와 프로토콜에 대해 친숙해 지십시오.
8. 로그 파일을 아카이브하는 방법을 결정하십시오. 아카이브는 Windows NT 스케줄러 서비스에서 스케줄된 작업을 위한 이상적인 후보입니다. 113페이지의 『제15장 로그 및 아카이브 파일 관리』를 참조하십시오.

## 네트워크 구성 계획 워크시트

IBM Firewall 구성에 대한 계획의 한 부분으로 다음 정보를 채우십시오.

Firewall의 호스트명

_____

보안 네트워크 인터페이스(내부 보안 네트워크에 연결)

IP 주소 _____ 서브네트 마스크 _____

IP 주소 _____ 서브네트 마스크 _____

IP 주소 _____ 서브네트 마스크 _____

IP 주소 _____ 서브네트 마스크 _____

비보안 네트워크 인터페이스(신뢰할 수 없는 비보안 네트워크에 연결)

IP 주소 _____ 서브네트 마스크 _____

IP 주소 _____ 서브넷 마스크 _____

IP 주소 _____ 서브넷 마스크 _____

IP 주소 _____ 서브넷 마스크 _____

라우터명 _____

라우터 주소 _____

보안 도메인명 _____

보안 도메인 이름 서버(DNS)의 IP 주소 _____

비보안 도메인 이름 서버(DNS)의 IP 주소 _____

보안 전자우편 서버 _____

공용 도메인 이름 _____

구성 클라이언트의 IP 주소 _____

원격 클라이언트의 IP 주소 _____

Windows NT Firewall의 루트 디렉토리 _____
(이 책자 전체에서 이를 ROOTDIR로 언급합니다)

c:\winnt (이 디렉토리에 Windows NT가 설치되어 있는 것으로 간주합니다).

# 제3장 구성 서버 및 구성 클라이언트 설정

이 장에서는 IBM Firewall을 위한 그래픽 사용자 인터페이스(GUI)인 구성 서버와 구성 클라이언트를 설정하는 방법에 대해 설명합니다.

## 구성 서버 설정

구성 서버는 Firewall에 대한 구성 클라이언트의 인터페이스입니다. 구성 서버는 구성 클라이언트가 보내는 요청을 처리합니다. 이 서버는 Firewall 시스템에서 수행되며 로컬 또는 원격 시스템에 위치하는 구성 클라이언트가 보내는 요청을 처리할 수 있습니다. 일단 이 서버를 설정했으면, 이를 Firewall 시스템의 일부로 간주하십시오.

구성 서버의 포트 번호는 Windows 운영 체제를 설치한 디렉토리에 들어 있는 NT 서비스 파일 `c:\winnt\system32\drivers\etc\services`에 지정됩니다. 디폴트 포트 번호는 1014이나 구성 서버 서비스를 중지하고 서비스 파일을 변경한 다음 구성 서버 서비스를 재시작하면 보안을 추가하기 위해 이 번호를 변경할 수 있습니다.

구성 서버는 처음에는 로컬 시스템의 구성 클라이언트가 보내는 요청을 수용할 수는 상태로만 설정됩니다. 초기 요청은 암호화되지 않습니다. 이러한 옵션을 변경하려면, 명령 행에서 `fwcfgsrv cmd=change`를 사용하십시오.

**localonly=**

Firewall이 로컬 시스템으로부터만 관리될 수 있는지 여부를 지정합니다.

**localonly=yes**

구성은 로컬 기계에서만 발생할 수 있습니다. 이는 디폴트입니다.

**localonly=no**

구성은 모든 기계에서 발생할 수 있습니다.

**encryption**

구성 서버에서 보안 Socket 층(ssl)을 통해 수신 데이터가 암호화될지 여부를 나타냅니다.

암호화 옵션이나 sslfile을 변경하면, 구성 서버 서비스를 중단한 후 다시 시작해야 합니다.

**encryption=none**

암호화가 일어나지 않습니다. 이는 디폴트입니다.

**encryption=ssl**

SSL 암호화가 발생합니다.

**sslfile=**

SSL 암호화에 사용될 SSL 키 파일의 이름을 나타냅니다. 디폴트는 `ROOTDIR\config\fwkey.kyr`입니다. *ROOTDIR*은 설치 프로세스 중에

IBM Firewall의 목표 위치로 선택한 디렉토리입니다. 키 파일 작성 방법에 대해서는 *IBM eNetwork Firewall 참조서*를 참조하십시오.

구성 클라이언트가 Firewall 시스템에 연결할 수 없고 다른 시스템 상에 있으면 `fwcfgsrv cmd=list`를 사용하여 `localonly=no`가 설정되어 있는지 확인하십시오. 또한 클라이언트와 서버에서 사용되는 언어가 일치해야 합니다. 마지막으로 서비스 패널을 화면에 표시하고 구성 서버 서비스 상태를 점검하여 구성 서버 서비스가 실행되고 있는지 확인하십시오. 이렇게 하려면, 제어판으로 가서 서비스 아이콘을 두 번 눌러 각 서비스의 상태를 점검하십시오. 이 서비스가 실행되고 있지 않으면 재시작해야 합니다.

## 구성 클라이언트 (GUI) 설정

IBM Firewall을 설치할 때 구성 클라이언트는 자동으로 설치됩니다. 구성 클라이언트는 또한 Firewall 없이 Windows NT 시스템에 따로 설치되어 여러분이 원격 관리를 수행할 수 있게 합니다. 구성 클라이언트를 시작하려면, IBM Firewall 프로그램 그룹에서 구성 클라이언트 아이콘을 두 번 누르십시오. 구성 클라이언트가 시작되면, 먼저 Windows NT 관리자 계정을 사용하여 Firewall에 로그온해야 합니다.

적절한 관리 사용자 확인을 거친 Windows NT 관리자와 Firewall 관리자만이 구성 클라이언트를 사용하여 Firewall으로 로그온할 수 있습니다.

Firewall이 설치된 후에는 모든 Windows NT 관리자가 1차 Firewall 관리자로 지정됩니다. 구성 클라이언트를 사용하여 1차 Firewall 관리자를 사용하는 구성 서버에 로그온한 후, 필요하면 추가 Firewall 관리자 사용자 이름을 정의하십시오. 구성 클라이언트를 사용하는 Firewall 관리자를 정의하는 방법에 대해 81페이지의 『제12장 Firewall에서 사용자 관리』를 참조하십시오.

더 빠르거나 느린 시스템에 대하여 로그온 시간종료 값을 설정하려면, IBM Firewall 구성 클라이언트 아이콘을 누른 후 **특성**을 눌러, 다음과 같이 변경하십시오. **바로 가기** 탭을 사용하여 특성을 변경하십시오. 매개변수 `timeout`을 *20*으로 변경하십시오. 여기서 20은 연결이 수행되기를 기다리는 시간(초 단위)을 나타냅니다. 더 빠른 기계는 10으로 설정될 수 있고 더 느린 기계는 디폴트 값을 채택해야 합니다.

JAVA 콘솔에서의 디버그 정보 수준을 증가시키려면, 구성 클라이언트 아이콘을 사용하는 대신 `ROOTDIR\cfgcli\gui`의 `ibmfw.bat`를 실행시키십시오. 그러나 콘솔 기록이 가능하면, 성능이 저하된다는 점에 유의하십시오.

### 구성 클라이언트로의 로그온

구성 클라이언트(로컬 또는 원격 시스템에 위치)로 로그온하려면 다음과 같이 하십시오.

- 사용자는 Firewall 관리자이어야 합니다

- Firewall 관리자에게는 사용자 확인 스킴이 정의되어 있어야 합니다. 86페이지의 『사용자 확인 방법』을 참조하십시오.
- 사용자는 특정 구성 기능을 수행하기 위한 권한을 가지고 있어야 합니다

### 구성 클라이언트를 통해 원격 구성 작동시키기

구성 클라이언트를 통해 원격 구성을 작동 가능하게 하려면, 로그온할 관리자는 반드시 다음과 같은 속성이 Firewall 기계에 정의되어 있어야 합니다.

- 만일 관리자가 네트워크의 보안쪽에 있고 Firewall 시스템에서 보안 인터페이스를 사용하고 있다면, 그는 보안 관리를 위해 적절한 사용자 확인 방법으로 정의되어야 합니다. (이것은 모두 거부로 설정될 수 없습니다). 이 사항은 로컬로 Firewall에 로그온할 경우에도 적용됩니다.
- 이와 비슷하게, 관리자가 비보안 쪽에 있고 Firewall 시스템의 비보안 인터페이스를 사용하는 경우에는 비보안 관리에 대해 적절한 사용자 확인 방법으로 정의되어야 합니다. (이것은 모두 거부로 설정될 수 없습니다).

모든 사용자 속성은 구성 클라이언트의 사용자 변경 대화 상자를 사용하거나 명령 fwuser를 사용하여 설정될 수 있습니다. 모든 Firewall 관리자에게는 Firewall 설치 후 위의 모든 필드가 적절히 설치된 상태로 제공됩니다. 더 자세히 알고 싶으면, 81페이지의 『제12장 Firewall에서 사용자 관리』를 참조하십시오.

## 원격 구성 서버를 위한 샘플 로깅 출력

다음은 원격 구성 서버를 위한 로깅 출력의 샘플입니다.

```
1998년 2월 3일 13:52:15 mr16n18: ICA9005i: 원격 구성 서버 시작중.

Feb 03 13:52:21 1998 mr16n18: ICA2024i: 보안 네트워크:127.0.0으로부터 NT를
사용하여
사용자 관리자가 성공적으로 확인되었습니다.
Feb 03 13:52:21 1998 mr16n18: ICA2169i: 보안 네트워크:127.0.0.1로부터 NT를
사용하여
원격 관리 서버에 대하여 사용자 관리자가 성공적으로 확인되었습니다.
```

# 제4장 구성 클라이언트 사용

그래픽 사용자 인터페이스인 구성 클라이언트를 사용해서 IBM Firewall을 구성하고 관리하십시오.

처음 IBM Firewall을 설치할 경우 로컬 시스템에서 구성 클라이언트로부터의 요청을 받아들이도록 설정됩니다. 그러나, 다른 기계에 구성 클라이언트를 설치하여 원격으로 Firewall을 관리할 수도 있습니다. 이에 대한 정보는 11페이지의 『구성 서버 설정』을 참조하십시오.

특정 지역(locale)의 언어로 시작할 구성 클라이언트를 설정하려면, IBM Firewall 구성 클라이언트 아이콘을 누른 후, **특성**을 누르십시오. **바로 가기** 탭을 사용하여 특성을 변경하십시오. 디폴트로, 호스트 시스템의 로케일이 사용됩니다. IBM Firewall은 다음과 같은 특정 지역 언어를 지원합니다.

- en_US - 미국 영어
- ja_JP - 일본어 PC
- ko_KR - 한국어
- zh_CN - 간체 중국어 EUC
- zh_TW - 정체 중국어 (Big 5)
- fr_FR - 불어
- it_IT - 이태리어
- pt_BR - 브라질 포루트갈어
- es_ES - 스페인어 PC

구성 클라리언트를 사용하기 위해서는 마우스가 필요합니다.

**도움말** 단추는 구성 클라이언트 주요 패널 상단 근처에 위치해 있습니다. 기능에 대한 정보를 보려면 **도움말**을 누르십시오.

## 구성 클라이언트로 로그온하는 방법

1. 로그온 유형에 대해 Firewall과 동일한 기계에 있으면, 로컬을 선택하십시오. 로컬은 디폴트입니다. 또 다른 Firewall을 원격으로 액세스하고자 하는 경우에는 원격을 선택하십시오. 원격의 경우 호스트명을 입력해야 합니다.
2. 만일 원격 로그온을 선택했다면, 로그온할 Firewall 기계의 호스트명 또는 IP 주소를 입력해야 합니다.
3. Firewall에 어떤 암호화가 사용되는지에 따라 SSL 또는 없음을 선택하십시오. 클라이언트에 대해 로컬에 대한 디폴트는 없음이고 원격에 대한 디폴트는 SSL입니다.
4. Firewall 관리자나 Windows NT 관리자의 사용자 이름을 입력하십시오.
5. 서버가 연결대기하고 있는 포트 번호를 입력하십시오. 디폴트는 1014입니다.

6. 모드의 경우, 로그온하고 있는 Windows NT Firewall 시스템을 구성하려면, 호스트를 선택하십시오. 호스트 관리로, 관리자는 한 번에 하나의 Firewall을 로컬로 또는 원격으로 갱신할 수 있습니다. AIX Firewall의 엔터프라이즈 Firewall 관리(EFM)에 대한 엔터프라이즈를 선택하십시오.
7. 로그온한 후에 사용자 확인 메세지를 보게 되며 암호 입력이 사용자명에 대해 설정된 사용자 확인 방법일 경우, 이를 입력하도록 프롬프트됩니다. 암호에 대한 프롬프트가 표시되면, 사용자 응답 필드에 암호를 입력한 후 Enter 키를 누르거나 승인을 누르십시오. 틀린 암호를 입력하면, 메세지가 표시됩니다. 닫기를 누르고 로그온 프로세스를 재시작하십시오. 암호를 입력하라는 메세지가 나타나지 않으면 사용자 확인 방법이 모두 허용일 수 있습니다. 이런 경우에 즉시 IBM Firewall 구성 클라이언트 패널을 얻게 됩니다.
8. 성공적으로 사용자를 확인한 경우에는 주 구성 패널이 표시됩니다.


*그림 4. 구성 클라이언트 로그온 패널*

## 네비게이션 트리

구성 클라이언트는 17페이지의 그림 5에서와 같이 왼쪽에 축소될 수 있는 트리 유형의 네비게이션 지원을 가지고 있습니다.

만일 이 트리 밑에 노드 또는 기능의 항목이 있으면, 파일 폴더 아이콘이 노드 왼쪽에 나타납니다. 서브기능을 보기 위해서는 아이콘을 두 번 눌러서 그 보기를 확장시킬 수 있습니다. 아이콘을 다시 두 번 누르면, 이 노드의 보기가 다시 원래의 보기로 접힙니다.

누른 모든 기능은 선택된 것으로 간주되고 강조표시됩니다. 오른쪽에 있는 창 보기를 변경하지 않고 노드를 확장시키거고 접을 수 있습니다. 확장된 트리가 사용 가능한 수직 공간을 초과하면, 스크롤 바가 네비게이션 트리 오른쪽에 나타납니다. 기능명 중에서 네비게이션 트리에 맞지 않는 것이 있으면, 수평 스크롤 바가 나타납니다.

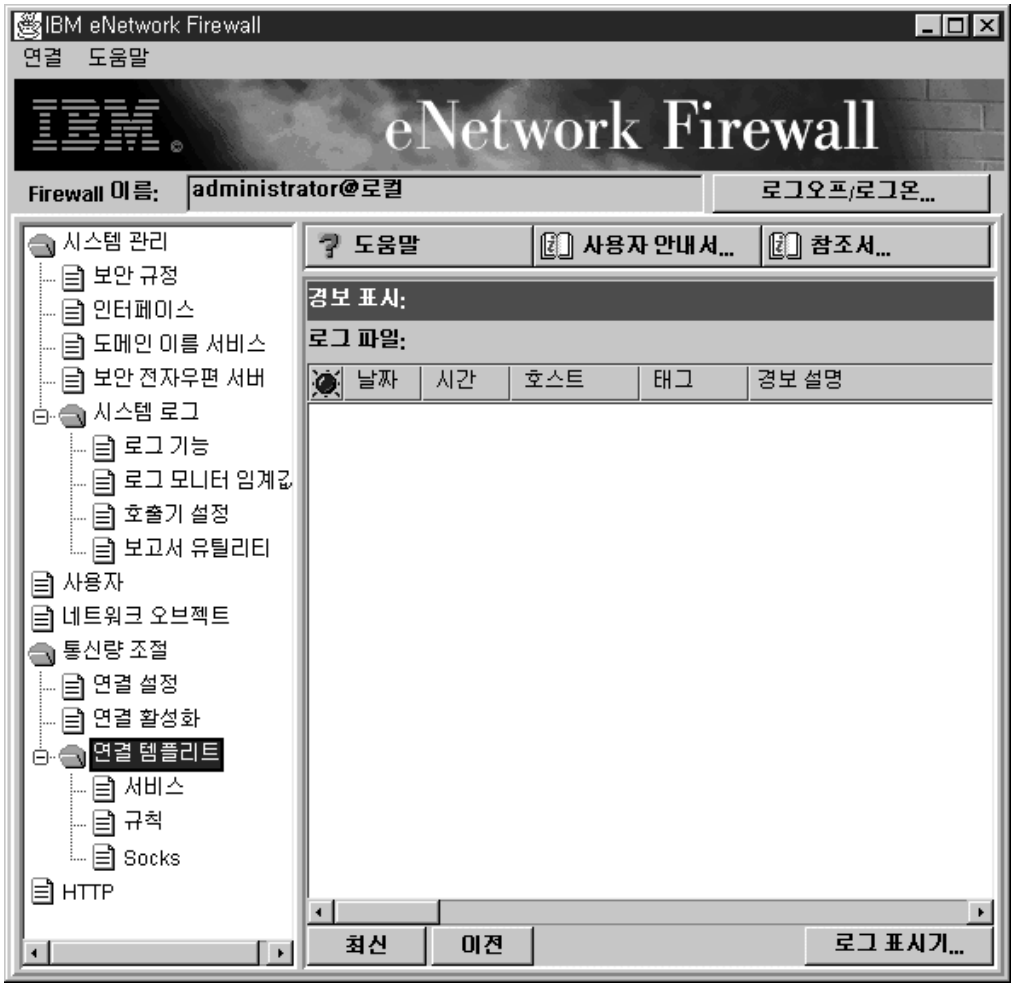


*그림 5. 구성 클라이언트 네비게이션 트리*

## 주요 패널상의 일반 피처

**경보 표시**위에 17페이지의 그림 5에서 보듯이 다음과 같은 세 개의 단추가 나타납니다.

**도움말**

**도움말** 단추는 구성 클라이언트 주요 패널 상단 근처에 위치해 있습니다. **도움말**을 눌러서 IBM Firewall을 가져와서 수행시키는 방법을 알아보십시오.

**사용자 안내서**

**사용자 안내** 단추는 구성 클라이언트 주요 패널 상단 근처에 위치해 있습니다. **사용자 안내**를 눌러서 이 소프트카피 출판물을 보십시오.

**참조** **참조** 단추는 구성 클라이언트 주요 패널 상단 근처에 위치해 있습니다. **참조**를 눌러서 이 소프트카피 출판물을 보십시오.

주 패널에 표시될 기타 버튼은 다음과 같습니다.

**최신** **최신** 단추는 구성 클라이언트 주요 패널 하단에 위치해 있습니다. **최신**을 눌러서 가장 최근의 경보를 보십시오.

**로그오프/로그온**

**로그오프/로그온** 단추는 구성 클라이언트의 상단 오른쪽 구석에 위치해 있습니다. 이는 재연결 단추입니다. 로그온 순서를 재시작해서 다른 Firewall로 연결하거나 또는 다른 관리자로 로그온할 수 있습니다.

로그오프하려면, 로그오프를 누르고, 로그온 패널 및 응용 프로그램에서 취소를 누르십시오.

**로그 표시기**

**로그 표시기** 단추는 구성 클라이언트의 하단 오른쪽 구석에 위치해 있습니다. 이것으로 Firewall 로그를 브라우즈할 수 있습니다.

**이전** **이전** 단추는 구성 클라이언트 주요 패널 하단에 위치해 있습니다. **이전**을 눌러서 이전 경보를 보십시오.

# 경보 표시

19페이지의 그림 6에서와 같이 주요 구성 클라이언트 창의 하단 오른쪽 섹션에서 시스템 로그 모니터에 의해 생성된 경보 레코드를 볼 수 있습니다.

표시된 경보는 ROOTDIR\config\syslog.conf에 정의된 첫번째 경보 로그 기능에 의해 식별되는 파일로부터 얻어집니다. 경보 로그 기능이 정의되지 않으면, 공백 화면이 표시됩니다. 경보 로그 기능을 정의하는 데 있어 도움말을 보려면, 114페이지의 『로그 기능 추가』를 참조하십시오.

패널은 경보 파일의 이름과 그 파일에서 현재 표시된 행 번호를 보여줍니다. **최신**을 눌러 가장 최신의 경보를 볼 수 있습니다. **이전**을 누르면, 이전 경보를 볼 수 있습니다.

표시된 각 행은 경보의 날짜와 시간, 경보가 발생한 Firewall의 호스트명, 경보 메세지 태그, 그리고 경보 메세지의 텍스트를 보여줍니다. 태그는 경보 유형을 나타냅니다.

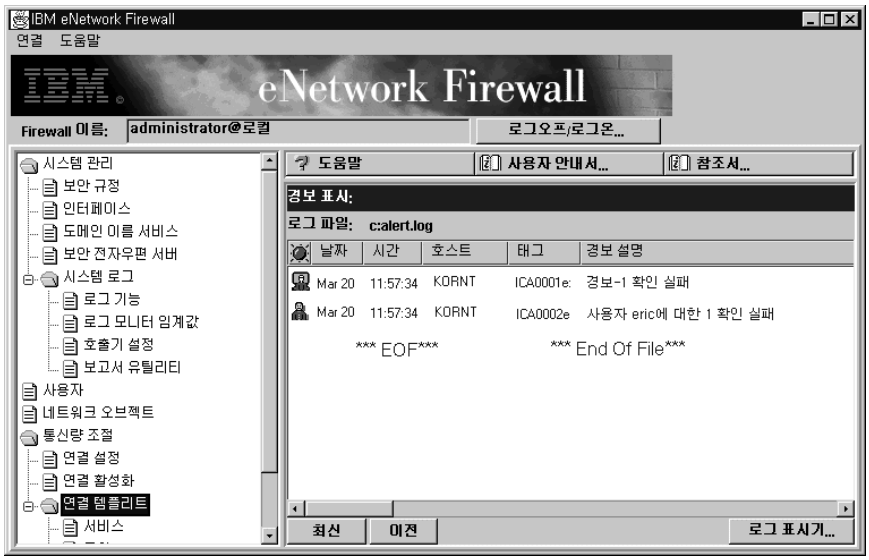


*그림 6. 경보 디스플레이*

## 로그 표시기

**로그 표시기**를 누르면, 20페이지의 그림 7에 표시된 대로 로그 표시기 창이 표시됩니다. 로그 표시기로 Firewall 로그 레코드를 볼 수 있습니다. 로그 파일과 레코드 계수(디폴트는 25)를 지정할 수 있습니다.

디폴트 로그는 ROOTDIR\config\syslog.conf에 정의된 첫번째 Firewall 로그 기능에 의해 식별되는 파일입니다. 파일명 필드의 풀-다운 메뉴에서 다른 목표 로그 파일을 선택하거나 또는 열람할 파일의 이름을 입력할 수 있습니다.

특정 시작 라인을 요청하려면, 그 옆의 필드에 라인 번호를 입력한 후 **시작할 라인:**을 누르십시오. 마지막의 여러 라인을 요청하려면, 파일의 맨 아래에 표시되어 있는 **아래쪽**을 누르십시오. **다음**은 파일의 다음 라인 세트로 진행합니다. **이전**은 파일의 이전 라인 세트로 되돌아갑니다. **위쪽**은 파일의 맨 위로 갑니다. **예**를 체크 표시하여, 선택적으로 Firewall 로그를 읽을 수 있는 텍스트로 확장할 수 있습니다.

로그 파일, 기능, 모니터 및 경보에 대해 더 알고 싶으면, 113페이지의 『구성 클라이언트를 사용한 로그 파일 작성 및 아카이브』 및 103페이지의 『제 14장 Firewall 로깅 모니터』를 참조하십시오.

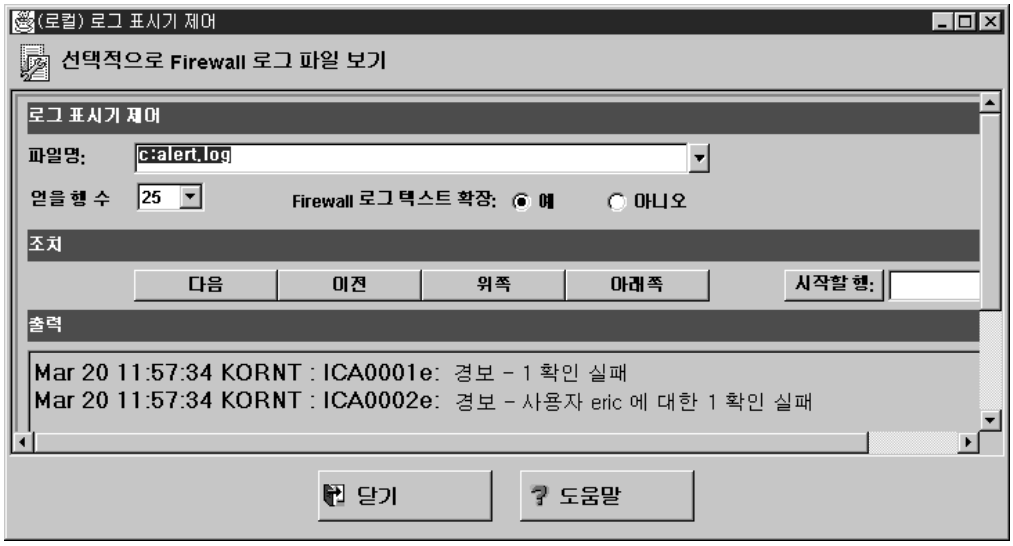


*그림 7. 로그 표시기*

## 기타 피처

찾기 필드는 일부 패널의 왼쪽 구석 근처에 위치해 있습니다. 찾기 스트링을 입력하고 **찾기**를 누를 수 있습니다.

다수의 구성 클라이언트 대화 상자에 표시될 다른 버튼은 다음과 같습니다.

**적용** **적용**을 눌러서 이전 패널의 필드에 현 선택을 입력하거나 또는 패널에서 변경한 내용을 저장하십시오. **적용** 단추로 창이 사라지지는 않습니다.

**단추** **단추**를 눌러서 패널 하단으로 가십시오.

**취소** **취소**를 눌러서 변경된 내용을 저장하지 않고 창을 닫으십시오.

**닫기** **닫기**를 눌러서 창을 디스플레이에서 삭제하십시오.

**복사** **복사** 단추는 새로운 항목을 리스트에 추가할 때 시간을 절약해 줍니다. 리스트에서 항목을 선택한 후 **복사**를 눌러서 선택된 항목과 비슷한 항목을 작성하십시오. 선택된 항목과 비슷한 항목을 작성하기 위해 **복사**를 누르면, 리스트의 선택된 항목에서 필드 값을 복사하는 새로운 항목이 열립니다. 그러면, 새로운 항목에 필요한 대로 필드 값을 변경할 수 있습니다.

**삭제** **삭제**를 눌러서 리스트에서 선택된 항목을 삭제하십시오.

**아래로 이동**
리스트에서 항목을 선택하고 **아래로 이동**을 눌러서 리스트에서의 항목의 상대적인 위치를 아래로 낮추십시오. 누를 때마다 항목이 한 위치 아래로 이동합니다.

**위로 이동**
리스트에서 항목을 선택하고 **위로 이동**을 눌러서 리스트에서의 항목의 상대적인 위치를 위로 올리십시오. 누를 때마다 항목이 한 위치 위로 이동합니다.

**확인** **확인**을 눌러서 변경 내용을 저장하고 창을 닫으십시오.

**열기** 리스트에서 항목을 선택한 후 **열기**를 눌러서 그 항목을 보거나 변경하십시오. 새로운 항목을 추가하려면, 리스트에서 **신규** 항목을 누른 후 **열기**를 누르십시오.

**최신 고침**
**최신 고침**을 눌러서 Firewall에서 데이터를 다시 액세스하고 패널에서 데이터를 다시 표시하십시오.

**삭제** **삭제**를 눌러서 선택된 항목을 리스트에서 삭제하십시오. 이 조치는 단지 리스트에서 항목을 삭제합니다. 이 조치는 항목이 정의되어 있는 다른 위치에 영향을 주지 않습니다.

**선택** **선택**을 눌러서 이 기능에 대해 유효한 후보 항목의 리스트를 액세스하십시오.

**위로** **위로**를 눌러서 패널 상단으로 가십시오.

## 공동 필드

다수의 구성 클라이언트 대화 상자에 표시될 공통 필드는 다음과 같습니다.

**출력** 시작한 명령이 진행함에 따라 진행 정보가 여기에 나타납니다.

**이름** 이 항목에 대한 이름을 제공하십시오. 이 항목명은 Firewall에서 이 특정 기능에 대해 고유해야 합니다. 이름에는 파이프 기호(|), 단일 따옴표(또는 어포스트로피) 문자('), 또는 이중 따옴표(″) 문자를 포함할 수 없습니다. 왜냐하면, 이는 SMIT와 파일 분리 문자로 사용되기 때문입니다. 이런 문자를 사용하면 신뢰할 수 없는 데이터를 초래할 수 있습니다.

**설명** 이 필드는 선택적이며 이 항목에 대한 주석이나 또는 추가 정보를 제공하고 싶을 때 사용 가능합니다.

## 고유 특징

구성 클라이언트의 여러 가지 고유 특징 중에서 알고 있어야 할 것이 몇 가지 있습니다.

Windows 95 또는 Windows NT 구성 클라이언트의 경우, 최소 1024 픽셀 x 768 픽셀의 해상도에서 구성 클라이언트가 가장 훌륭히 보입니다.

만일 스핀 제어를 통해 진행하기 위해 왼쪽 마우스 단추를 누르고 마우스 단추를 해제하지 않은 상태에서 마우스를 다른 위치로 잘못 끌면, 스핀 제

어가 계속됩니다. 이를 정지시키기 위해서는 왼쪽 마우스 단추로 스핀 제어 방향 화살표 중 하나를 누르십시오.

SSL을 사용하여 안속적으로 두 번 이상 빠르게 Firewall에 로그온하는 경우에는 연결이 거부됩니다. 구성 클라이언트를 종료하고 재시작하십시오.

# 제5장 IBM Firewall 시작

이 장에서는 IBM Firewall 설정에 필요한 기본 구성 단계를 제공합니다. 여기에서는 보안 인터페이스를 정의하는 방법, 보안 규정을 결정하는 방법 및 네트워크 오브젝트를 정의하는 방법에 대해 설명합니다.

## 기본 구성 단계

기본 IBM Firewall 설정:

1. IBM Firewall 설정을 계획하십시오. 먼저 사용하려는 Firewall의 기능과 원하는 사용 방법을 결정하십시오. 다음 섹션이 도움이 될 것입니다.
   - 1페이지의 『제1장 IBM Firewall 소개』
   - 7페이지의 『제2장 계획』
   - 55페이지의 『계획 고려사항』
2. 어느 인터페이스가 보안 네트워크에 연결되는지를 Firewall에 알리십시오. Firewall이 제대로 작동되기 위해서는 보안 인터페이스와 비보안 인터페이스가 있어야 합니다. 구성 클라이언트 네비게이션 트리에서 시스템 관리 폴더를 열고 **인터페이스**를 눌러 Firewall상에 있는 네트워크 인터페이스의 리스트를 보십시오. 인터페이스의 보안 상태를 변경하려면, 인터페이스를 선택하고 **변경**을 누르십시오. 더 자세히 알고 싶으면, 24페이지의 『네트워크 인터페이스 지정』을 참조하십시오.

   인터넷에 연결할 경우에는 ISP로 연락하여 등록된 Firewall 비보안 인터페이스 IP 주소를 받으십시오.
3. 시스템 관리 폴더에서 **보안 규정** 대화 상자를 액세스하여 일반 보안 규정을 설정하십시오. 일반적인 Firewall 구성의 경우:
   - DNS 조회의 승인
   - 비보안 인터페이스에 대한 브로드캐스트 메세지 거부
   - 비보안 어댑터에 대한 Socks 거부

   더 자세히 알고 싶으면, 25페이지의 『보안 규정을 정의하기 위해 구성 클라이언트 사용』을 참조하십시오.
4. 도메인 이름 서비스와 전자우편 서비스를 설정하십시오. 구성 네비게이션 트리의 시스템 관리 폴더에서 이러한 기능에 액세스하십시오. 먼저, 31페이지의 『제6장 도메인 이름 서비스 처리』를 참조하십시오.
5. 구성 클라이언트 네비게이션 트리의 **네트워크 오브젝트** 기능을 사용하여 Firewall에 대한 네트워크의 주요 요소를 정의하십시오. 네트워크 오브젝트는 Firewall을 통한 통신을 제어합니다. 다음 중요 요소를 네트워크 오브젝트로 정의하십시오.
   - Firewall의 보안 인터페이스
   - Firewall의 비보안 인터페이스

- 보안 네트워크
- 보안 네트워크상의 각 서브네트.
- 해당되는 경우, SDI 서버 및 NT 도메인 서버에 대한 호스트 네트워크 오브젝트.

더 자세히 알고 싶으면, 27페이지의 『네트워크 오브젝트』를 참조하십시오.

6. Firewall에서 서비스를 작동 가능하게 하십시오. 이는 보안 네트워크의 사용자가 비보안 네트워크(Socks 또는 프록시와 같은)를 액세스할 수 있는 방법입니다. 구현되는 서비스는 계획 단계에서 내린 결정에 따라 달라집니다. 서비스를 구현할 때 특정 유형의 통신을 허용하도록 일부 연결 구성을 설정해야 하는 경우가 있습니다. 예를 들어, 보안 사용자가 HTTP 프록시를 사용해서 인터넷의 웹에서 자유롭게 이동하게 하려면, Firewall의 HTTP 프록시 디먼을 구성하는 것뿐만 아니라 HTTP 통신량을 허용하기 위해 연결도 설정해야 합니다. 특정 서비스를 지원하는 연결 설정 방법에 대해서는 55페이지의 『제9장 서비스 예제』를 참조하십시오.
7. Firewall 사용자를 설정하십시오. 아웃바운드 웹 액세스와 같은 기능이나 Firewall 관리자에게 사용자 확인이 필요할 경우, Firewall에 이들 사용자를 정의해야 합니다. 더 자세히 알고 싶으면, 81페이지의 『제12장 Firewall에서 사용자 관리』를 참조하십시오.
8. 사용자 확인에 Windows NT 도메인 암호를 사용하려면, 사용자 확인을 위해 위탁된 Windows NT 도메인을 탐색하고 NETBIOS 대신에 TCP를 사용할 능력을 구현하는 Windows 클라이언트 코드를 구성해야 합니다. NETBIOS는 사용이 중단됩니다. 위탁된 Windows NT 서버에는 TCP/IP 호스트 이름 및 주소가 있어야 하며, 이들과 Firewall 사이에 TCP/IP 연결성이 있어야 합니다. Firewall 관리자는 Firewall과 위탁된 Windows NT 서버간의 소통이 허용될 수 있도록 이들간의 연결을 작성해야 합니다.
9. 네트워크 주소 변환을 사용할 경우에는 먼저 ISP로 연락하여 여러 주소를 하나의 주소로 변환할 때 사용할 등록된 인터넷 주소를 받으십시오. 그런 후 *NAT 구성 추가* 패널로 가서 *다-대-일 IP Address* 필드의 등록된 인터넷 주소를 추가하십시오. 자세한 내용은 121페이지의 『제16장 네트워크 주소 변환하기』를 참조하십시오.

이러한 단계를 수행하는 것은 기본 Firewall 구성을 설치하여 실행하는 데 도움이 됩니다. IBM Firewall은 네트워크의 보안을 보장해 주는 시스템 로그와 같은 기타 기능을 제공합니다. 더 자세히 알고 싶으면, 113페이지의 『제15장 로그 및 아카이브 파일 관리』를 참조하십시오.

## 네트워크 인터페이스 지정

이 책에서는 보안 및 비보안 인터페이스, 네트워크 및 호스트간을 구분합니다. 보안 인터페이스는 보호하려는 내부 네트워크에 있는 호스트의 네트워크로 IBM Firewall 호스트를 연결합니다. **Firewall이 작동되게 하려면 하나 이상의 보안 인터페이스가 있어야 합니다.** 비보안 인터페이스는 IBM Firewall

을 하나 이상의 외부 네트워크나 인터넷으로 연결합니다. IBM Firewall에는 하나 이상의 비보안 인터페이스가 있어야 합니다.

보안 인터페이스를 통해 접속된 모든 네트워크는 보안 네트워크로 간주됩니다. 보안 인터페이스에 접속되어 있는 다양한 서브네트 간을 구분하려면 Expert 필터 규칙을 사용하여 IP 주소나 주소 마스크를 기준으로 동일한 인터페이스 상에 있는 여러 서브네트 간의 액세스를 거부하거나 허용하십시오.

보안 및 비보안 인터페이스를 지정하려면 구성 클라이언트 네비게이션 트리의 시스템 관리 폴더를 사용하십시오. 알려진 모든 인터페이스(어댑터)가 표시되고 보안 또는 비보안으로 식별됩니다.

특정 인터페이스 필터링을 수행하기 전에 각 인터페이스에 대하여 이름을 제공해야 합니다.

보안 또는 비보안으로 네트워크 인터페이스를 확인하려면, 다음과 같이 하십시오.

1. 인터페이스를 선택하고 **변경**을 누르십시오.
2. 필요한 대로 반복하십시오.
3. **닫기**를 누르십시오.

인터페이스를 보안 또는 비보안으로 구분하고 그 인터페이스에 의미있는 이름을 부여하려면 **열기**를 누르십시오. 이 이름은 특정 인터페이스 필터링을 위한 필터에서 사용됩니다.

## 보안 규정을 정의하기 위해 구성 클라이언트 사용

IBM Firewall을 구성하는 것이 설치시 일반적인 보안 규정에 해당할 경우 고려해야 할 첫번째 사항.

IBM Firewall은 26페이지의 그림 8에서와 같이 보안 규정을 설정할 때 도움이 되는 대화 상자를 제공합니다.

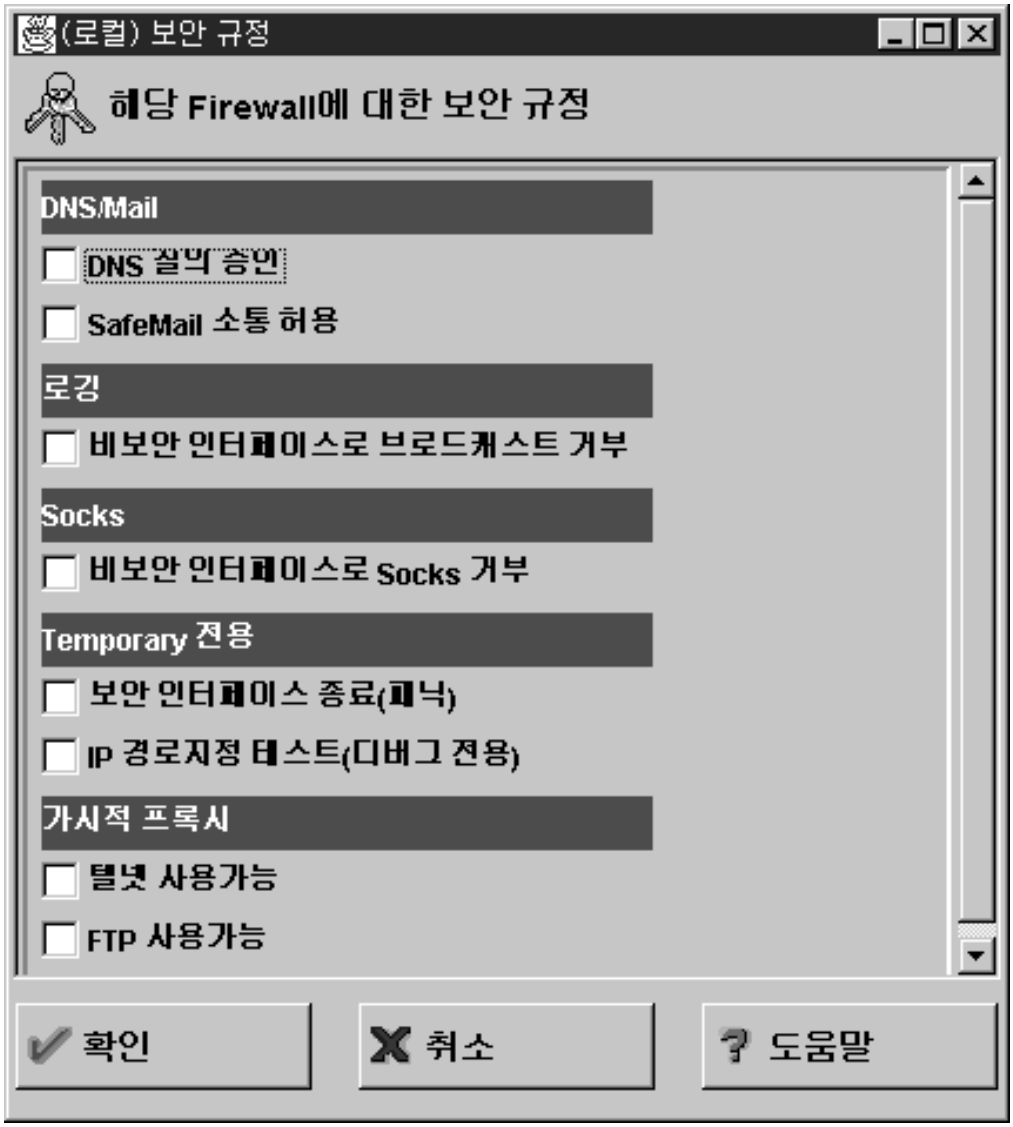


*그림 8. 보안 규정*

보안 규정 패널에 대해 좀더 학습하려면 도움말을 누르십시오.

보안 규정은 관리자가 Firewall에 대한 blanket 규정을 빠르고 쉽게 설정할 수 있는 방법을 제공합니다. 보안 규정 창에 표시된 대부분의 확인란은 Firewall에서 수신된 모든 네트워크 통신량에 적용될 특정 사전정의된 서비스를 선택할 수 있는 빠른 경로를 제공합니다. 예외는 단순히 가시적 텔넷과 가시적 FTP를 작동 가능 또는 불가능으로 만들기 위해 동작하는 가시적 프록시 선택입니다.

보안 규정을 선택하면, Firewall이 활성화되어야 하는 필터 규칙을 구축합니다. Firewall은 선택된 서비스를 작동 가능하게 하여 이들을 전역에서 사용할 수 있게 해 줍니다.

사전정의된 서비스에 관련된 확인란을 선택하고 **확인**을 누를 때마다 이런 변경사항을 연결 활성화 창을 통해 활성화시켜야 합니다. 가시적 프록시 선택은 사전정의된 서비스에 속하지 않기 때문에 활성화시킬 필요가 없습니다. 사전정의된 서비스의 리스트는 66페이지의 『사전정의된 서비스』를 참조하십시오.

사용자의 사이트에 대한 보안 규정을 반영하는 속성을 선택할 수 있는 다음과 같은 점검박스가 나타납니다. 선택된 속성은 IBM Firewall 양쪽에 있는 모든 주소에 적용됩니다.

- **DNS 조회의 승인**을 선택해서 도메인 이름 서비스 분석 요청과 응답을 허용하십시오.
- **SafeMail**을 선택하여 전자우편이 Firewall을 통과할 수 있도록 하십시오.
- **비보안 인터페이스로의 브로드케스트 거부**를 선택하여 비보안 포트에서 브로드캐스트 메세지가 수신되지 않게 하십시오. Firewall의 비보안 인터페이스가 인터넷에 연결되어 있으면, 이 서비스가 Firewall에서의 로깅양을 줄이는 데 도움을 줄 수 있습니다.
- **비보안 어댑터로의 Socks 거부**를 선택하여 비보안 네트워크로부터 Firewall로 Socks 통신량이 들어 가는 것을 막으십시오.
- **보안 인터페이스 종료(panic)**를 선택해서 보안 인터페이스를 지나 Firewall로 들어가고 나가는 모든 통신량을 막으십시오. 이는 비상용으로만 사용됩니다.
- **IP 경로지정 검사(디버그만)**를 선택해서 어떤 인터페이스를 거쳐서든 Firewall로 들어가고 나가는 모든 통신량을 허용하십시오. 이 확인란의 값을 변경하는 경우 **확인**을 눌러 값을 저장하고 연결 활성화 창을 통해 활성화해야 합니다. **이 서비스를 사용하면 Firewall에 대해 보안 노출이 유발될 수 있습니다. 아주 조심스럽게 이를 사용하십시오.**
- **텔넷 사용 가능**을 선택하여 가시적 프록시 텔넷을 허용하십시오.
- **FTP 사용 가능**을 선택하여 가시적 프록시 FTP를 허용하십시오.

## 네트워크 오브젝트

네트워크 오브젝트는 호스트, 네트워크, 라우터, 가상 개인 네트워크 또는 사용자와 같이 네트워크에 존재하는 구성요소들을 나타냅니다. 네트워크 오브젝트는 연결 작성시 서비스의 출발지 및 목적지 주소를 지정합니다.

오브젝트는 이름, 아이콘 표현, 유형, 그리고 설명으로 식별될 수 있습니다. 네트워크 오브젝트에는 여러 가지 유형이 있지만 호스트와 Firewall이 가장 일반적입니다. IBM Firewall과 함께 오는 디폴트 네트워크 오브젝트는 ″The World″ 입니다. 이는 모든 가능한 IP 주소를 포함하는 글로벌 오브젝트입니다. 네트워크 구성 워크시트를 다 채웠으면 (8페이지의 『네트워크 구성 계획 워크시트』 참조) 오브젝트 구축 준비가 완료된 것입니다.

단일 또는 그룹 오브젝트를 작성할 수 있습니다. 모든 네트워크 오브젝트가 하나의 IP 주소와 주소 마스크(서브네트 마스크)로 정의되므로 한 오브젝트가 광범위한 네트워크 주소를 나타낼 수 있습니다.

## 네트워크 오브젝트를 정의하기 위해 구성 클라이언트 사용

단일 네트워크 오브젝트를 정의하려면 구성 클라이언트 네비게이션 트리에서 **네트워크 오브젝트**를 선택하십시오. 네트워크 오브젝트 대화 상자가 나타납니다. **신규**를 두 번 누르십시오. 28페이지의 그림 9에서 보여주는 바와 같이 **네트워크 오브젝트 추가** 대화 상자가 나타납니다.

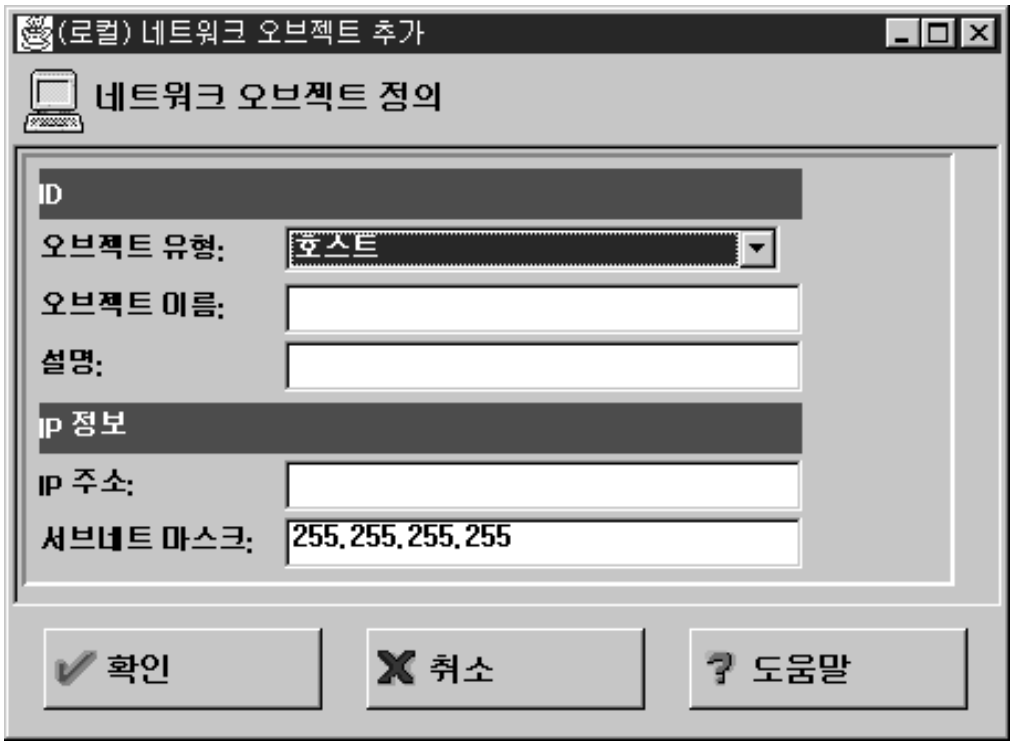


*그림 9. 네트워크 오브젝트 추가*

1. 오브젝트 유형을 입력하십시오. **오브젝트 유형** 화살표를 눌러 작성할 수 있는 오브젝트 유형을 보십시오. 성능상의 이유로 인해, 호스트 유형 오브젝트 대신에 네트워크 유형 오브젝트를 작성하는 것이 더 좋습니다. 작성할 수 있는 오브젝트 유형은 다음과 같습니다.
   - 호스트 - 255.255.255.255의 마스크를 가진 네트워크상의 특정 노드.
   - 네트워크 - 주소 범위와 특정 서브네트 마스크로 특징지어지는 네트워크 주소의 집합적 범위.
   - Firewall - Firewall이 설치되어 있는 255.255.255.255의 마스크를 가진 단일 시스템. Firewall 네트워크 오브젝트만이 IBM 또는 수동 터널의 목표가 될 수 있습니다.

- 라우터 - 둘 이상의 네트워크 사이에서 통신 경로를 지정하는 255.255.255.255의 마스크를 가진 호스트.
- 인터페이스 - 255.255.255.255의 마스크를 가진 시스템상의 네트워크 어댑터. 이는 Firewall에 있는 어댑터일 필요는 없습니다.

2. 오브젝트 이름을 채우십시오.
3. 설명을 채우십시오. 이 필드는 선택적입니다.
4. 이 오브젝트에 대한 점분리 - 십진수 IP 주소를 입력하십시오.
5. 주소에 있는 비트를 지정하는 서브네트 마스크를 입력해서 IP 패킷의 주소와 비교하십시오.
6. **확인**을 누르십시오.

## 네트워크 오브젝트 그룹

그룹은 네트워크 오브젝트의 집합을 나타냅니다. 그룹은 연결을 설정할 때 편리하도록 사용되며, 반복되는 작업을 없앨 수 있습니다. 예로는 각각이 네트워크 오브젝트로 표현되는 일부 주소를 하나의 부서를 나타내는 네트워크 오브젝트 그룹으로 그룹화하는 것이 있습니다. 이 부서는 연결에 대한 출발지 또는 목적지 주소로 사용될 수 있습니다.

네트워크 오브젝트의 그룹을 정의하려면, 구성 클라이언트 네비게이션 트리에서 네트워크 오브젝트를 선택하십시오. **네트워크 오브젝트** 대화 상자가 나타납니다. **신규 그룹**을 두 번 누르십시오. **네트워크 오브젝트 추가** 대화 상자가 나타납니다.

1. 그룹명을 채우십시오.
2. 설명을 채우십시오. 이 필드는 선택적입니다.
3. **선택**을 눌러 그룹에 대한 오브젝트를 선택하십시오.
4. **확인**을 누르십시오.

**힌트:** 가능할 때는 언제든지 인접 주소 범위를 단일 네트워크 오브젝트에 포함시키는 것이 바람직합니다. 이는 연결 규칙 처리의 성능을 향상시킵니다. 다음 예제는 이를 설명합니다.

```
ACCOUNTING DEPARTMENT
  Kevin's machine  191.1.10.1
  Susan's machine  191.1.10.3
  Helen's machine  191.1.10.5
  Peter's machine  191.1.10.7
  Bob's machine    191.1.10.9
```

이 ACCOUNTING DEPARTMENT에 대한 네트워크 오브젝트를 작성하려면, 이 그룹에 대한 IP 주소 정보를 서브네트 마스크 255.255.255.0의 191.1.10.0으로 입력하십시오. ACCOUNTING DEPARTMENT인 이 네트워크 오브젝트는 연결에 대한 출발지 또는 목적지로 사용될 수 있습니다.

## Firewall 구성 백업

Firewall은 구성 파일 모두를 ROOTDIR\config에 저장합니다. Firewall 파일을 보두 백업하지 않고 Firewall 구성만을 백업하고자 하는 경우, ROOTDIR\config 디렉토리의 내용 전체를 백업하십시오.

백업되어 있는 Firewall 구성을 복원하고자 하는 경우, ROOTDIR\config 디렉토리의 기존 파일을 모두 삭제하고, 파일들의 백업 버전을 복원하십시오. 복원된 구성이 효력을 발휘하려면, 필터 규칙을 재생성하고 활성화 시켜야 할 것입니다.

주요 Firewall 구성 파일은 다음과 같습니다. 여기에 나열된 파일들이 모두 Firewall 상의 \config 디렉토리에 들어 있지 않을 수도 있습니다. Firewall 구성 파일 대부분이 텍스트 편집기로 열람이 가능한 단순한 텍스트 파일이지만 **이들 파일을 직접 편집하는 것은 지원되지 않습니다.**

- carriers.cfg - 호출기 반송자 정의
- cfgfilt.output
- explode.cfg
- filters.active - 필터링이 활성화 되어 있는지를 나타냅니다.
- fwadpt.cfg - 네트워크 인터페이스에 대한 정의
- fwconfig.map - 구성 파일 이름을 가지고 있습니다.
- fwconns.cfg - 필터 연결 정의
- fwfilters.cfg - 현재 활성화 되어 있는 필터
- fwhttp.cfg - HTTP 프록시 구성
- fwmail.conf - SafMail 구성
- fwobjects.cfg - 네트워크 오브젝트 정의
- fwpolicy.cfg - 보안 규정 옵션
- fwrules.cfg - 필터 규칙 템플리트 정의
- fwservices.cfg - 서비스 정의
- fwsocks.cfg - 구성 클라이언트로부터의 Socks 5 규칙
- fwtdefn.conf - 경보 정의
- fwtpproxy.cfg - 가시적 프록시 정의
- fwusrdb.cfg - Firewall 사용자 데이타베이스
- logmgmt.cfg - 아카이브 정의
- modems.cfg - 모뎀 정의
- pager.cfg - 호출기 정의
- rcsfile.cfg - 구성 서비스 매개변수
- Socks5.conf - 생성된 Socks 5 구성 파일
- Socks5.header.cfg - 생성된 Socks5.conf에서 사용자가 제공하는 부분
- syslog.conf - 로그 기능 정의

# 제6장 도메인 이름 서비스 처리

이 장에서는 IBM Firewall과 관련해서 도메인 이름 서비스(DNS)를 구성하는 방법을 설명합니다. DNS의 목표는 보안 네트워크 밖에 있는 호스트에게는 어떠한 정보도 제공하지 않으면서 보안 네트워크 내에 있는 호스트에게는 완전한 도메인 이름 서비스를 제공하는 것입니다. 이렇게 하면 보안 네트워크 내에 있는 사용자들은 인터넷이 제공해야 하는 모든 서비스를 액세스할 수 있습니다. 그러나, 보안 네트워크에 대한 정보를 누설하지 못하게 함으로써 침입자가 공격할 컴퓨터의 위치를 찾는 것을 더 어렵게 합니다.

이를 이루기 위해서는 3개의 도메인 이름 서버가 필요합니다.

1. 하나는 IBM Firewall에서
2. 하나는 보안 네트워크 내에서
3. 하나는 보안 네트워크 밖에서

DNS가 IBM Firewall과 작업하는 방법에 대해서는 31페이지의 그림 10을 참조하십시오.

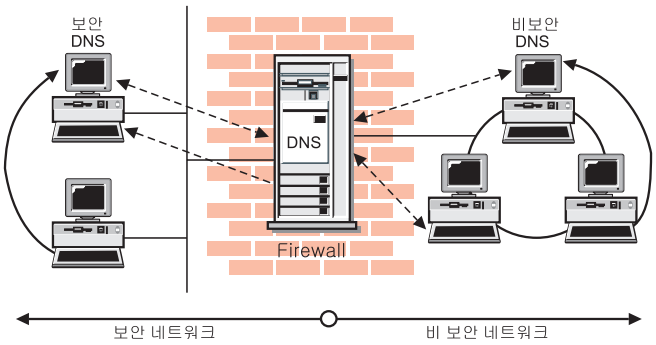


*그림 10. DNS*

Firewall은 보안 네트워크를 위한 이름 서버와 비보안 네트워크를 서비스하는 것들간의 게이트웨이로서 작용하도록 구성됩니다. Firewall의 역할에 대한 공식 용어는 *캐싱 전용 이름 서버*인데, 이는 Firewall의 DNS 자신은 어떠한 데이타베이스도 포함하지 않기 때문입니다.

31페이지의 그림 10는 Firewall의 역할을 보여줍니다. Firewall은 자체 용도로 이름을 분석할 필요가 있을 때마다, 보안 측 이름 서버에게 묻습니다. 조회가 Firewall이 전달되면 언제든 다시 조회를 비보안 이름 서버에게 전달합니다.

보안 네트워크상의 클라이언트가 보안 측 정보에 대해 물으면, 응답하는 보안 측 DNS에게 요청을 보냅니다. 동일한 클라이언트가 비보안 측 정보에 대해 물으면, 동일한 보안 측 DNS에게 요청을 보냅니다. 조회가 비보안 정보에 대한 것이기 때문에, 보안 측 DNS가 응답할 수 없으며 따라서 Firewall

에 조회를 전달합니다. 비보안 DNS가 Firewall에 요청을 전달해야 하는 경우에는, 그 요청이 비보안 DNS 도메인에 전달될 것이고 따라서 어떠한 민감한 정보도 노출되지 않습니다.

## 구성 클라이언트를 사용해서 DNS 구성

DNS를 구성하려면 구성 클라이언트 네비게이션 트리에서 시스템 관리를 선택하십시오. 파일 폴더를 두 번 눌러서 보기를 확장하십시오. **도메인 이름 서비스**를 선택하십시오. IBM Firewall은 사용자가 변경할 수 있는 현재 DNS 구성을 표시합니다.

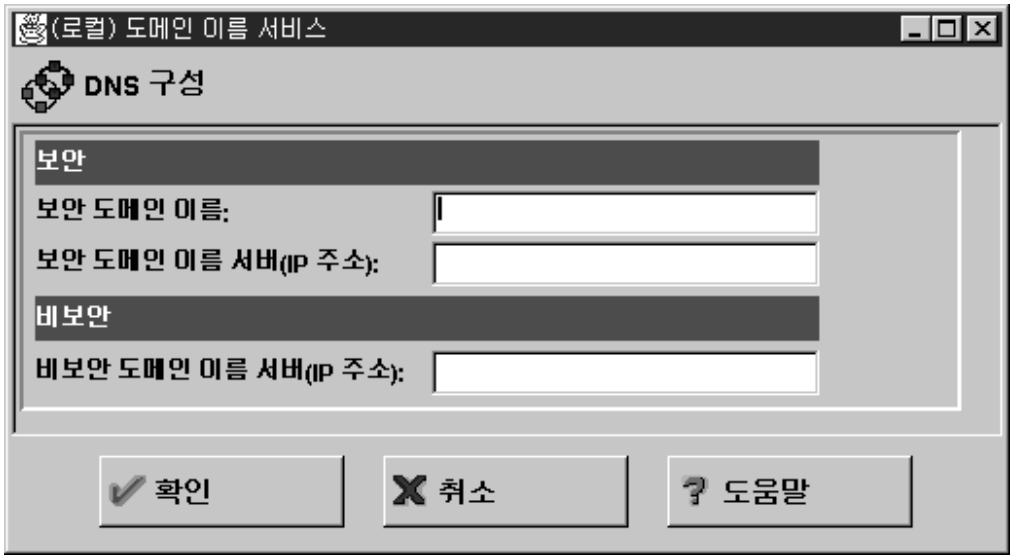


*그림 11. 도메인 이름 서비스*

**주:** DNS를 추가할 때 Firewall은 기존의 모든 도메인-이름 서비스 구성 파일을 저장하고 재명명합니다.

1. **보안 도메인 이름** 필드는 Firewall이 부적격 호스트 명에 첨부할 도메인 명을 식별합니다.
2. **보안 도메인 이름** 필드는 IBM Firewall에 의해 인터넷으로부터 보호되는 호스트에 대한 이름 및 IP 주소를 분석하는 서버를 참조합니다. 점분리 십진 IP 주소를 입력하십시오. 주소들 사이는 공백으로 구분하십시오.
3. **비보안 도메인 이름 서버** 필드는 여러분의 서비스 제공자가 제공하는 서버를 참조하여 비보안 네트워크에 대한 정보를 분석합니다. 점분리 십진 IP 주소를 입력하십시오. 주소들 사이는 공백으로 구분하십시오.

**주:** 이름 서버가 초기화할 때, 조회를 보내 루트 이름서버의 리스트를 확보합니다. 대부분의 구현에서 이 리스트를 메모리에 보유합니다. 그러나 Mircosoft의 구현에서는 이 리스트를 구성 파일에 다시 씁니다. 그렇다고 해서 이름 서버의 행동이 변경되는 것은 아니나, **비보안 이름 서버** 필드에 표시되는 값이 변경됩니다. 이는 걱정할 일이 아닙니다.

## 보안 이름 서버 구성하기

Firewall에 미분석된 조회를 전달하기 위해 보안 이름 서버가 구성되어야 합니다. 표준 BIND 구현인 경우에는, 다음과 같이 *forwarders* 명령문과 *cache* 명령문을 보안 이름 서버상의 *boot* 파일에 추가하십시오.

```
forwarders     aaa.bbb.ccc.ddd
cache          .               named.cache
```

Firewall을 지시하도록 캐쉬 파일, *named.cache*를 작성하십시오.

```
. 99999999 IN NS Firewall.private.com
firewall.private.com   99999999 IN A aaa.bbb.ccc.ddd
```

여기서 *private.com*은 보안측으로부터 사용된 도메인명이며 *aaa.bbb.ccc.ddd*는 Firewall의 IP 주소입니다.

이에 더하여, DNS 데이타베이스에 Firewall의 호스트명을 추가하고자 할 수도 있습니다. 이런 식으로 여러분의 사용자들이 IP 주소 대신에 Firewall의 호스트명을 사용하여 Firewall의 Socks 서버, HTTP 프록시, 텔넷 프록시 및 FTP 프록시를 액세스할 수 있습니다. 이를 위해 *DNS 및 BIND*의 *제 4장*에서 기술된 대로 2개의 추가 단계가 필요합니다. 책에 대해 더 상세한 것은 *참고 문헌*을 보십시오.

먼저 A 레코드를 도메인 데이타베이스 파일에 추가하십시오.

```
firewall.private.com     IN A aaa.bbb.ccc.ddd
```

그리고 나서 역 찾기 파일에 PTR 레코드를 추가하십시오.

```
ddd.ccc.bbb.aaa.in-addr.arpa.     IN PTR   firewall.private.com.
```

보안 네트워크를 위한 DNS를 사용하지 않는 경우, Firewall이 자기 자신의 정보를 여전히 분석할 수 있어야 합니다. 정상 경우에 대해 기술된 대로 Firewall을 구성하되, **보안 이름 서버** 필드에 Firewall의 보안 인터페이스를 나열하십시오. 그리고 나서 c:\winnt\system32\dns\boot에 다음 행을 추가하십시오.

```
primary ccc.bbb.aaa.in-addr.arpa c:\winnt\system32\dns\fwnamed.rev
```

그리고 나서 다음과 비슷하게 *fwnamed.rev*를 작성하십시오.

```
ccc.bbb.aaa.in-addr.arpa  IN SOA firewall.private.com. root.public.com. (
                          9        ; 직렬
                          86400    ; 1 일 이후 최신 고침
                          300      ; 5 분 이후 재시도
                          654000   ; 1 주 이후 만기
                          3600  )  ; 최소한 1 일의 TTL
ccc.bbb.aaa.in-addr.arpa.          IN NS    firewall.private.com.
ddd.ccc.bbb.aaa.in-addr.arpa.      IN PTR   firewall.private.com.
```

## 보안 클라이언트 구성하기

Firewall이 아니라 보안 이름 서버에 조회를 보내도록 보안 네트워크상의 클라이언트가 구성되어야 합니다. 이는 어떠한 보안 측 정보도 Firewall의 메모리내 캐쉬에 보관되지 않게하기 때문에 중요합니다. 또한, 조회가 보안 측으로부터 비보안 측으로 조회를 전달하는 일을 수반하지 않는한 Firewall이 연루되지 않기 때문에 Firewall의 워크로드를 절감시킵니다.

보안 네트워크를 위한 DNS를 사용하지 않는 경우, 클라이언트가 자신의 이름 서버로서 Firewall을 지시해야 할 것입니다.

## 공공에 서비스 발표하기

많은 조직들이 인터넷 대중에게 특정 서비스를 발표하기 원합니다. 비록 어떤 유형의 TCP/IP 서버든 사용될 수 있을 지라도, 이런 서비스들에는 종종 전자우편과 웹 서버가 포함됩니다. 그러한 서비스들을 사용 가능하게 하려면, 도달될 수 있는 네트워크상에 서버를 배치해야 할뿐만 아니라, 공용 DNS와 그 서버를 나열하여 사용자가 올바른 정보를 확보할 수 있게 해야 합니다.

이를 성취하는 데는 두 가지 방법이 있습니다. 서비스 제공자가 그들 도메인의 일부로서 (그러므로 이름 서버상에) 여러분의 서버를 나열하거나, 여러분이 자신의 이름 서버를 제공하고 이를 인터넷에 등록해야 합니다. 여러분의 인터넷 서비스 제공자(ISP)가 여러분을 위해 이 서비스를 제공하는 편이 훨씬 쉽습니다. 이 옵션을 고를 수 있다면, 여러분이 원하는 호스트명과 IP 주소를 제공할 필요가 있습니다. 예를 들어, 공용 웹 서버를 *www.public.com*으로 운용하고 그 IP 주소가 *50.100.150.200*이면, ISP에게 *50.100.150.200*로 *www.public.com*을 나열하도록 요구할 필요가 있습니다.

이에 더하여, 전자우편을 수신하기 바란다면 ISP에게 여러분의 Firewall을 여러분의 공용 e-mail 도메인을 위한 *Mail Exchanger*로 나열하도록 요구해야 합니다. ISP는 호스트명*(gateway.public.com)*, IP 주소*(50.100.150.201)* 그리고 여러분이 전자우편을 수신하고자 하는 도메인명*(public.com)*을 알 필요가 있습니다.

ISP가 여러분을 위해 이러한 서비스를 제공하려고 하지 않으면, 여러분 스스로 이를 행하여야 합니다. 여기서 다시 두 가지 추가 선택 사항이 있습니다. 여러분의 DNZ에 DNS를 배치하거나 혹은 여러분의 Firewall을 그 이름 서버로 사용할 수 있습니다. 그곳에 놓을 데이타베이스 파일이 여러분의 보안 네트워크에 대한 어떠한 정보도 포함하지 않기 때문에 Firewall의 사용이 추가 보안 위험을 유발하지 않습니다. 보관될 유일한 정보는 여러분이 제공하기로 선택하는 공용 서비스에 관한 것입니다.

DNS 서버 설정에 관련된 세부사항은 *참고 문헌*에 나열되어 있는 *DNS 및 BIND*의 제 4장에 들어 있습니다. 필요하다면 이전 장들과 마찬가지로 그 장을 반드시 읽어 볼 것을 권합니다. DNS 서버를 설정하는 일은 결코 사소

한 일이 아니며 때로는 전문가에게 맡기는 것이 최선입니다. 그러한 전문가가 있다면, 그 전문 기술의 활용을 진지하게 고려하십시오.

자세한 내용은 35페이지의 『구성 예제』를 참조하십시오.

## Microsoft의 DNS 서버 설치

Microsoft의 DNS 서버를 설치하려면, 제어판으로 가서 **네트워크**를 누르고, **서비스 탭**을 누르고, **추가**를 누른 다음 **Mircosoft DNS 서버**를 선택하십시오. 설치 CDROM이 필요합니다.

## DNS 문제 발견 및 수리

*IBM eNetwork Firewall 참조서*에는 Firewall 고장 발견 수리에 관한 장이 들어 있습니다. 그 장에 DNS 문제에 대한 섹션이 있습니다. 이 섹션은 *nslookup* 명령을 사용하여 DNS 시스템의 장애 세그먼트를 식별하는 데 대한 제안을 제공합니다.

## 구성 예제

이 절에서는 Firewall이 사용되는 구성 예제를 보여드립니다. 이들 예제 대부분은 DNS 조작에 필요한 구성에 주로 촛점을 맞추었습니다@232E 이 예제들이 여러분의 네트워크를 반영한 것이 아니므로, 각 예제를 잘 이해하고 적절한 개념을 여러분의 특정 설치에 적용하십시오.

### 예 1: 비보안 인터페이스 상에서 DMZ의 DNS 서버

첫번째 예에서는 35페이지의 그림 12에서와 같이, 비보안 네트워크 내에 위치한 DMZ의 이름 서버를 조작하는데 필요한 파일들을 보여줍니다.

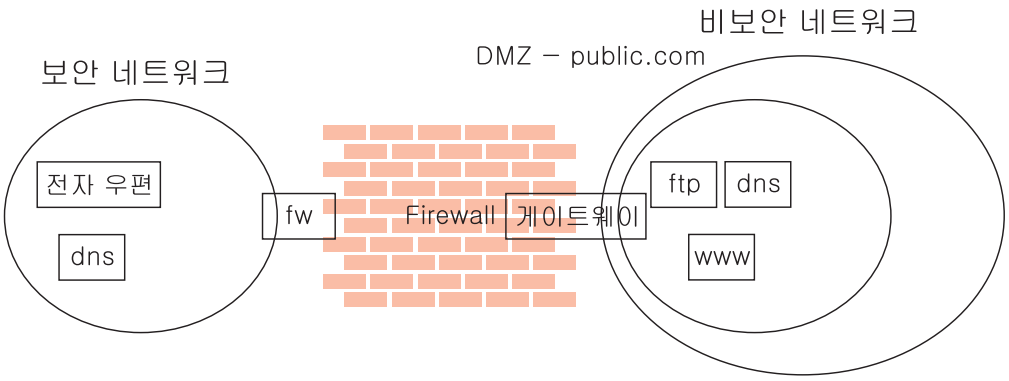


*그림 12. 비보안 네트워크 내 DMZ의 이름 서버*

이 그림은, 보안 인터페이스가 *fw.private.com*이고 비보안 인터페이스가 *gateway.public.com*인 개별 네트워크 *private.com*을 보여줍니다. 회사의 DMZ는 비보안 인터페이스에 접속되어 있으며, 이름 서버 *dns.public.com*, FTP 서버 *ftp.public.com* 및 웹 서버 *www.public.com*을 가지고 있습니다. 이 시나리오를 구현하기 위한 *dns.public.com* 상의 파일들은 다음과 같습니다.

**db.public**

```
public.com.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; 일련 번호
                  10800       ; 3시간 후 최신 고침
                  3600        ; 1시간 후 재시도
                  604800      ; 1주일 이후 만기
                  86400 )     ; 최소한 1일의 TTL
;
; 이름 서버
;
public.com           IN NS  dns.public.com.
;
; DMZ의 호스트
;
dns.public.com.      IN A 50.100.150.202
gateway.public.com.  IN A 50.100.150.201
www.public.com.      IN A 50.100.150.200
ftp.public.com.      IN A 50.100.150.203
;
; 우편 관련 항목
;
public.com.          IN MX  0  gateway.public.com.
public.com.          IN CNAME gateway.public.com.
```

**db.50.100.150**

```
150.100.50.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; 일련 번호
                  10800       ; 3시간 후 최신 고침
                  3600        ; 1주일 후 재시도
                  604800      ; 1주일 이후 만기
                  86400 )     ; 최소한 1일의 TTL
202.150.100.50.in-addr.arpa.      IN NS dns.public.com.
]203.150.100.50.in-addr.arpa.      IN PTR  ftp.public.com.
202.150.100.50.in-addr.arpa.      IN PTR  dns.public.com.
201.150.100.50.in-addr.arpa.      IN PTR  gateway.public.com.
200.150.100.50.in-addr.arpa.      IN PTR  www.public.com.
```

**db.127.0.0**

```
0.0.127.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; 일련 번호
                  10800       ; 3시간 후 최신 고침
                  3600        ; 1주일 후 재시도
                  604800      ; 1주일 이후 만기
                  86400 )     ; 최소한 1일의 TTL
0.0.127.in-addr.arpa.   IN NS  dns.public.com.
1.0.0.127.in-addr.arpa.   IN PTR localhost.
```

**db.cache**

이 파일에 대한 최선의 선택은 *ftp://ftp.rs.internic.net/domain/named.root*의 현재의 루트 이름 서버 리스트로 FTP 하는 것입니다.

**부트**

```
primary public.com                  db.public
primary 150.100.50.in-addr.arpa     db.50.100.150
primary 0.0.127.in-addr.arpa        db.127.0.0
cache   .                           db.cache
```

통신량 필터를 설정하여 적절한 DNS 통신량을 허용하려면, **보안 규정** 패널에서 *DNS 질의 승인*을 사용 가능하도록 하십시오.

## 예 2: DMZ 전용 인터페이스의 DNS

두 번째 예에서 DMZ에 대한 DNS가 전용 이름 서버에 있지만, 이번에는 DMZ가 비보안 네트워크와 같은 인터페이스가 아닌 다른 인터페이스에 접속되어 있습니다.

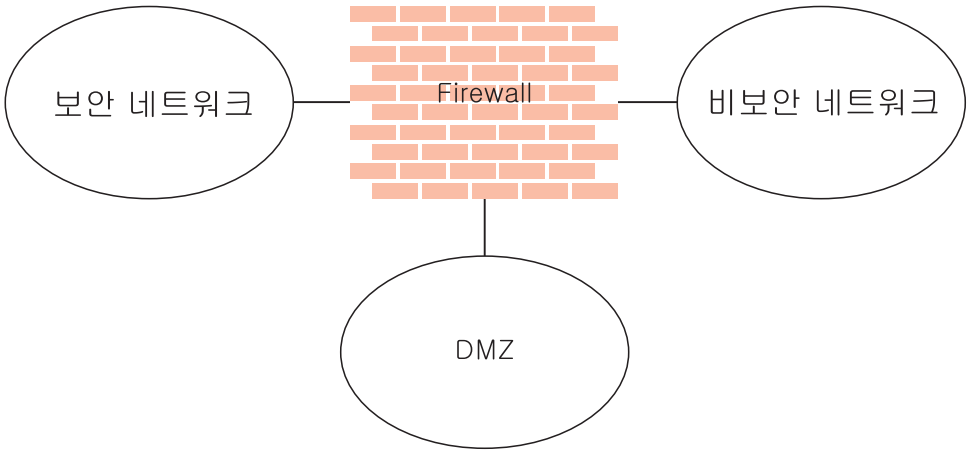


*그림 13. 전용 인터페이스 상의 DMZ의 DNS*

*dns.public.com* 상의 DNS 데이터 파일은 앞의 예에서와 같습니다. 그러나 이 이름 서버가 공용 네트워크에 액세스 할 수 있도록 하려면, 데이터 파일을 Firewall로 복사하기 위해 통신량 필터를 열거나 지역 전송을 수행할 필요가 있습니다.

통신량 필터를 열려면 *DNS 서버 조회*, *DNS응답*, 및 *DNS 클라이언트 조회*라고 하는 세 가지 규칙 템플리트를 복사하십시오. 각 규칙의 경로지정 설정을 *로컬*에서 *경로지정됨*으로 변경하십시오. 그리고나서 세 개의 신규 규칙 템플리트를 서비스에 포함시키고, 흐름 표시자를 다음과 같이 설정하십시오.

- DNS 클라이언트 조회: --->
- DNS 응답: <---
- DNS 서버 조회: --->

• DNS 서버 조회: <---

이 서비스를 소스 오브젝트로 *The World*를 사용하고, 목적지 오브젝트로 *dns.public.com*을 사용하는 연결에 포함시키십시오.

지역 전송을 수행하려면 통신량 필터를 설정하고 이름 서버에게 적절한 파일을 복사하도록 지시해야 합니다. 통신량 필터를 설정하려면 다음과 같이 하십시오.

1. **보안 규정** 패널에서 *DNS 조회의 승인*을 사용 가능으로 설정 하십시오.
2. *dns.public.com*(소스 오브젝트)으로부터 Firewall의 DMZ 인터페이스(목적지 오브젝트)로 연결을 추가하는데, 여기에는 *DNS 전송*이라는 서비스가 포함됩니다.

지역 전송을 활성화하려면, c:\winnt\system32\dns의 Firewall 부트 파일에 다음 행을 추가하십시오.

```
secondary public.com     50.100.150.202 db.public
secondary 150.100.50.in-addr.arpa  50.100.150.202 db.50.100.150
```

그리고 나서 서비스 제어 관리자로 가서, DNS 서버 서비스를 중단한 후 다시 시작하십시오.

## 예 3: 보안 이름 서버로 Firewall 사용

보안 이름 서버로 Firewall을 사용하려면, 보통 보안 서버에 들어 있는 데이타베이스 파일들을 Firewall로 옮기십시오. 그러면 클라이언트가 DNS 서버로 Firewall을 지정할 수 있습니다. 이 방식에 있어서의 위험은 DNS 서버가 보안 쪽에서 오는 요구와 비보안 쪽에서 오는 요구를 구분할 수 없다는 점입니다. 따라서 DNS 서버는 보안 쪽의 정보를 요구하는 클라이언트라면 누구에게나 이 정보를 제공할 것이며, 더 이상 보안 DNS 정보 은닉이 불가능합니다.

이 방식을 구현하려면, 구성 클라이언트를 사용하여 Firewall DNS 기능을 구성하는 것으로 시작하십시오. *보안 도메인명* 필드에 대해서는, 보안 네트워크에서 사용하게 될 도메인명을 나열하십시오. *보안 이름 서버*에서는 Firewall의 보안 인터페이스를 나열하십시오. *비보안 이름 서버*에서는 ISP에 의해 제공되는 이름 서버를 나열하십시오. 그리고나서 이 구성을 보완하기 위해 Firewall 상에서 역탐색 파일을 작성해야 합니다.

다음의 예와 유사한 c:\winnt\system32\dns\fwnamed.rev 파일을 작성하십시오.

이 예에서 Firewall의 보안 인터페이는 *fw.private.com*이고 IP 주소는 *10.100.100.1*입니다.

```
100.100.10.in-addr.arpa.   IN SOA fw.private.com. admin.fw.private.com. (
                  1          ; 일련 번호
                  10800      ; 3시간 후 최신 고침
                  3600       ; 1주일 후 재시도
                  604800     ; 1주일 이후 만기
```

```
                    86400 )     ; 최소한 1일의 TTL
1.100.100.10.in-addr.arpa.          IN NS fw.private.com.
1.100.100.10.in-addr.arpa.          IN A  fw.private.com.
```

그리고나서 c:\winnt\system32\dns\boot에 다음 행을 추가하십시오.

```
primary 100.100.10.in-addr.arpa     fwnamed.rev
```

이 시나리오에서 클라이언트는 DNS 서버로 Firewall을 지정하도록 구성되어야 합니다. Firewall은 외부 정보 분석의 도움을 받는데, 보안 쪽 정보의 분석은 없을 것입니다. 이는 Firewall 상의 구성 서버나 프록시 서버에 연결하고자 하는 보안 쪽 클라이언트는 호스트명이 아닌 IP 주소로 Firewall을 참조해야 한다는 의미입니다.

# 제7장 SafeMail

IBM Firewall SafeMail 게이트웨이는 SMTP 소통을 위한 게이트웨이를 제공합니다. 민감한 도메인 명을 숨기면서 보안 전자우편 서버로부터 비보안 측으로 메세지를 중계합니다. 비보안 측으로부터 보안 전자우편 도메인안으로 메세지를 중계하고 시스템공격으로부터 보안 네트워크를 차단합니다.

SafeMail이 비록 내용 검사를 수행하지 않을지라도, SafeMail은 내용 검사가 수행될 수 있는 사용자 exit을 제공합니다. 더 자세한 정보는 43페이지의 『SafeMail 사용자 나감(Exit)』을 참조하십시오.

SafeMail은 송신자로부터 수신자에게로 실시간으로 메세지를 중계합니다. 이는 Firewall상의 메세지 큐를 유지보수하는 데 수반된 위험 및 복잡성을 피하기 위한 것입니다. 이는 근접 전자우편 도메인상의 특정 구성 요건을 필요로 합니다. 일부 경우에는, 특정 설치에 대해 이러한 요건이 실용적이지 않을 것입니다. 그러한 경우에는, SafeMail을 대신하여 여러가지 SMTP 서버들 중 어떤 것이든 별도로 구입하여 설치할 수 있습니다. 전체 SMTP 서버를 설치하기로 선택하면, 보안을 염두에 두고 설치하십시오. 더 자세한 내용은 44페이지의 『SafeMail 대신 SMTP 서버 사용』를 참조하십시오.

## 구성 클라이언트를 사용한 SafeMail 구성

SafeMail을 구성하려면 구성 클라이언트 네비게이션 트리에서 시스템 관리를 선택하십시오. 파일 폴더를 두 번 눌러서 보기를 확장하십시오. **SafeMail**을 선택하십시오. IBM Firewall이 구성된 전자우편 서버 및 도메인의 리스트를 표시합니다. 구성되고 있는 각각의 개인 측 전자우편 도메인에 대해 하나의 입력항목을 구성해야 합니다.

1. 도메인을 추가하려면, **신규**를 선택하고 **열기**를 누르십시오. **전자우편 서버 추가** 대화 상자가 나타납니다.
2. **보안 도메인명** 필드에는 설명되고 있는 전자우편 도메인이 Firewall의 보안 부분에서 사용자에게 알려져 있는 이름이 들어 있습니다.
3. **보안 전자우편 서버명** 필드에는 이 항목이 적용되는 전자우편 서버의 호스트명이나 점분리 십진 IP 주소가 들어 있습니다. 이 서버는 보안 네트워크 중 하나에 위치해야 합니다. 주어진 도메인에 대해 하나의 전자우편 서버만을 나열할 수 있습니다.
4. **공용 도메인 이름** 필드에는 설명되고 있는 전자우편 도메인이 Firewall의 비보안 부분에서 사용자에게 알려져 있는 이름이 들어 있습니다. 이 이름은 보안 네트워크의 구조를 감추기 위해 보안 도메인 이름 대신 대체됩니다.
5. **확인**을 누르십시오.

### 전자우편 구성 항목 변경

전자우편 구성 항목을 변경하려면, 리스트에서 항목을 선택하고 **열기**를 누르십시오. **전자우편 서버 구성 변경** 대화 상자가 나타납니다.

**보안 도메인명** 필드는 사용중단되지만, 41페이지의 『구성 클라이언트를 사용한 SafeMail 구성』에서 기술된 대로 다른 필드들은 변경할 수 있습니다.

**주:**

1. 이전에 SafeMail을 구성했으며 여기에서 보안 전자우편 서버를 지정한 경우 이 전자우편 서버는 먼저 구성한 서버를 대신합니다.
2. 이전에 SafeMail을 구성하지 *않았으며* 여기에서 보안 전자우편 서버를 지정하는 경우, 이 전자우편 서버가 구성에 추가됩니다.

### 전자우편 구성 항목 삭제

SafeMail 구성 항목을 삭제하려면 리스트에서 항목을 선택한 다음 **삭제**를 누르십시오. 삭제 경고가 표시됩니다. **확인**을 눌러 삭제하거나, 마음이 변했으면 **취소**를 누르십시오.

## 보안 서버 구성하기

알 수 없는 도메인들에 대해 자신의 게이트웨이를 나열하도록 보안 전자우편 서버를 구성해야 합니다. 이는 비보안 네트워크를 향한 전자우편이 Firewall로 전달되게 합니다. 또한, 각각의 서버는 개인 도메인명 외에 공용 도메인명으로 주소지정된 메세지를 받아들이도록 구성되어야 합니다. Firewall이 비보안 네트워크로부터 노트를 전달하면, 모든 수신자가 그들의 공용측 도메인명과 함께 나열될 것입니다.

보안 네트워크 내에 두 개 이상의 뚜렷한 전자우편 도메인이 있으면, 다른 보안측 도메인을 향한 전자우편이 Firewall을 통해서가 아니라 직접 그 서버로 전달되도록 각각의 서버를 구성해야 합니다. 이는 Firewall의 불필요한 워크로드를 삭제하며 Firewall의 실시간 메카니즘이 제대로 기능하게 합니다.

## 공용 도메인 구성하기

비보안 네트워크에서 필요한 유일한 구성은 여러분의 Firewall을 네트워크에 대한 Mail Exchanger로서 나열하는 것입니다. DNS 서버에 필요한 정보를 추가하도록 서비스 제공자에게 요구하십시오. 수반된 기술에 관한 추가 명세는 31페이지의 『제6장 도메인 이름 서비스 처리』를 보십시오.

Firewall을 전자우편을 받아들이고자 하는 각각의 공용 도메인명에 대한 *Mail Exchanger*로서 나열하는 것이 목적입니다. 예를 들어, 보안 네트워크 안에서 도메인명 *private.com*을 사용하고 보안 네트워크 밖에서는 *public.com*을 사용하면, 여러분의 Firewall을 *gateway.public.com*으로 명명할 것입니다. 그런 경우에는, 제공자에게 호스트로서 Firewall의 호스트명과 IP 주소를 나열하도록

요구할 것입니다 (보통 ″A″ 레코드와 ″PTR″ 레코드로 나열될 것입니다). 그리고 나서, *user@public.com*주소로 전자우편을 받기를 원하면, 제공자에게 도메인에 대한 Mail Exchanger로서 *gateway.public.com*을 나열하는 도메인 *public.com*에 대한 MX 레코드를 추가하도록 요구해야 합니다. *user@somethingelse.com*으로 주소지정된 전자우편도 수신하길 원한다면, 역시 Firewall을 가리키는 추가 MX 레코드를 나열할 수 있습니다.

## SafeMail 사용자 나감(Exit)

SafeMail은 설치가 잠재적으로 해로울 수 있는 통신량을 거부하도록 SafeMail을 조정할 수 있는 사용자 나감(exit)을 제공합니다. 이러한 목적으로 제공되는 소프트웨어 개발 도구에 대한 자세한 설명은 *IBM eNetwork Firewall 참조서*를 참조하십시오.

이 피처는 SafeMail이 송신자로부터 패킷을 수신할 때마다 호출되는 *UsrCheck()* 함수를 작성할 수 있게 합니다. 시스템의 상태에 관련된 여러 필드를 포함하는 구조체에 함수가 전달됩니다. 이 구조체는 고유한 세션 ID, 송신 및 수신 서버의 IP 주소, 이전에 수신된 명령에 대한 표시자, 그리고 분석되고 있는 패킷을 포함하는 플레인 텍스트 버퍼를 포함합니다.

이 함수에서 구현될 수 있는 일부 점검 유형들에는 다음과 같은 것들이 있습니다.

- *금지된* 호스트 리스트
- 부적합한 언어나 프로젝트 코드명과 같은 금해진 문자 순서 살펴보기
- 내포 인용된 문자열 조사
- 메세지 길이 제한

원한다면, 사용자 나감(exit) 역시 제삼자 내용 검사 제품으로의 인터페이스를 구현하는 데 사용될 수 있습니다.

사용자 나감(exit) 함수가 메세지가 처리되어서는 안된다고 결정하면, 함수는 SafeMail로 원인 코드를 반환합니다. SafeMail은 SMTP 서버로의 연결을 즉시 거부할 것입니다. 동시에, 사용자 나감(exit)에 의해 반환된 원인 코드를 포함하여 메세지가 Firewall 로그에 쓰여질 것입니다.

사용자 나감(exit) 작성시, 수신된 모든 패킷에 대해 이 함수가 호출됨을 염두에 두십시오. 시스템 성능에 부정적인 영향을 끼치는 것을 피하기 위해, 가능한 효과적으로 작성하도록 주의하십시오. 또한, 이 함수가 다중 쓰레드 환경에서 수행될 것이며, 따라서 thread-safe 방식으로 쓰여져야 함을 명심하십시오. 다중 쓰레드 조작을 지원하며 *_cdecl* 링키지 규약을 사용할 수 있는 어떤 컴파일러로든 사용자 exit을 작성할 수 있습니다. 샘플 makefile들이 IBM Visual Age C++ 및 Microsoft Visual C++을 위해 제공됩니다.

# SafeMail 대신 SMTP 서버 사용

## SafeMail 작동불능화

다른 SMTP 서버 제품과의 충돌을 피하기 위해 SafeMail을 불능화 시키려면, **서비스 제어 관리** 프로그램으로부터 SafeMail 서비스를 불능화 시키십시오. Windows **시작** 메뉴에서, **설정, 제어판, 서비스**를 선택하십시오. 화면 이동하여 *IBM Firewall SafeMail 서버*를 선택하십시오. **시동**을 누르십시오. **시동 유형** 필드에서, **사용불가**를 선택하십시오. **확인**을 누르십시오.

## SMTP 서버 구성하기

SafeMail을 대신하여 전체 SMTP 서버를 설치할 때에는 여러가지 측면을 고려해야 합니다. 이 섹션에서는 유사한 기능을 수행하도록 SMTP 서버를 구성할 수 있게 하려는 의도로, SafeMail의 보안 피처들을 설명합니다. 특정 SMTP 서버 제품들은 이들 타스크중 일부는 수행할 수 없을 지도 모릅니다. 그러므로 제품을 구매하기 전에 사용 가능한 선택 사항 및 여러분의 필요를 주의깊게 연구하십시오.

오버플로우하려 하거나 그렇지 않으면 전자우편 큐를 손상시키는 특정 시스템 공격이 있습니다. 완전히 꽉찬 어떠한 서버도 전자우편 큐 없이 조작할 수 없을지라도, 그 타스크 전용으로 디스크 볼륨을 지정할 수 있으면 전자 우편 큐와 연관된 위험이 줄어듭니다. 이는 오버플로우된 큐가 Firewall의 다른 조작에 영향을 미칠 가능성을 최소화시킵니다.

전자우편 서버가 보안 네트워크에 대한 정보를 숨시는 것도 중요합니다. SMTP의 규칙에 따라, 전자우편을 전달하는 각각의 서버는 *Received:* 헤더 행을 삽입해야 합니다. 이러한 헤더 행들은 보안 네트워크를 대응시키기 위해 시스템 공격자에 의해 사용될 수 있습니다. SafeMail은 노트 처리시 이러한 헤더를 모두 떼어냅니다. 똑같은 행동을 하도록 SMTP 서버를 구성하십시오. 또한, SafeMail은 모든 개인측 호스트명을 공용 도메인명에 다시 씁니다. 이는 네트워크를 대응시키기 위해 사용될 수 있었던 훨씬 더 많은 정보를 삭제합니다.

# SafeMail에 대한 샘플 로깅 출력

다음은 SafeMail에 대한 로깅 출력의 샘플입니다.

```
1998년 2월 3일 13:46:11 mr16n18: ICA2163i: safemaild가 시작되었습니다.

1998년 2월 3일 13:41:14 mr16n18: ICA2177i: SafeMail 연결 0xd71e7a19
가 RACK3BD로부터 수신되었습니다.
1998년 2월 3일 13:41:21 mr16n18: ICA2179i: SafeMail이
9.67.144.52로부터 9.67.131.250으로 연결 0xd71e6118에 대
한 215575 바이트를 전달했습니다.
1998년 2월 3일 13:41:21 mr16n18: ICA2178i: SafeMail 세션 0xd71e7a19
기 9.67.144.52로부터 9.67.131.250으로 형성되었습니다.
1998년 2월 3일 13:41:23 mr16n18: ICA2177i: SafeMail 연결 0xd71e831a
가 RACK3BD로부터 수신되었습니다.
```

```
1998년 2월 3일 13:41:36 mr16n18: ICA2177i: SafeMail 연결 0xd71e901b
가 RACK3BD로부터 수신되었습니다.
1998년 2월 3일 13:41:56 mr16n18: ICA2179i: SafeMail이 9.67.144.52로부터
9.67.131.250으로 연결 0xd71e7a19에 대한 215567 바이트
를 전달했습니다.
1998년 2월 3일 13:41:56 mr16n18: ICA2178i: SafeMail 세션 0xd71e831a
기 9.67.144.52로부터 9.67.131.250으로 형성되었습니다.
1998년 2월 3일 13:41:56 mr16n18: ICA2178i: SafeMail 세션 0xd71e901b
기 9.67.144.52로부터 9.67.131.250으로 형성되었습니다.
1998년 2월 3일 13:41:57 mr16n18: ICA2179i: SafeMail이 9.67.144.52로부터
9.67.131.250으로의 연결 0xd71e901b에 대한 346 바이트
를 전달했습니다.
1998년 2월 3일 13:41:57 mr16n18: ICA2179i: SafeMail이 9.67.144.52로부터
9.67.131.250으로의 연결 0xd71e831a에 대한 358 바이트
를 전달했습니다.
```

로그 메세지는 다음과 같은 내용을 담고 있습니다.

- ICA2177 - 신규 연결의 시작을 나타냅니다.
- ICA2179 - 성공적인 종료를 나타냅니다.
- ICA2178 - 수신하는 SMTP(단순 전자우편 전송 규약) 서버와 접속이 이루어졌음을 나타냅니다.
- ICA2181 - SafeMail이 세션을 거부했음을 나타냅니다. 이유 코드는 *IBM eNetwork Firewall 참조서*를 참조하십시오.
- ICA2180 - 세션 종료를 나타냅니다.
- ICA2182 - 사용자 나감이 세션이 거부되어야 한다고 결정했음을 나타냅니다.

# 제8장 Firewall을 통해 통신량 조절

이 장에서는 구성 클라이언트를 사용하여 Firewall을 통해 네트워크 통신량을 조절하는 방법을 알려줍니다. expert 필터를 사용하여, 세션 레벨의 Firewall 필터 패킷은 시각, IP 주소 및 서브네트와 같은 여러 가지 기준을 따릅니다. 이 필터는 보안 및 비보안 네트워크 인터페이스 사이에서 작동합니다. 이 필터는 Firewall 경로지정 표에는 영향을 미치지 않습니다.

디폴트로 Firewall에서는 보안 및 비보안 네트워크간의 어떠한 통신량도 흐르도록 허용하지 않습니다. 특정 유형의 통신이 보안 및 비보안 네트워크 사이에서 이동할 수 있게 하려면, 연결을 작성해야 합니다.

## 연결을 구축하기 위해 구성 클라이언트 사용

48페이지의 그림 14에서 설명된 구성 클라이언트의 구성요소를 사용하여 네트워크 오브젝트, 규칙 템플리트, 서비스, 그리고 연결을 작성하십시오.

**연결** 네트워크 오브젝트를 서비스와 또는 Socks 템플리트를 연관시켜서 끝점간에 허용된 통신의 유형을 정의하십시오. 각 연결은 출발지 및 목적지 네트워크 오브젝트 간에 허용되거나 거부되는 특정한 IP 통신 유형을 정의합니다.

**서비스**

하나 이상의 규칙 템플리트의 구축입니다. 출발지 및 목적지 오브젝트간에 허용되거나 거부되는 IP 통신 유형을 정의합니다. 예를 들면 텔넷을 허용하거나 ping을 거부하도록 서비스를 구축할 수 있습니다. (FTP 서비스 중 하나는 8개의 규칙 템플리트로 구성됩니다). IBM Firewall은 디폴트 서비스 세트에 있습니다. 이런 사전로드된 디폴트 서비스를 삭제할 수 없지만 특정 필드는 변경할 수 있습니다. 그러나, 만일 이런 사전정의된 서비스가 사용자의 필요를 만족시키지 못하면, 규칙 템플리트로 새로운 규칙을 작성해서 서비스에 추가할 수 있습니다. 더 자세히 알고 싶으면, 69페이지의 『서비스 정의』를 참조하십시오.

**규칙 템플리트**

다양한 속성에 근거하여 IP 패킷을 허용 또는 거부하도록 Firewall에 지침을 제공합니다.

**Socks 템플리트**

Firewall Socks 디먼이 IP 패킷을 그 다양한 속성에 근거하여 허용 또는 거부하도록 명령을 제공합니다.

**네트워크 오브젝트**

Firewall과 상호작용하는 호스트, 사용자 및 서브네트와 같은 다양한 네트워크 구성요소를 나타냅니다. 이들은 하나의 IP 주소와 주소 마스크로 정의되므로 한 오브젝트가 광범위한 네트워크 주소를 나타낼 수 있습니다. 네트워크 오브젝트는 그룹을 이룰 수 있습니다.

**네트워크 오브젝트 그룹**

하나 이상의 네트워크 오브젝트를 나타냅니다. 이는 연결을 설정할 때 편의로 사용되고 반복적인 작업을 삭제할 수 있습니다. 예제로는 여러 주소를 함께 네트워크 오브젝트 그룹으로 모아서 부서를 나타내는 것입니다. 이 네트워크 오브젝트 그룹은 연결의 출발지 또는 목적지로 사용될 수 있습니다.

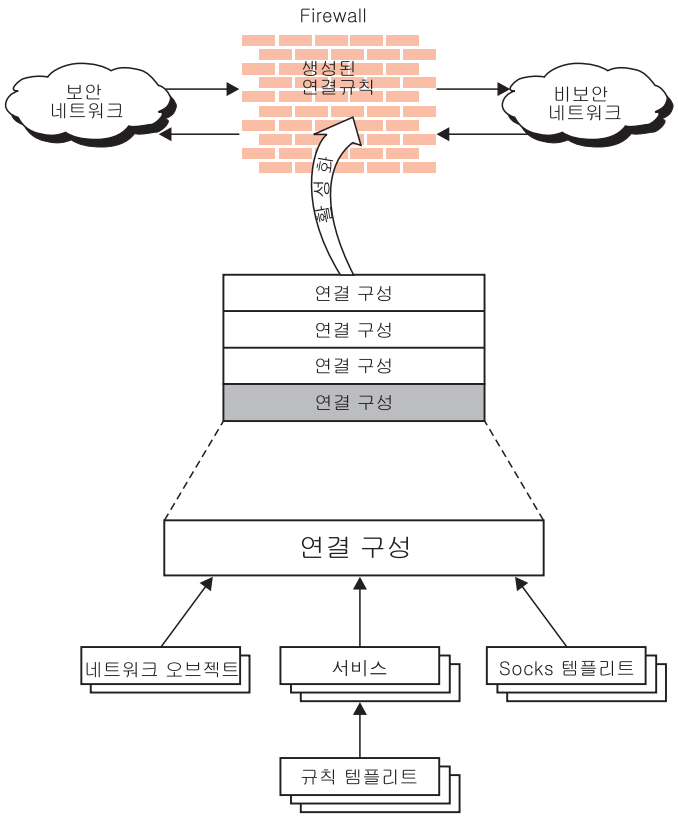


*그림 14. 연결 구축하기*

## 사전정의된 서비스를 사용해서 연결 구축

두 개의 명명된 네트워크 오브젝트와 끝점으로 제공되는 네트워크 오브젝트 그룹간의 특정 유형의 통신을 허용하거나 거부하기 위해서는, 연결을 구축해야 합니다.

네트워크 오브젝트를 정의한 후에 연결을 작성하십시오. Firewall을 통한 통신 흐름에 대한 출발지가 될 하나의 네트워크 오브젝트나 그룹을 선택하고 목적지가 될 또다른 네트워크 오브젝트나 그룹을 선택하십시오.

연결을 구축하려면, 구성 클라이언트 네비게이션 트리에서 통신량 조절을 선택하고 파일 폴더를 두 번 눌러서 보기를 확장하십시오. **연결 설정**을 선택하십시오. **연결 리스트** 대화 상자가 나타납니다. **신규**를 선택하고 **열**

기를 누르십시오. 49페이지의 그림 15에서 보여주는 바와 같이 **연결 추가** 대화 상자가 나타납니다.

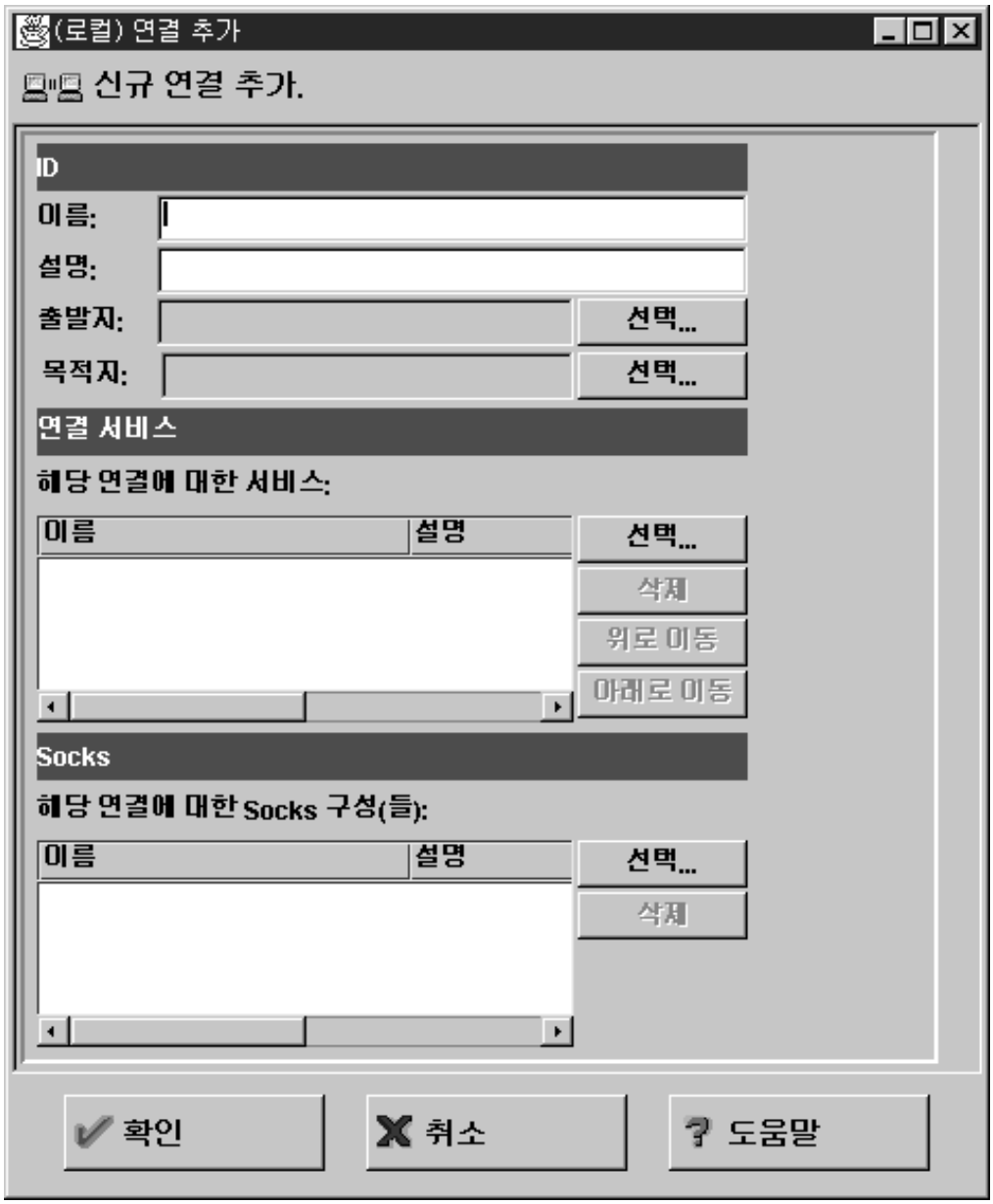


*그림 15. 연결 추가*

1. 연결의 이름을 채우십시오.
2. 연결의 설명을 채우십시오.
3. 출발지 필드의 경우, **선택**을 누르고 **네트워크 오브젝트** 대화 리스트에서 네트워크 오브젝트를 고르십시오.
4. 목적지 필드의 경우, **선택**을 누르고 **네트워크 오브젝트** 대화 리스크에서 네트워크 오브젝트를 고르십시오.

5. 이 연결을 위한 서비스를 선택하려면, **선택**을 누르고 끝점간에 조절하고 싶은 통신량의 유형을 고르십시오.
6. 리스트에서 한 개 이상의 서비스를 선택해서 서비스를 연결에 추가하십시오.
7. 서비스를 선택하고 **위로 이동** 또는 **아래로 이동**을 눌러 리스트의 순서를 다시 정할 수 있습니다. 50페이지의 『연결 순서 지정』을 참조하십시오.
8. 서비스를 선택하고 **삭제**를 눌러 서비스를 삭제할 수 있습니다.
9. **이 연결을 위한 Socks 구성**을 사용하십시오. Socks를 위한 연결을 이루기 위해 단계 5–7을 따르십시오.
10. 모든 것을 정의한 후에는, **확인**을 누르십시오.
11. 모든 연결을 활성화시키십시오. 50페이지의 『연결 활성화』를 참조하십시오.

## 연결 순서 지정

대부분의 IBM Firewall 사용자는 1000가지 이하의 규칙을 가집니다. 규칙이 많을 수록 성능에 미치는 영향이 커집니다.

네트워크 인터페이스에서 패킷이 수신되면 이 패킷이 Firewall 호스트로 들어가든지 이 호스트에서 나오든지에 관계없이 생성된 연결 규칙의 맨 위부터 규칙들이 적용됩니다. 패킷의 정보와 규칙의 정보가 정확히 일치하면 조치(허용 또는 거부)가 수행됩니다. 전체 파일 탐색시 일치되는 것이 없으면 요청은 거부됩니다.

**힌트:** 좀더 특정한 연결은 위쪽에 가깝게 두고 덜 특정한 연결은 아래쪽에 가깝게 두십시오. 예를 들어 (1.1.10.X)의 주소를 가진 부서 ABC와 (1.1.10.7)의 주소를 가지며 부서 ABC 내에서 서버로 사용되는 시스템을 가질 수 있습니다. 텔넷 소통에 사용되어서는 안되는 서버이기 때문에 시스템 1.1.10.7을 제외시키고자 하는 경우 부서 ABC 서버에 대해 텔넷 거부를 부서 ABC에 대해 텔넷 허용 연결 앞에 놓아야 합니다. 연결 순서를 거꾸로 하면 거부 연결이 절대로 발생하지 않게 됩니다.

## 연결 활성화

**주: 연결을 활성화하기 전에 보안 인터페이스가 정의되어 있는지 확인하십시오.**

구성 클라이언트 네비게이션 트리로부터 **연결 활성화**를 선택하여 다음을 수행하십시오.

**연결 규칙 재작성 및 활성화**
Firewall은 연결 구성으로부터 생성된 연결 규칙을 구축하고 해당 규칙 세트를 활성화합니다.

**연결 규칙 비활성화**
이제 Firewall은 디폴트 규칙으로 보호됩니다.

**현재 연결 규칙 나열**
가장 최근에 생성된 연결 규칙 세트를 표시합니다. 이전에 규칙들을 비활성화하면, 규칙들이 사용되지 않습니다.

**규칙 생성 유효성 확인**
작성된 규칙이 유효하거나 유효하지 않습니다.

**연결 규칙 로깅 가능**
Firewall은 선택된 통신량을 Firewall 로그 기능에 기록합니다.

**연결 규칙 로깅 불능**
Firewall 로깅을 중단합니다.

**연결 활성화** 대화 상자가 52페이지의 그림 16에서 처럼 나타납니다.

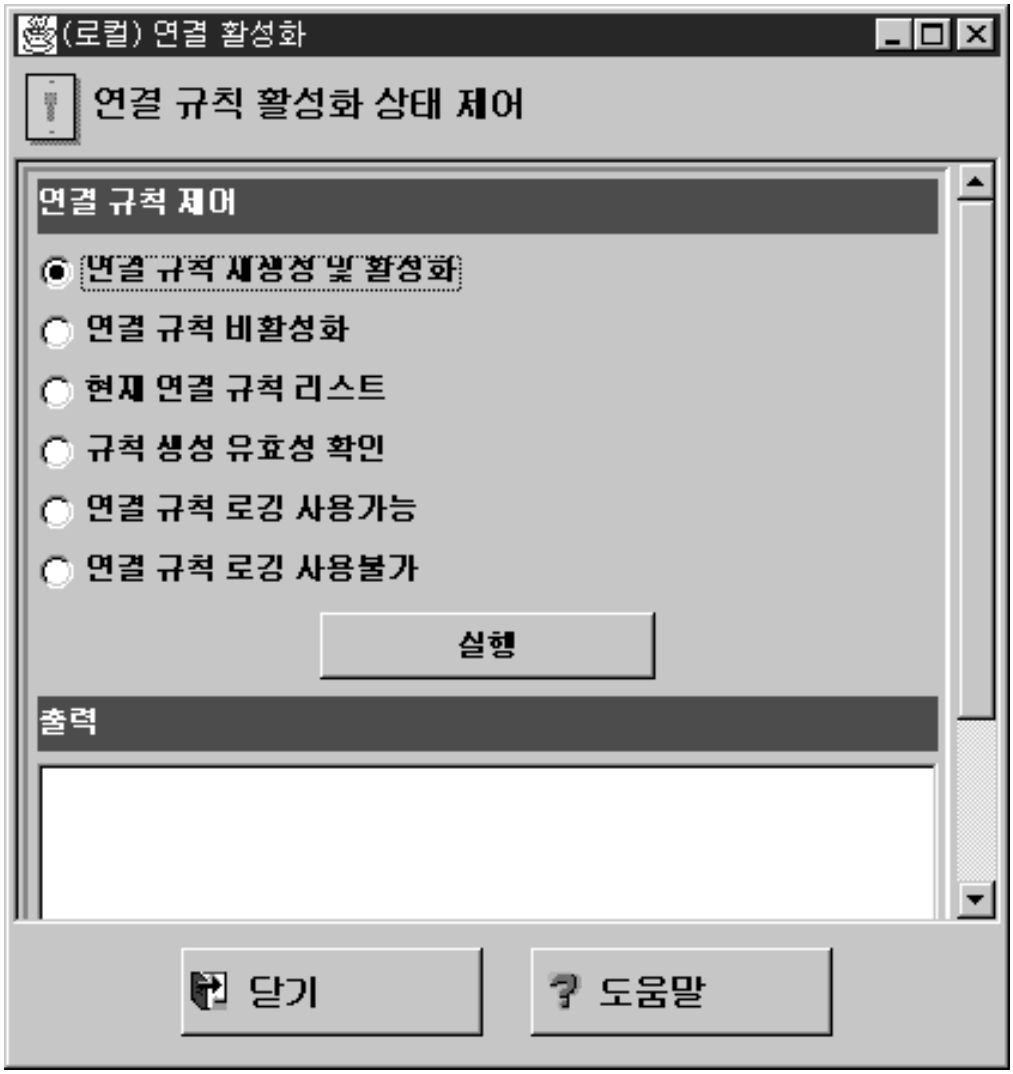


*그림 16. 연결 활성화*

선택을 한 후에, **실행**을 누르십시오.

## 연결 규칙 재생성 및 활성화시의 샘플 로깅 출력

다음은 연결 규칙을 재생성하여 활성화할 때의 로깅 출력의 샘플입니다.

```
1998년 2월 3일 13:46:53 mr16n18: ICA9037i: 1998년 2월 3일 화요일
에 Firewall 인터페이스가 자동으로 갱신됩니다.

1998년 2월 3일 13:46:55 mr16n18: ICA1032i: 1998년 2월 3
일 13시 46분 55초에  필터 규칙이 갱신되었습니다.

1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 eq 53 both local both l=n f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp gt  1023 eq 53 both local both l=n f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 gt  1023 both local both l=n f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:4 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp     gt  1023 eq 25 both local both l=y f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:5 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

```
tcp/ack eq  25 gt 1023 both local both l=y f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:6 permit 9.67.144.49 255.255.255.240
9.67.130.154 255.255.248.0 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:7 permit 9.67.130.154 255.255.248.
0 9.67.144.49 255.255.255.240 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:8 permit 9.67.144.49 255.255.255.240
9.67.131.250 255.255.255.255 tcp     gt  1023 eq  21 secure local inbound
l=n f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:9 permit 9.67.131.250 255.255.255.255
9.67.144.49 255.255.255.240 tcp/ack eq  21 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:10 permit 9.67.131.250 255.255.255.
255 9.67.144.49 255.255.255.240 tcp     eq  20 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:11 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp/ack gt  1023 eq  20 secure local inbound
l=n f=y t=0 e=none a=none
1998년 2월 3일 13:46:55 mr16n18: ICA1037i: #:12 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp     gt  1023 gt  1023 secure local inbound
l=n f=y t=0 e=none a=none
.
.
.
1998년 2월 3일 13:46:58 mr16n18: ICA1037i: #:100 deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
all any 0 any 0 both both both l=y f=y t=0 e=none a=none
```

## 규칙 상태 판별하기

IBM Firewall은 다음 상태중 하나에 있을 수 있습니다.

1. 구성은 활성화되지 않았습니다.

   아직 구성을 활성화시키기 위해 구성 클라이언트를 사용하지 않았거나 또는 구성을 비활성화시켰습니다. 이것은 맨 처음 IBM Firewall을 설치한 후 시스템을 부트하거나 필터 규칙을 비활성화할 경우의 구성 상태입니다. 디폴트 필터는 Firewall을 처음으로 설치할 때 네트워크를 침입으로부터 보호하기 위해 배치됩니다.

   Firewall 액세스:

   - 디폴트 필터 구성은 모든 로컬 인바운드 통신을 허용하고 모든 아웃바운드 통신을 허용합니다.

2. 구성은 활성화되지만 오류는 없습니다.

   구성을 활성화시켰습니다. 구성에 오류(유효하지 않은 규칙)가 있거나 또는 아무것도 구성되지 않았습니다. 오류와 경고는 활성화 출력 창에 표시됩니다.

   Firewall 액세스:

   - 모든 로컬 인바운드 통신을 허용합니다.
   - 모든 아웃바운드 통신을 허용합니다.

3. 구성은 활성화되고 유효합니다. 몇 가지 경고가 있을 수 있는데, 그 중에서도 특히 필터 규칙 복제등입니다.

   구성 클라이언트의 통신량 조절 섹션을 사용해서 정의한 구성을 활성화했습니다.

   **주:** 구성 파일은 유효하면서도 여전히 규칙을 포함하지 않을 수 있습니다. 이런 경우에는 내포된 『모든 액세스 거부』 규칙이 적용됩니다.

Firewall 액세스:

- 구성 파일에 의해 결정된 액세스.

  수신되거나 곧 전송될 각 패킷, 네트워크 인터페이스는 검토되고 생성된 연결 규칙에 있는 각 규칙과 그 내용이 비교됩니다. 일치하는 것을 찾게 되면, 그 규칙에 대한 조치(허용 또는 액세스 거부)가 수행됩니다.
- 패킷과 일치하는 규칙이 없으면 액세스를 거부하는 암시적인 『모두 거부』 규칙이 존재합니다.

# 제9장 서비스 예제

이 장에서는 특정한 공통 타스크를 수행하도록 Firewall을 구성하는 방법에 대해 설명합니다. 나열된 타스크는 단지 예제이지만, 이것을 이해하고 나면 제공된 모든 서비스를 사용하기 위해 Firewall을 구성할 수 있어야 합니다.

## 계획 고려사항

Firewall의 통신량 조절은 끝점 쌍 사이에서 허용되거나 금지되는 통신 유형을 정의하는 연결에 의해 구성됩니다. 따라서 이러한 끝점에 따라 연결을 계획하는 것이 중요합니다.

47페이지의 『제8장 Firewall을 통해 통신량 조절』에서 기술된 대로, 끝점은 네트워크 오브젝트에 의해 Firewall에 표시됩니다. 만일 아직 그렇게 하지 않았다면, 7페이지의 『제2장 계획』의 네트워크 계획 워크시트를 완료하고 네트워크를 나타내기 위해 필요한 네트워크 오브젝트를 작성해야 합니다.

이 장에 나오는 예제는 다음의 네트워크 오브젝트를 사용합니다.

**보안 인터페이스**
Firewall의 보안 인터페이스.

**비보안 인터페이스**
Firewall의 비보안 인터페이스.

**보안 네트워크**

Firewall의 보안 인터페이스를 통해 액세스할 수 있는 주소의 범위. 이것은 각각이 그 자체의 네트워크 오브젝트로 표현되는 여러 개의 구분되는 도메인을 포함할 수 있는 네트워크 오브젝트 그룹일 수 있습니다.

**월드** 비보안 네트워크.

원하는 각 통신 유형은 관련된 지점간 통신에 따라 열람되어야 합니다. 이 단계에서 Firewall이 프록시에 의해 이러한 통신을 제공하는지 혹은 Firewall이 이러한 통신의 경로를 지정할 것인지의 여부를 고려하십시오.

Firewall이 프록시의 역할을 하면, Firewall은 보안 사용자 대신에 필요한 작업을 수행하게 되며, 비보안 호스트는 보안 호스트가 존재한다는 것을 결코 모르게 됩니다. Firewall이 통신 경로를 지정하면 보안 호스트와 비보안 호스트는 서로 직접 대화하게 됩니다.

Firewall을 프록시로 사용하면 통신의 끝점에는 56페이지의 그림 17에서와 같이 Firewall이 포함됩니다.

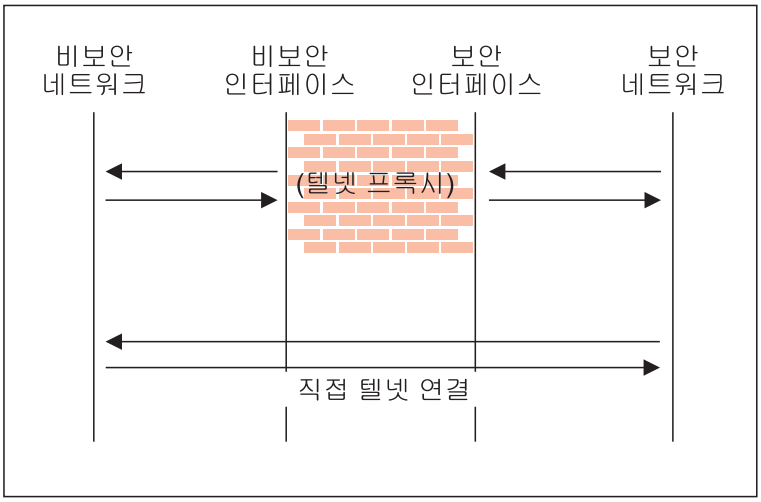


*그림 17. 텔넷 프록시 및 직접 텔넷 연결*

## 텔넷 프록시의 예제

이 첫번째 예제는 간단한 아웃바운드 텔넷 프록시 연결입니다. 이 예제에서, 보안 네트워크의 사용자는 비보안 네트워크에 있는 호스트의 텔넷 서비스를 액세스할 수 있도록 Firewall의 텔넷 프록시를 사용할 수 있게 됩니다.

56페이지의 그림 17에서 설명된 대로 두 개의 연결이 이루어집니다.

1. 보안 네트워크내에 있는 클라이언트는 Firewall의 텔넷 프록시에 연결됩니다.
2. Firewall의 텔넷 프록시는 보안 사용자 대신 비보안 네트워크에 있는 호스트로 연결됩니다.

이 통신에 대해 Firewall의 통신량 조절을 구성하려면, 두 개의 연결을 설정해야 합니다.

*표 1. 텔넷 프록시*

| 출발지 오브젝트 | 목적지 오브젝트 | 필수 서비스 |
|---|---|---|
| 보안 네트워크 | 보안 인터페이스 | 텔넷 프록시 아웃 1/2 |
| 비보안 인터페이스 | The World | 텔넷 프록시 아웃 2/2 |

## 필터된 텔넷의 예제

위의 예제를 필터된 단순 텔넷 연결과 대조해 보십시오. 이 경우, 보안 측의 클라이언트는 비보안 측이 호스트와 직접 연결됩니다.

*표 2. 필터된 텔넷*

| 출발지 오브젝트 | 목적지 오브젝트 | 필수 서비스 |
|---|---|---|
| 보안 네트워크 | The World | 텔넷 직접 아웃 |

앞서 언급한 대로, 이 구성은 비보안 호스트에 연결할 때 보안 클라이언트의 주소를 노출하게 됩니다.

## 프록시 HTTP의 예제

대부분의 설치는 최소한 몇 몇 보안 클라이언트가 웹을 자유롭게 이동할 수 있도록 합니다. IBM Firewall은 필터된 텔넷 예제와 정확히 동일하게 기능하는 경로지정된 HTTP를 허용하도록 사전정의된 HTTP 아웃바운드 직접 서비스를 제공합니다. 이 외에, Firewall은 HTTP 프록시도 제공합니다.

HTTP 프로토콜은 기타 프로토콜을 포장할 수 있다는 점에서 텔넷과 다릅니다. 단순 서핑의 경우에도 대부분의 사용자는 HTTP 뿐 아니라 FTP 서비스를 요구합니다. 전체 범위의 HTTP 기능을 제공하려면, Gopher 및 WAIS가 덜 자주 사용되더라도, 허용되어야 합니다.

비록 이런 추가 프로토콜이 사용되고 이는 클라이언트와 프록시 사이의 HTTP에 랩됩니다. 그러므로, 통신은 57페이지의 그림 18에 있는 도표와 비슷합니다.

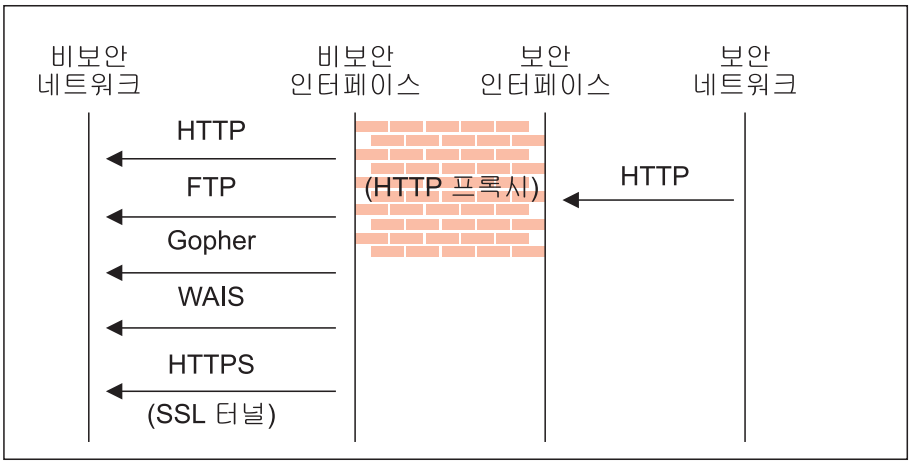


*그림 18. 프록시 HTTP*

두 쌍의 끝점이 포함되어 있으므로, 두 개의 연결을 코딩해야 합니다.

*표 3. 프록시 HTTP*

| 출발지 오브젝트 | 목적지 오브젝트 | 필수 서비스 |
|---|---|---|
| 보안 네트워크 | 보안 인터페이스 | HTTP 프록시 아웃바운드 1/2 |

*표 3. 프록시 HTTP (계속)*

| 출발지 오브젝트 | 목적지 오브젝트 | 필수 서비스 |
|---|---|---|
| 비보안 인터페이스 | The World | 선택...<br>• HTTP 프록시 아웃 2/2<br>• FTP 프록시 아웃 2/2<br>• Gopher 프록시 아웃 2/2<br>• WAIS 프록시 아웃 2/2<br>• HTTPS 프록시 아웃 2/2 |

HTTP 프록시에 대해 더 자세히 알고 싶으면, 93페이지의 『제13장 프록시 서버 구성』을 참조하십시오.

## Socks의 예제

SOCKS는 SOCKS 디먼이 여러 다른 프로토콜을 처리하고 이를 Firewall과 클라이언트 간의 단일 데이터 스트림으로 포장한다는 점에서 HTTP 프록시의 SOCKS와 유사합니다. SOCKS는 TCP 또는 UDP 지향 프로토콜을 수용할 수 있고 Firewall이 통신을 좀더 잘 제어할 수 있도록 필터와 독립적으로 구성될 수 있다는 점에서 HTTP 프록시보다 좀더 유동적입니다.

융통성이 추가된 Socks로 인해 Socks를 구성하면, HTTP 프록시로 실연되는 연결외에도 제 3의 연결이 필요합니다. 두 개의 기본 연결은 패킷이 Firewall으로 흐르거나 또는 Firewall에서 외부로 흐르도록 합니다. Socks 디먼이 패킷을 일단 수신하면 요청을 프록시하도록 지시하기 위해서는 제 3의 연결이 필요합니다.

*표 4. Socks*

| 출발지 오브젝트 | 목적지 오브젝트 | 필수 서비스 |
|---|---|---|
| 보안 네트워크 | 보안 인터페이스 | Socks 1/2 |
| 비보안 인터페이스 | The World | 선택...<br>• HTTP 프록시 아웃 2/2<br>• FTP 프록시 아웃 2/2<br>• 텔넷 프록시 아웃 2/2<br>(지원을 제공하려는 2/2 프록시 서비스) |
| 보안 네트워크 | The World | Socks 구성 창에서 다음을 선택...<br>• Socks-준수 HTTP 허용<br>• Socks-준수 FTP 허용<br>• Socks-준수 텔넷 허용 |

물론, 보안 네트워크내의 클라이언트는 Socks를 준수해야 하며 Firewall을 Socks 서버로 사용하기 위해 구성되어야 합니다.

Socks에 대해 더 알고 싶으면, 73페이지의 『제11장 Socks 서버 구성』을 참조하십시오.

## DNS에 대한 힌트

DNS 분석을 제공하지 않으면 매우 적은 통신만이 효율적으로 이루어집니다. DNS 구성에 대한 세부사항은 31페이지의 『제6장 도메인 이름 서비스 처리』를 보십시오. 잊지말고 보안 규정에서 ″DNS 질의 승인″을 작동가능하게 하십시오.

## 비보안 SOCKS 클라이언트에 대한 힌트

보안 규정 패널에는 **비보안 인터페이스에 대한 Socks 거부**를 위한 확인란이 들어 있습니다. 이 서비스는 비보안 인터페이스에서 SOCKS 디먼으로 주소가 지정된 패킷을 거부하며 Firewall을 좀더 안전하게 구성해 줍니다.

클라이언트가 비보안 네트워크로부터 여러분의 네트워크로 들어가도록 허용하려면, 이 *확인 상자*에 표시해서는 안됩니다.

# 제10장 통신량 조절 조정

이 장은 필터 규칙과 서비스를 정의하는 데 도움을 줍니다. 서비스는 텔넷 세션과 같이 Firewall을 통해 특정 유형의 통신량을 허용하거나 또는 거부하는 규칙의 집합 또는 일연의 명령입니다. 규칙 템플리트로 새로운 규칙을 작성해서 서비스에 추가할 수 있습니다. 서비스를 삭제할 수도 있습니다. Socks 서비스는 Socks-준수 연결에 적용됩니다.

IBM Firewall은 디폴트 서비스 세트로 사전로드됩니다. 모든 사전정의된 서비스를 특정 필요에 맞게 조정하거나 또는 새로운 서비스를 작성할 수 있습니다.

## 규칙 템플리트를 작성하기 위해 구성 클라이언트 사용

이 프로시듀어를 사용해서 새로운 규칙을 사용 가능한 규칙 템플리트에 추가하십시오.

1. 구성 클라이언트 네비게이션 트리에서 통신량 조절을 선택하고 파일 폴더 아이콘을 두 번 누르십시오. **연결 템플리트**를 선택하고 나서 **규칙**을 선택하십시오.
2. **규칙 리스트** 대화 상자에서, **신규**를 두 번 누르십시오.

   IBM Firewall은 62페이지의 그림 19에서 보여주는 바와 같이 **IP 규칙 추가** 대화 상자를 표시하여, 여러분이 규칙을 정의할 수 있게 합니다.

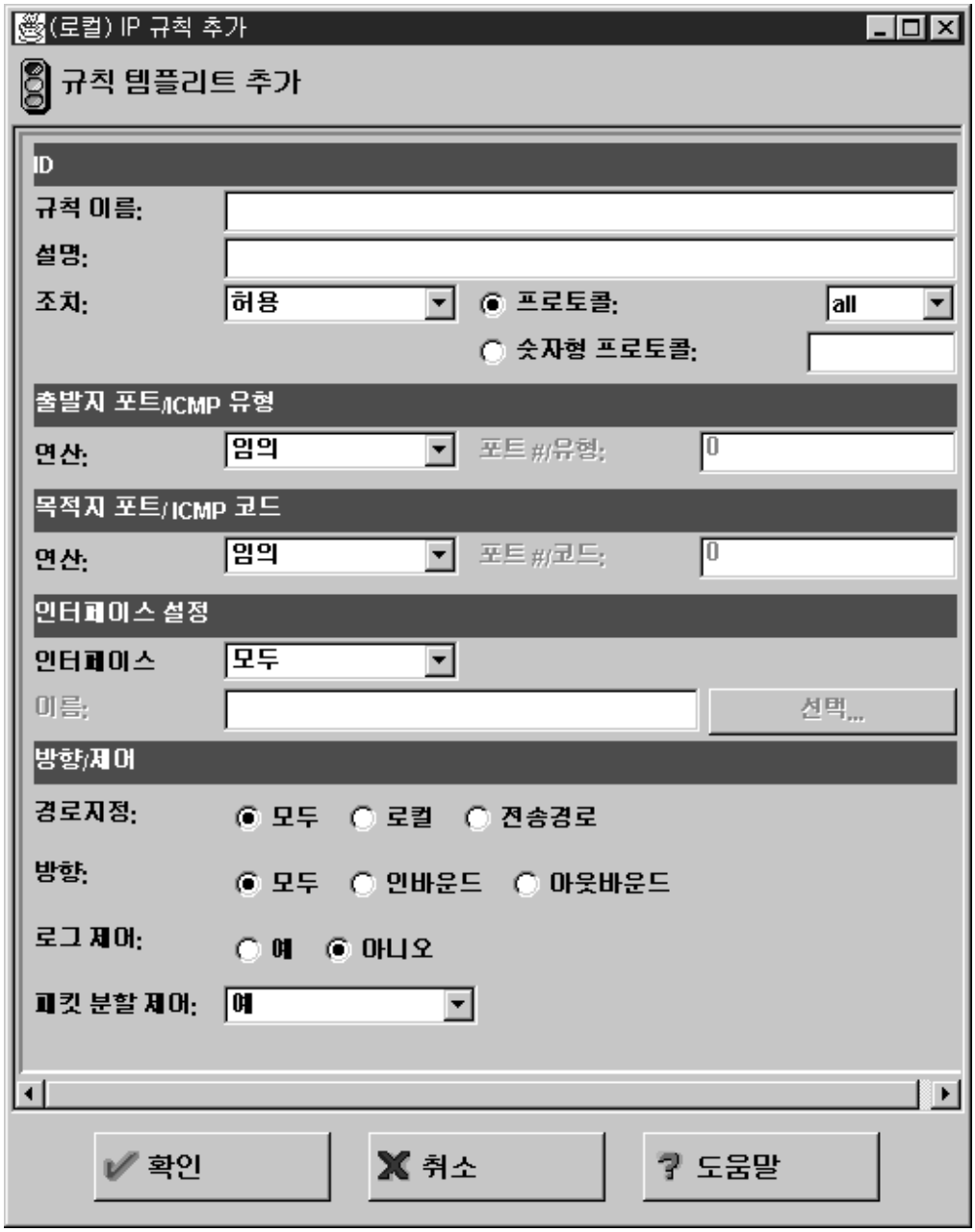


*그림 19. IP 규칙 추가*

3. 규칙명을 입력하십시오.
4. 규칙 설명을 입력하십시오. 이 필드는 선택적입니다.
5. 조치 화살표를 누르고 Firewall로의 액세스 허용 또는 거부를 선택하십시오.
6. 프로토콜 화살표를 누르고 다음 리스트에서 선택하십시오.

   **all** 이 규칙과 일치하는 모든 프로토콜.

   **tcp** 패킷 프로토콜은 이 규칙에 일치하려면 전송 제어 프로토콜(TCP)이어야 합니다.

**tcp/ack**

패킷 프로토콜은 이 규칙에 일치하려면 확인 응답을 나타내는 TCP여야 합니다.

**udp** 패킷 프로토콜은 이 규칙에 일치하려면 사용자 패킷 프로토콜(UDP)이어야 합니다.

**icmp** 패킷 프로토콜은 이 규칙에 일치하려면 인터넷 제어 메세지 프로토콜(ICMP)이어야 합니다.

**ospf** 패킷 프로토콜은 이 규칙에 일치하려면 개방형 최단 경로 첫번째 프로토콜(OSPF)이어야 합니다. OSPF가 프로토콜로 지정되면, OSPF 레코드 유형 값에 대해 출발지 포트 조작과 출발지 포트 값이 사용됩니다. 필터링은 OSPF 유형에 대해서도 수행될 수 있습니다. **임의**의 유형 값이 지정될 수 있으며 목적지 포트 필드는 **임의 0**으로 지정되어야 합니다. 그 외에는 무시됩니다.

**ipip** 패킷 프로토콜은 이 규칙에 일치하려면 IP-in-IP protocol(IPIP)이어야 합니다. IPIP가 지정되면, 포트 필드는 **임의 0**으로 지정되어야 합니다.

**esp** 패킷 프로토콜은 이 규칙에 일치하려면 포장된 IP 패킷을 전송하기 위해 가상 개인 네트워크에서 사용하는 포장 보안 프로토콜이어야 합니다.

**ah** 사용자 확인 헤더 프로토콜은 관련된 사용자 확인 토큰을 가지는 IP 패킷을 전송하기 위해 가상 개인 네트워크에서 사용하는 패킷 프로토콜입니다.

7. 숫자 프로토콜은 십진 값을 사용해서 프로토콜을 지정할 수 있게 합니다(RCF-1700에 따라). 유효 값의 범위는 1에서 252입니다. 이 규칙에 대한 포트 필드는 이 옵션을 사용할 때 0(임의 포트 의미)으로 지정되어야 합니다. 모든 프로토콜의 리스트에 대해 RFC-1700을 참조하십시오. 아니면, 브라우저를 사용하여 인터넷 번호 할당 기관(IANA)에 액세스할 수 있습니다.
8. 조작과 포트 번호 피조작자는 함께 사용됩니다. 출발지 및 논리적 조작이 패킷에 대한 포트 번호(목적지 또는 출발지)와 출발지 port# 조작자 및 목적지 port# 조작자간의 관계를 기술합니다. 예를 들어 패킷 목적지 포트가 포트 20이고 목적지 조작과 목적지 port#가 『ge 15』이면 패킷이 일치됩니다. (20은 15보다 크거나 같습니다. )

   **any**의 출발지 또는 목적지 조작을 사용하면, 필터가 포트 번호를 보지 않습니다. 어떤 포트든 일치됩니다. 포트 번호는 이런 경우에 변경될 수 없습니다.

   ICMP 프로토콜에 대해 출발지 포트를 지정하기 보다는 ICMP 유형을 지정하고 목적지 포트 자리에 ICMP 코드를 지정하십시오. 지정된 논리적 조작자가 유형 또는 코드에 적용되며, 포트에 대해서 any의 조작자는 어떠한 유형 또는 코드 값이든 규칙과 일치됨을 의미합니다. 포트 번호는 이런 경우에 변경될 수 없습니다.

   조작에 대한 값들은 다음과 같습니다.

- 임의
- 같음
- 같지 않음
- 보다 작음
- 보다 큼
- 작거나 같음
- 크거나 같음

여기에는 보고해야 하는 좀더 중요한 일부 포트가 나와 있습니다. 포트 번호에 대한 값의 범위는 1에서 65535이어야 합니다.

**포트** **사용**

**20** FTP 데이터

**21** FTP 제어

**23** 텔넷

**25** 전자우편

**53** 도메인 이름 서버

**70** Gopher

**80** HTTP

**111** RPC

**161** SNMP

**1080** Socks

여기에 ICMP 유형과 코드중 일부가 있습니다.

**유형** **코드 및 설명**

**0** 0 - Ping 응답

**8** 0 - Ping 요청

**3** 1 - 호스트에 도달 불가능

**3** 3 - 포트에 도달 불가능

**5** 1 - 호스트에 대해 경로 재지정

9. **인터페이스** 화살표를 눌러 인터페이스 유형(어댑터)을 선택하십시오.

   **모두** 보안 또는 비보안 인터페이스 상을 오가는 패킷

   **보안** 보안 인터페이스 상을 오가는 패킷

   **비보안**
   비보안 인터페이스 상을 오가는 패킷

   **특정** 인터페이스에 이미 이름을 지정한 경우, 인터페이스 선택시 인터페이스 이름 필드와 함께 사용하십시오.

10. 만일 인터페이스 유형으로 특정을 선택하면, 특정 인터페이스의 이름이 이름 필드에 나타납니다.
11. 원하는 경로지정을 누르십시오.

    **모두** 모든 통신량에 적용됩니다.

    **로컬** 패킷이 Firewall 호스트에 대해 로컬이라는 것을 의미합니다. 이는 다음을 의미합니다.

    - 수신 로컬 패킷은 인터페이스에서 수신되는 패킷이며 이 Firewall 호스트로 향하고 있습니다. 이는 또다른 호스트로 경로지정되지 않습니다. 목적지는 로컬입니다.
    - 송신 패킷은 인터페이스에서 전송되지만 Firewall 호스트에서 시작됩니다. 출발지는 로컬입니다.

    **경로지정**

    패킷이 Firewall 호스트에 의해 경로지정된다는 것을 의미합니다. 이는 다음을 의미합니다.

    - 들어오는 로컬 패킷은 인터페이스에서 수신되는 패킷이며 다른 호스트로 향하고 있습니다. 이는 Firewall에 남아 있지 않습니다. 목적지는 원격입니다.
    - 송신 패킷은 인터페이스에서 전송되지만 다른 호스트에서 시작됩니다. 출발지는 원격입니다.
12. 원하는 방향을 누르십시오.

    **모두** 선택된 인터페이스로 들어오거나 나가는 패킷

    **인바운드**

    네트워크로부터 선택된 인터페이스로 들어오는 패킷

    **아웃바운드**

    선택된 인터페이스에서 인터페이스로 나가는 패킷
13. 로그 제어 필드에 대해 예를 선택하면, 해당 규칙에 맞는 모든 패킷이 우선순위 레벨 오류와 함께 Firewall 로그에 기록됩니다. 이 매개변수가 지정되지 않으면, 디폴트는 아니오입니다.
14. **패킷 분할 제어** 화살표를 눌러 원하는 패킷 분할 제어를 선택하십시오. 패킷 분할 제어 규칙 스펙과 일치하는 IP 패킷에 대해 제어는 다음과 같이 해석됩니다.

    **예** 규칙은 분할 헤더, 분할부분과 비분할부분을 대응시킵니다. 분할부분에 대해 포트 정보는 무시되고 일치하는 것으로 간주됩니다.

    **전용** 분할부분과 분할부분 헤더만 대응될 수 있습니다. 분할부분 헤더에 대해 포트 정보는 일치해야 합니다. 분할부분에 대해 포트 정보는 무시됩니다.

    **아니오**

    비분할부분만 일치할 수 있습니다. 분할부분 헤더와 분할부분은 이 매개변수에 의해 제외될 수 있습니다.

**헤더** 비분할부분과 분할부분 헤더만 대응될 수 있습니다. 분할부분은 이 매개변수에 의해 제외됩니다.

만일 이 매개변수가 지정되지 않으면, "허용" 규칙과 "거부" 규칙에 대한 디폴트는 예입니다.

**주: 이 제어의 설정값에 관계없이 일(1)의 오프셋을 가진 IP 분할부분은 포기됩니다.** 이 조치는 TCP 헤더 플래그에 겹쳐쓰기 위해 패킷 분할부분을 사용하는 알려진 시스템 공격을 삭제합니다.

패킷 헤더가 정의된 IP 규칙에 일치하기 위해서는 패킷 정보가 코드화된 규칙에 지정된 모든 매개변수와 일치해야 합니다. 패킷 분할부분에 대해 포트 정보를 제외한 모든 매개변수를 사용해서 대응을 판별해야 합니다.

예 또는 전용으로 코드화된 이전 규칙에 의해 분할부분이 허용되지 않으면, 규칙 파일 아래쪽에 항상 첨부 되는 최종 규칙에 의해 거부됩니다.

## IP 규칙 구성 항목 변경

작성한 IP 규칙을 변경하려면, 다음과 같이 하십시오.

1. **규칙 리스트**에서 기존의 규칙을 두 번 누르십시오. **IP 규칙 구성 변경** 대화 상자가 나타납니다.
2. 61페이지의 『제10장 통신량 조절 조정』에서 기술된 대로 적당한 필드를 변경하고 **확인**을 눌러 변경을 적용시키십시오.

## 규칙 구성 항목 삭제

규칙을 삭제하려면 **규칙 리스트**에서 규칙을 선택하고 **삭제**를 누르십시오.

## 사전정의된 서비스

IBM Firewall은 디폴트 서비스 세트로 사전로드됩니다. 서비스는 텔넷 세션과 같이 Firewall을 통해 특정 유형의 통신량을 허용하거나 또는 거부하는 규칙의 집합 또는 일연의 명령입니다. 규칙 템플리트로 새로운 규칙을 작성해서 서비스에 추가할 수 있습니다.

사전로르된 디폴트 서비스는 다음과 같습니다.

**모든 비보안**
비보안 인터페이스를 통하는 모든 통신량 거부

**모두 허용**
모든 통신량 허용(디버깅 용도로만)

**모두 허용, 한 방향으로**
모든 통신량 허용(디버깅 용도로만)

**모든 보안**
보안 인터페이스를 통하는 모든 통신 거부(보안 위반시)

**모든 종료**
모든 패킷 거부(종료 또는 디버그)

**속이기 금지**
보안 출발지 주소를 가진 인바운드 비보안 패킷 거부

**브로드캐스트**
비보안 인터페이스로의 메세지 브로드캐스트 거부

**구성 클라이언트 비보안**
비보안 네트워크로부터 구성 클라이언트의 사용 허용

**구성 클라이언트 보안**
보안 네트워크로부터 구성 클라이언트의 사용 허용

**CU-SeeMe**
디폴트 포트 7649 및 7648상의 CU-SeeMe Video

**DNS 질의**
(보안 규정) DNS 질의 승인

**DNS 전송**
DNS 지역 전송 허용(2차 이름 서버의 경우)

**도메인 제어기 확인**
사용자 확인을 위한 도메인 제어기의 사용 허용

**FTP 프록시 인 1/2**
비보안 네트워크에서 Firewall로의 FTP 인바운드 허용

**FTP 프록시 인 2/2**
Firewall에서 보안 네트워크로의 FTP 인바운드 허용

**FTP 프록시 아웃 2/2**
보안 네트워크에서 Firewall로의 FTP 아웃바운드 허용

**FTP 프록시 아웃 2/2**
Firewall에서 비보안 네트워크로의 FTP 아웃바운드 허용

**고퍼 프록시 인 2/2**
Firewall에서 비보안 네트워크로의 고퍼 허용

**고퍼 프록시 아웃 2/2**
Firewall에서 비보안 네트워크로의 고퍼 허용

**HTTP 거부 비보안**
비보안 인터페이스로의 HTTP 거부

**HTTP 직접 아웃**
보안 네트워크에서 직접 비보안 네트워크로의 HTTP 허용

**HTTP 프록시 인 2/2**
Firewall에서 보안 네트워크로의 HTTP 허용

**HTTP 프록시 아웃 1/2**
보안 네트워크에서 Firewall로의 HTTP(포트 8080) 허용

**HTTP 프록시 아웃 2/2**
Firewall에서 비보안 네트워크로의 HTTP 허용

**HTTPS 직접 아웃**
보안 네트워크에서 비보안 네트워크로의 HTTPS(SSL) 허용

**HTTPS 프록시 아웃 2/2**
Firewall에서 비보안 네트워크로의 HTTPS(SSL 터널) 허용

**IDENTD**
SOCKS 프로토콜을 통한 사용자 식별 허용

**전자우편**
(보안 규정) Firewall을 통한 전자우편 통신량 허용

**NetBT 이름 서비스 브로드캐스트**
TCP/IP 이름 서비스 브로드캐스트를 거친 NetBIOS 허용

**Ping** 모든 위치로의 아웃바운드 보안 네트워크 ping 허용

**SDI 사용자 확인**
보안 네트워크에서 SecurID ACE 서버로의 연결 허용

**Socks 1/2**
보안 네트워크에서 Firewall로의 Socks 사용 허용

**Socks 거부 비보안**
비보안 어댑터로부터의 Socks 거부

**Socks 인 1/2**
비보안 네트워크에서 Firewall로의 Socks 사용 허용

**텔넷 직접 아웃**
보안 네트워크에서 비보안 네트워크로의 텔넷 아웃바운드 허용

**텔넷 프록시 인 1/2**
비보안 네트워크에서 Firewall로의 텔넷 인바운드 허용

**텔넷 프록시 인 2/2**
Firewall에서 보안 네트워크로의 텔넷 인 허용

**텔넷 프록시 아웃 1/2**
보안 네트워크에서 Firewall로의 텔넷 아웃 허용

**텔넷 프록시 아웃 2/2**
Firewall에서 비보안 네트워크로의 텔넷 아웃 허용

**VDOLIVE 다이렉트 인**
보안 서버로의 비보안 클라이언트 허용

UDP 포트 7001만을 사용하도록 사용자들이 개별 재생기 등록정보를 구성해야 한다는 사실을 주목하십시오.

**VDOLIVE 다이렉트 아웃**
비보안 서버로의 보안 클라이언트 허용

**WAIS 프록시 인 2/2**
Firewall에서 보안 네트워크로의 WAIS(z39.50) 허용

**WAIS 프록시 아웃 2/2**
Firewall에서 비보안 네트워크로의 WAIS(z39.50) 허용

## 서비스 정의

규칙(들)을 정의한 후에 규칙(들)을 서비스에 추가해야 합니다. 구성 클라이언트 네비게이션 트리에서 통신량 조절을 선택하고 연결 템플리트를 두 번 누른 후 서비스를 선택하십시오. 서비스 리스트 대화 상자가 나타납니다. 신규를 두 번 눌러 70페이지의 그림 20에 표시된 대로, 서비스 추가 대화 상자를 표시하십시오.

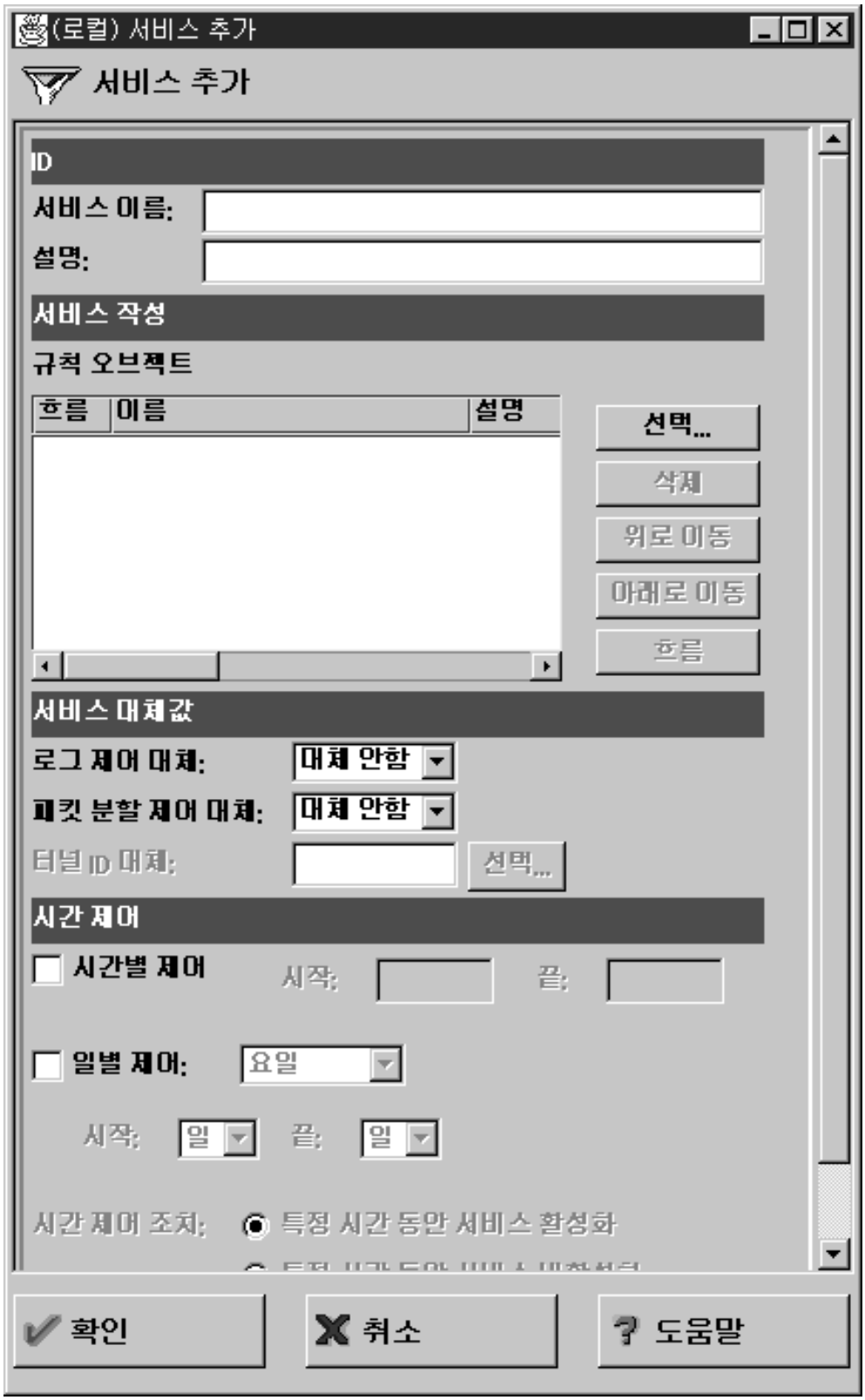
(로컬) 서비스 추가
서비스 추가
ID
서비스 이름:
설명:
서비스 작성
규칙 오브젝트
흐름
이름
설명
선택...
삭제
위로 이동
아래로 이동
흐름
서비스 대체값
로그 제어 대체:
대체 안함
패킷 분할 제어 대체:
대체 안함
터널 ID 대체:
선택...
시간 제어
시간별 제어
시작:
끝:
일별 제어:
요일
시작:
일
끝:
일
시간 제어 조치:
특정 시간 동안 서비스 활성화
확인
취소
도움말

*그림 20. 서비스 추가*

## 서비스를 작성하기 위해 구성 클라이언트 사용

1. 서비스명을 입력하십시오.
2. 설명을 입력하십시오.
3. **로그 제어 덮어쓰기** 필드는 이 서비스에 대해 선택된 규칙 템플리트에서 로그 제어를 덮어쓰는 수단을 제공합니다. 예를 들어, 원래 로그 제어가 아니오로 설정된 규칙 템플리트의 세트를 포함하고 있으면, 이 서비스의 목적을 위해 이 설정값을 예로 대체할 수 있습니다. 대체 설정값은 이 서비스의 모든 규칙에 대해 동작합니다. **로그 제어 덮어쓰기** 필드에 다음 선택 사항중 하나를 입력하십시오.
   - 대체 안함 - 대체는 꺼져 있고 규칙에 있는 설정값 자체가 계속 적용됩니다
   - 예 - 이 서비스에 있는 규칙이 일치하면 로그 레코드를 쓰십시오
   - 아니오 - 이 서비스에 있는 규칙이 일치하면 로그 레코드를 쓰지 마십시오

   로그 레코드가 필터 규칙에 대해 쓰여지면, 로그 레코드에 있는 값이 IP 패킷에서 온 실제값이 됩니다. 로깅 대응 필터 규칙은 Firewall에서 볼 수 있는 실제 프로토콜과 포트 번호와 같은 IP 패킷의 내용에 대한 유용한 정보를 제공합니다.
4. **분할부분 제어 덮어쓰기** 필드는 이 서비스에 대해 선택된 규칙 템플리트에서 패킷 분할 제어 설정값을 덮어쓰는 수단을 제공합니다. 예를 들어, 일반적으로 패킷 분할 제어가 아니오로 설정된 규칙 템플리트의 세트를 포함하고 있는 경우에는 이 서비스의 목적을 위해 이 설정값을 예로 대체할 수 있습니다. 대체 설정값은 이 서비스의 모든 규칙에 대해 동작합니다. 대체 패킷 분할 제어 필드에 다음 중 하나를 입력하십시오.
   - 대체 안함 - 대체는 꺼져 있고 규칙에 있는 설정값 자체가 계속 적용됩니다
   - 예 - 예를 들어, 비분할부분, 분할부분 헤더 그리고 헤더가 없는 분할부분과 같은 모든 IP 패킷을 대응시킵니다
   - 아니오 - 비분할부분 패킷만 대응시키고 분할부분 헤더나 또는 헤더가 없는 분할부분은 대응시키지 않습니다
   - 전용 - 분할부분 헤더와 헤더가 없는 분할부분만 대응시키고 비분할부분은 대응시키지 않습니다
   - 헤더 - 비분할부분과 분할부분 헤더만 대응시키고 헤더가 없는 분할부분은 대응시키지 않습니다
5. 시간 제어는 각 서비스와 시간 범위를 연관시킬 수 있게 합니다. 그러므로, 이 서비스는 지정된 시간 기간 동안만 유효합니다. 만일 서비스에 대한 시간 스펙이 없으면, 그 서비스는 언제든지 유효합니다.

   **하루의 시간별 제어**

   이 서비스를 하루의 시작과 종료 시간에 따라 활성화 또는 비활

성화시키고자 하는지 선택하십시오. 24 시간의 형식을 사용하십시오. 이 필드가 작동 가능하지 않으면, 하루의 시간 필드가 하루 24시간 유효해야 합니다.

**일별 제어**

이 서비스를 요일 또는 달력 날짜에 기초하여 스케쥴에 따라 활성화 또는 비활성화시키고자 하는지 선택하십시오. 서비스가 시간 제어 조치 필드의 값에 따라 활성화되었는지 아니면 비활성화되었는지 주의하십시오.

**시간 제어 조치**

이 서비스를 지정된 시간중에 활성화시키려면, **지정된 시간중 서비스 활성화**를 선택하십시오. 이 서비스는 지정된 시간외에는 비활성화됩니다.

이 서비스를 지정된 시간중에 비활성화시키려면, **지정된 시간중에 서비스 비활성화**를 선택하십시오. 이 서비스는 지정된 시간 외에는 활성화됩니다.

6. **선택**을 눌러 이 서비스를 구성하는 규칙을 선택하십시오.
7. 흐름 토글 단추를 사용하여 규칙 기본 파일에 기록된 것과 같이 연결의 출발지 및 목적지 값이 필터에 어떻게 할당되어야 하는지를 결정하십시오.

   **--->** 왼쪽에서 오른쪽은 연결이 규칙 기반 파일에 쓰여지면서 출발지와 목적지가 규칙에 직접 쓰여진다는 것을 나타냅니다.

   **<---** 오른쪽에서 왼쪽은 연결이 규칙 기반 파일에 쓰여질 때 출발지와 목적지가 역순이 된다는 것을 나타냅니다.

8. 패킷이 수신되면 IBM Firewall은 패킷에 있는 정보를 파일 맨 위에서 시작하는 규칙 구성 파일에 있는 규칙과 비교합니다. 첫번째로 정확하게 일치하는 것을 찾아 규칙에 있는 조치를 수행하면 비교를 멈춥니다.

   일단 서비스에 일련의 규칙을 추가했다면, 그 순서를 변경할 수 있습니다. **서비스 오브젝트** 리스트에서 규칙을 선택하고 **위로 이동**이나 **아래로 이동** 단추를 눌러 규칙을 재배치하십시오. 또는 **삭제**를 눌러 규칙을 삭제할 수 있습니다. 구성 클라이언트는 최신 것으로 고쳐진 규칙의 리스트를 표시합니다. **확인**을 눌러 변경사항을 저장하십시오.

# 제11장 Socks 서버 구성

Socks는 회선 레벨 게이트웨이에 대한 인터넷 표준입니다. 웹 브라우저, FTP 또는 텔넷 응용 프로그램과 같은 프로그램이 TCP를 사용하는 경우 주소 변환을 위해 Socks 서버를 사용하게 됩니다. Socks는 내부 IP 주소를 감추면서 인터넷에 액세스하는 데 도움을 줄 수 있습니다.

보안 클라이언트에서 비보안 서버로의 아웃바운드 요청의 경우, Socks 서버에는 프록시 서버와 동일한 목표가 있어 Firewall에서 세션을 중단하고 내부 네트워크의 주소 처리방식 및 구조를 보호하는 동안 외부의 비보안 네트워크에 사용자가 액세스할 수 있는 보안 도어(door)를 제공합니다. Socks 서버는 추가적인 관리 작업이 없어도 사용자가 간단히 작업할 수 있게 해줍니다.

Socks 서버는 네트워크와 인터넷 간을 통과하는 모든 아웃바운드 TCP 요청을 가로챌 수 있습니다. socks 서버는 보안 도메인의 클라이언트 프로그램이 실행하는 기능들이 Firewall 워크스테이션의 보안 서버를 통해 파이프되어 클라이언트의 IP 주소를 감출 수 있도록 원격 응용 프로그램 인터페이스를 제공합니다. SOCKS 규칙과 관련된 필터에 의해 액세스가 제어됩니다.

Socks 서버는 프록시 서버와 유사합니다. 그러나 프록시 서버가 실제로 Firewall에서 TCP/IP 기능을 수행하는 반면 Socks 서버는 단지 시용자를 식별하고 Firewall을 통하는 기능의 경로를 재지정해 줍니다. 실제 TCP/IP 기능은 Firewall이 아닌 클라이언트 워크스테이션에서 수행됩니다. 이를 통해 Firewall에서의 프로세싱이 줄어듭니다. 보안 네트워크의 사용자는 SOCKS 표준을 지원하는 많은 TCP/IP 제품을 사용할 수 있습니다. 그림 21는 보안 네트워크 내의 클라이언트로부터 나오는 HTTP 요청을 가로채는 socks 서버를 보여줍니다.

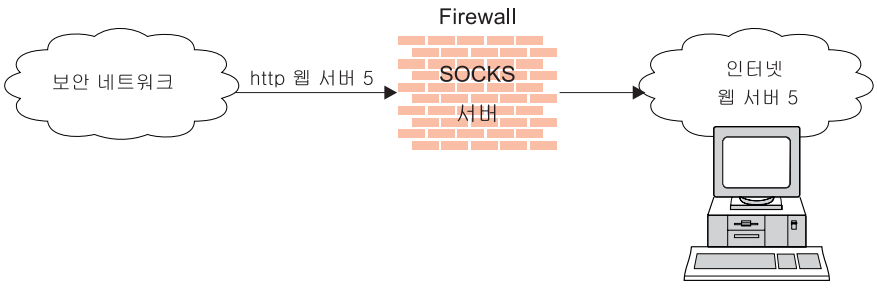


*그림 21. Socks 서버*

socks 서버는 외부로부터 사용자의 내부 IP 주소를 효과적으로 숨겨줍니다.

IBM Firewall은 비보안 네트워크에서 응용 프로그램에 액세스하기 전에 보안 네트워크 내의 클라이언트가 사용자 확인 단계를 통과할 수 있게 하는

Socks 프로토콜 버전 5를 제공합니다. 또한 확인된 범용 프록시와 일부 스트리밍 오디오 및 비디오 프로토콜에 대한 프록시를 제공하기도 합니다.

Socks 디먼은 시스템 시작시 자동으로 시작하여 Windows NT 서비스로 실행됩니다. 또한 서버의 모니터링을 위해 Watch 에이전트가 제공됩니다. 수작업으로 감시 에이전트(Watch Agent)를 시작할 수 있습니다.

IBM Firewall은 고객들이 Socks 클라이언트를 도입할 때 설치되어 있던 Socks 프로토콜 버전4 클라이언트를 계속 사용할 수 있도록, 세 가지 사용자 확인 프로파일 형태로 편리한 이주 경로를 제공합니다.

1. 대부분의 허용되는 프로파일에서는 아웃바운드 사용자 확인이 작동되지 않으며, 연결에 Socks 프로토콜 버전 4나 Socks 프로토콜 버전 5 클라이언트 중 어떤 것을 사용하는지에 관계없이, 모든 사용자를 허용합니다. 이 시나리오에서 인바운드 연결은 거부됩니다.
2. 이주 프로파일을 사용하면 Socks 프로토콜 버전 4 사용자들은 확인을 거치지 않고 통과될 수 있으나, Socks 프로토콜 버전 5 사용자의 경우 확인이 요구됩니다. 사용자 확인에 있어 인바운드 Socks 프로토콜 버전 4 연결은 거부되고, 인바운드 Socks 프로토콜 버전 5 연결이 요구됩니다. 이것은 디폴트 프로파일입니다.
3. 모든 사용자가 Socks 클라이언트를 사용하고 유효한 사용자 확인을 제공하도록 요구하는 프로파일이 가장 안전한 프로파일입니다.

Firewall이 설치되면 Socks 서버는 작동 가능해지지만 Socks 구성 파일에는 규칙이 없는 상태입니다. Socks 클라이언트가 Socks 서버를 사용하기 위해서는 구성 클라이언트를 사용해서 Socks를 구성해야 합니다. Socks 서비스 설정 방법에 대한 예를 보려면 58페이지의 『Socks의 예제』를 참고하십시오.

## Socks 프로토콜 버전 5 서버가 지원하는 프로토콜

Socks 프로토콜 버전 5서버는 다음과 같은 TCP와 UDP 프로토콜 및 그외 다수를 지원합니다.

- Archie
- 핑거
- FTP
- Gopher
- HTTP
- HTTP 프록시
- News
- SNMP
- 텔넷
- TFTP
- RealAudio

- RealPlayer
- Whois
- X-Windows

추가적으로 대부분의 e-mail 클라이언트가 지원됩니다. 이러한 프로토콜에 대한 지원 여부는 프로토콜의 실제 구현 상태에 따라 달라집니다.

## 구성 클라이언트를 사용하여 Socks 서버 구성

Socks 템플리트는 Socks 서버를 통해 보안을 제어하는 규칙입니다. SOCKS 템플리트를 사용하면 기존의 SOCKS 템플리트를 조정, 기존 템플리트에 추가 또는 삭제할 수 있습니다. 이러한 Socks 템플리트는 차례로 규칙 템플리트가 사용되는 동일한 방법으로 Firewall상의 연결 정의에서 사용될 수 있습니다.

### 새로운 Socks 규칙 추가

SOCKS 구성 파일에 규칙을 추가하려면 구성 클라이언트가 제공하는 SOCKS 템플리트를 사용하여 구성 클라이언트 네비게이션 트리에서 통신량 조절을 선택하십시오. 파일 폴더 아이콘을 두 번 눌러서 보기를 확장하십시오. 연결 템플리트를 선택하십시오. 파일 폴더 아이콘을 두 번 눌러서 보기를 확장하십시오. **Socks**를 선택하십시오. **Socks** 대화 상자가 나타납니다.

1. **신규**를 두 번 눌러 새로운 Socks 템플리트를 추가하십시오.

   76페이지의 그림 22에서 보여 주는 바와 같이 **Socks 규칙 추가** 대화 상자가 나타납니다.


*그림 22. Socks 규칙 추가*

2. **템플리트명** 필드에 Socks 항목의 이름을 입력하십시오. 이 이름은 고유해야 하며 파일 분리자로 사용될 수 있는 파이프 기호(|), 작은따옴표(또는 어포스트로피) (') 또는 큰따옴표(")가 포함되면 안됩니다. 이런 문자를 사용하면 신뢰할 수 없는 데이터를 초래할 수 있습니다.
3. 설명을 채우십시오.
4. 조치 화살표를 누른 후, 출발지에서 목적지로의 액세스를 허용하거나 거부하도록 선택하십시오.

   데이터그램이 Socks 서버에서 수신되면, 서버는 데이터그램 스펙을 구성 파일의 첫 규칙을 시작으로 정확하게 일치하는 규칙을 찾을 때까지 각 규칙과 비교합니다. 그리고 나서, 찾기를 정지하고 그 규칙과 관련된 조치(액세스 허용 또는 거부)를 수행합니다. 만일 일치하는 것을 찾지 못하면, 액세스는 자동으로 거부됩니다.
5. **사용자 리스트** 필드에 사용자 ID나 사용자 ID 리스트를 입력할 수 있습니다. 리스트를 입력할 때는 항목을 쉼표로 분리하십시오. 사용자 리스트에서 공백, 탭, 파이프 기호(|) 또는 큰따옴표(")를 사용하지 마십시오.
   - 사용자 리스트는 396 문자로 제한됩니다.
   - 사용자 ID는 요청하는 호스트의 사용자 ID어야 하며 목적지 호스트나 또는 Socks 서버 호스트의 것은 안됩니다.
   - 사용자 ID는 다음을 포함한 1에서 8개의 문자로 구성됩니다.
     – a에서 z
     – A에서 Z

- 0에서 9
- _(밑줄)

6. 사용자 ID는 파이프 기호(|) 이중 따옴표 문자(″)가 포함될 수 없습니다.
7. 만일 파일명이 사용되면, 이는 완전히 규정되어야 합니다(선행 ″/″를 사용해서 사용자 ID로 해석되는 것을 방지합니다). 각 파일은 쉼표로 분리되어 있으며 선택적으로 # 문자로 구분되는 주석을 포함하는 한 행당 한 개 이상의 사용자 ID 리스트를 포함할 수 있습니다. # 문자로 시작하는 완전한 주석 행도 지원됩니다. 파일의 각 행은 최대한 1023 문자까지 가능하며 ″개행문자(newline)″로 종료되어야 합니다.
8. **조작** 필드에, 포트 번호에서 수행될 논리 조작을 입력하십시오.

   **eq** 같음

   **neq** 같지 않음

   **lt** 보다 작음

   **gt** 보다 큼

   **le** 작거나 같음

   **ge** 크거나 같음

   포트 번호에 사용할 경우, 논리 조작은 만족해야 하는 관계를 설정합니다. 예를 들어, 조작 gt와 포트 번호 23을 입력하면, 포트 번호는 호출되는 규칙에 대해 23보다 커야 합니다.
9. **포트 #** 필드에, 포트 번호를 입력하십시오. 포트 번호는 만족해야 하는 관계를 설정하기 위해 조작에 사용됩니다. 예를 들어, 조작 gt와 포트 번호 23을 입력하면, 포트 번호는 호출되는 규칙에 대해 23보다 커야 합니다. 조작 및 포트 번호가 생략되면, 규칙은 모든 목적지 포트 번호에 적용됩니다.

이 **Socks 규칙 추가** 대화 상자를 사용하여 IP 주소에 근거하여 네트워크 호스트에 대한 Firewall 액세스를 허용하거나 거부할 수 있습니다.

## Socks 규칙 변경

1. **Socks** 대화 상자를 두 번 누르십시오.

   **Socks 규칙 변경** 대화 상자가 나타납니다.
2. 75페이지의 『새로운 Socks 규칙 추가』에서 기술된 대로 해당 필드를 변경하고 **확인**을 누르십시오.

## Socks 규칙 삭제

**Socks** 대화 상자에서 항목을 선택한 후, **삭제**를 누르십시오. 이 Socks 규칙을 정말로 삭제하고 싶은지 확인합니다. **확인**을 눌러 규칙을 삭제하십시오.

### 연결 규칙 활성화

필터 규칙에 대해 Socks 규칙을 활성화시켜야 합니다. 구성 클라이언트 네비게이션 트리에서 **연결 활성화**를 누르고 **연결 규칙 재생성 및 활성화**를 선택한 후 **실행**을 누르십시오.

Firewall은 Socks 구성 파일에서 Firewall 규칙으로 규칙을 복사하고 규칙을 활성화시킵니다. 규칙이 활성화되면 새로운 규칙은 Firewall 로그 파일에 기록됩니다.

### Socks에 대한 샘플 로깅 출력

다음은 Socks에 대한 로깅 출력의 샘플입니다.

```
Feb 03 13:46:20 1998 mr16n18: ICA3123i: Sockd 서버가 시작되었습니다.
Feb 03 13:47:31 1998 mr16n18: ICA3010i: 세션이 시작되었습니다.
Feb 03 13:47:31 1998 mr16n18: ICA3011i: 세션이 시작되었습니다.
Feb 03 13:49:15 1998 mr16n18: ICA3007i: 쓰레드가 너무 많습니다.
Feb 03 13:58:31 1998 mr16n18: ICA3015i: 세션이 종료했습니다.
```

### Socks 서버를 사용하기 위한 클라이언트 고려사항

대부분의 Web 브라우저는 Socks를 준수하며 거의 모든 플렛폼에 대해 Socks를 준수하는 스택을 확보할 수 있습니다. 기타 TCP/IP 응용 프로그램에 대한 Socks-준수 클라이언트는 많은 소스에서 사용 가능합니다. Socks가 구현하는 특정 클라이언트에 대해 클라이언트 문서를 참조하십시오. 추가 정보에 대해서는 다음을 참조하십시오.

http://www.raleigh.ibm.com/sng/sng-socks.html

http://www.socks.nec.com

## Socks-서버 변경

Socks-서버 변경이란 하나의 Socks 서버가 다른 Socks 서버 뒤에 있을 수 있는 피처로서, 그래도 여전히 가장 바깥쪽의 Socks 서버 너머의 네트워크로 액세스 할 수 있습니다. (이것은 Socks 서버의 Socks화로 생각할 수도 있습니다). 이는 매우 유용한 인트라넷 시나리오입니다.

Socks 서버에 Socks-서버 체인을 설정하려면 `socks5.header.cfg` 파일을 편집하십시오. 이 파일은 Firewall의 `config` 서브디렉토리에 있습니다. 이 파일에 다음을 추가하십시오.

- *no proxy* 지정문 - 사용자의 Firewall이 직접 액세스 하는 서브네트를 나타냅니다.
- *socks4* 지정문 - Socks 프로토콜 버전 4 서버를 통해 액세스 할 수 있는 서브네트를 나타냅니다.
- *socks5* 지정문 - Socks 프로토콜 버전 5 서버를 통해 액세스 할 수 있는 서브네트를 나타냅니다.

예를 들어 다음의 네트워크를 고려해 보십시오. 연구 부서에서는 Firewall 뒤에 *q.private.com*이라는 작은 개별 네트워크를 가지고 있습니다. 연구 부서의 서브네트는 10.007.007.0/255.255.255.0입니다. 이 회사의 개별 네트워크인 *private.com*에는 전체 10.0.0.0/255.0.0.0 네트워크가 들어 있습니다. 회사의 Socks 프로토콜 버전 4 서버인 *socks.private.com*에서는 인터넷에 대한 액세스를 제공합니다.

연구 부서의 Socks 서버인 *socks.q.private.com*에서 다음의 두 행을 socks5.header.cfg에 추가하십시오.

```
no proxy 10.0.0.0/255.0.0.0 - - -
socks4      0/0   - socks.private.com 1080
```

마지막으로 통신량 조절 연결을 추가하여, *socks.q.private.com*이 *socks.private.com*과 통신할 수 있도록 하십시오. 이는 더 일반적인 서비스에 의해 이미 수행되어 있을 수도 있습니다. 소스가 *q.private.com* Firewall의 비보안 인터페이스이고, 목적지가 *socks.private.com*이며, *Socks 프록시-변경* 서비스를 포함하고 있는 연결을 추가하십시오. 그리고나서 통신량 조절 규칙을 재활성화 하십시오.

# 제12장 Firewall에서 사용자 관리

이 장에서는 다음을 포함하여 IBM Firewall을 사용하여 매일의 관리 작업을 수행하는 방법에 대해 설명합니다.

- 사용자가 보호된 네트워크 외부의 호스트에 액세스할 수 있도록 IBM Firewall에 사용자 추가
- Firewall을 액세스하는 사용자의 속성 변경
- 네트워크 밖에서 더 이상 액세스할 필요가 없는 사용자 삭제

구성 파일을 직접 편집하지 마십시오. 이렇게 할 경우, IBM Firewall 사용자 속성은 올바로 설정되지 않습니다. 구성 클라이언트 대화 또는 명령 행을 사용하여 모든 IBM Firewall 관리를 실행하십시오.

## IBM Firewall에 사용자 추가

IBM Firewall은 세 가지 유형의 사용자를 정의하며 두 개의 다른 사용자 데이터베이스에 이들 사용자에 대한 정보를 저장합니다.

### 사용자 유형

IBM Firewall은 사용자들을 다음의 세 범주로 구분합니다.

**프록시 사용자**
HTTP 프록시 서비스와 같은 fierwall 서비스를 사용하여 기업 네트워크 내부로부터 인터넷상의 웹 사이트를 액세스합니다. 프록시 사용자는 Firewall을 통해 서비스를 사용할 수 있으나 Firewall 시스템에 대한 액세스 권한이 없으며 Firewall 시스템으로의 로컬 로그인을 수행할 수 없습니다.

**Firewall 관리자**
이들은 Firewall 프록시 서비스를 사용할 수 있으며, 구성 클라이언트를 사용하고 원격 호스트로부터 Firewall로 로그온하여 Firewall을 구성할 수도 있습니다. 프록시 사용자와 마찬가지로, Firewall 관리자도 Firewall 시스템으로의 로컬 로그인을 수행할 수 없습니다.

Firewall 관리자는 프록시 사용자에 대한 정의를 작성하고 변경할 수 있으나 다른 Firewall 관리자의 정의를 작성하거나 변경할 수는 없습니다.

**1차 Firewall 관리자**
Firewall 관리자와 동일한 기능을 가집니다. 또한 Firewall 시스템으로의 로컬 로그인을 수행할 수도 있습니다. 1차 Firewall 관리자는 다른 Firewall 관리자에 대한 정의를 작성하고 변경할 수 있습니다.

### 데이터베이스 유형

사용자 데이터베이스에는 두 가지 유형이 있습니다.

**Firewall 사용자 데이터베이스**

각 프록시 사용자 및 관리자마다의 Firewall 관련 속성이 포함되어 있습니다. 사용자의 Firewall 암호 및 암호 규칙과 같은 속성 및 사용자 확인 방법이 각 서비스마다 사용자를 확인하는 데 사용되어야 속성이 포함됩니다.

프록시 사용자가 Firewall 사용자 데이터베이스에 정의되어 있지 않은 상태에서 사용자가 Firewall 프록시 서비스를 사용하려 하면 사용자의 유효성을 검증하는 데 사용되는 속성과 사용자 확인 스킴(scheme)을 정의할 때 디폴트 사용자 레코드인 `fwdfusr`이 사용됩니다.

1차 Firewall 관리자가 Firewall 사용자 데이터베이스에 정의될 수 없습니다. 디폴트 Firewall 관리자 레코드 `fwdfadm`을 사용하여 관리자에게 속성을 지정할 수 있습니다.

프록시 사용자와 마찬가지로, Firewall 관리자가 Windows NT 사용자 데이터베이스에도 정의되어 있는 경우, 사용자가 NT 로그온 암호를 사용하여 확인해야 하는 서비스를 요청할 때 그 NT 로그온 암호가 사용됩니다.

**Windows NT 사용자 데이터베이스**

사용자에 대한 NT 로그온 암호가 들어 있습니다. 일반적으로, 프록시 사용자는 그 NT 로그온 암호를 사용하여 확인되지 않는 한, NT 사용자 데이터베이스에 정의될 필요가 없습니다.

다른 사용자 확인 방법이 프록시 사용자를 확인하는 데 사용되려면, 이들이 Windows NT 사용자 데이터베이스에 정의되어서는 안 됩니다.

1차 Firewall 관리자는 NT 관리자 그룹의 멤버인 Windows NT 사용자의 동의어이며, Windows NT 사용자 데이터베이스에 정의되어야 합니다.

## 구성 클라이언트를 사용한 사용자 추가

IBM Firewall에 사용자를 추가하면, 이들은 외부 네트워크에 액세스할 수 있습니다.

1. 구성 클라이언트 네비게이션 트리에서 사용자를 선택하십시오. **사용자 관리** 대화 상자가 나타납니다.
2. **사용자 관리** 대화 상자에서 **신규**를 선택하고 **열기**를 누르십시오. 83페이지의 그림 23에서 보여 주는 바와 같이 **사용자 추가** 대화 상자가 나타납니다.


*그림 23. 사용자 추가*

3. 다음과 같은 정보를 제공합니다.

**권한 레벨**

이 사용자에 대한 권한 수준을 지정하십시오. **권한 레벨** 화살표를 눌러 사용자 유형을 선택하십시오.

**Socks/Proxy 사용자**

정의되는 사용자가 Socks 서버 액세스와 프록시 액세스 모두를 위한 것입니다. 이 사용자에게는 관리 권한이 없습니다. 이는 디폴트입니다.

**Firewall 관리자**

관리자는 사용자의 모든 속성을 가지지만 Firewall로 로그인할 수 있으며 관리 작업을 수행할 수 있습니다. 관리자는 수행하도록 허용된 관리 기능을 정의해주는 추가 속성을 가집니다. Firewall 관리자는 Firewall 사용자를 작성할 수 있으나 다른 Firewall 관리자를 작성할 수는 없습니다. Firewall 관리자는 Firewall 시스템으로 로컬 로그인할 수 없습니다. 원격 시스템으로부터 구성 서버에 액세스해야 합니다.

**1차 Firewall 관리자**

1차 Firewall 관리자는 Firewall 시스템으로의 로컬 로그인이 허용됩니다. 이 관리자는 모든 관리 기능에 대한 완전한 액세스 권한을 가집니다. 또한 1차 Firewall 관리자를 제외한 다른 Firewall 관리자를 작성할 수 있습니다.

1차 Firewall 관리자는 NT 데이터베이스에 사용자를 작성하고 이 사용자가 NT 관리자 그룹의 멤버가 되게 함으로써 정의됩니다. fwdfadm 레코드를 변경하여 1차 Firewall 관리자에 대한 속성을 정의하십시오.

**사용자 이름**

이 사용자에 대한 이름을 지정합니다. 이는 이 사용자가 IBM Firewall의 텔넷 또는 FTP 서버로 로그하는 사용자 이름입니다. 이는 사용자 TCP/IP 사용자 이름 또는 호스트 이름일 필요는 없지만 같을 수 있습니다.

사용자 이름은 다음을 포함하는 1 내지 20자로 구성될 수 있습니다.

a에서 z

A에서 Z

0에서 9

_ (밑줄)

사용자 이름은 대소문자를 구분하지 않습니다.

Firewall은 두 개의 사전설치된 사용자와 함께 공급됩니다.

a. 디폴트 사용자 또는 fwdfuser. 사용자가 Firewall 데이터베이스에 정의되어 있지 않으면 사용자를 확인할 때 사용할 확인 방법과 같은 사용자의 Firewall 속성을 결정하는 데 fwdfuser이 사용됩니다.

   설치시 fwdfuser가 작성되면 모든 사용자 확인 방법이 모두 거부로 설정됩니다. fwdfuser 는 Firewall이 정의되지 않은 사용자명을 처리하는 방법을 제어합니다.

   관리자는 구성 클라이언트 또는 명령 행을 사용해서 fwdfuser를 열람하거나 또는 지정된 사용자 확인 방법을 변경할 수 있습니다. 그러나, fwdfuser는 삭제될 수 없으며 항상 Firewall에

있어야 합니다. 또한 Firewall 암호와 SNK는 fwdfuser에 대한 유효한 사용자 확인 유형이 아닙니다. 자세한 내용은 *IBM eNetwork Firewall 참조서*를 참조하십시오.

b. 디폴트 1차 Firewall 관리자 fwdfadm은 모든 1차 Firewall 관리자에 대한 Firewall 속성을 정의합니다. 1차 Firewall 관리자의 자체의 사용자 레코드가 Firewall 데이터베이스 내에 없으므로 1차 Firewall 관리자를 확인하는 데 사용되는 사용자 확인 방법을 정의하는 데 이 레코드가 사용됩니다.

   설치시, NT 로그온 암호로 설정되는 보안 및 비보안 관리 확인 방법을 제외한 fwdfadm에 대한 모든 사용자 확인 방법은 모두 *거부*로 설정됩니다. 1차 Firewall 관리자는 이 레코드를 보고 수정할 수 있으나 삭제할 수는 없습니다. 이 외에도, Firewall 암호와 SNK는 fwdfadm에 대해 유효한 사용자 확인 유형이 아닙니다.

**사용자 전체 이름**
사용자의 설명을 지정합니다.

다음 필드는 사용자 확인 방법을 참조합니다. 화살표를 눌러 사용자 확인 벙법 리스트에서 선택하십시오. 이는 86페이지의 『사용자 확인 방법』에서 설명됩니다.

**보안 텔넷**
보안 네트워크에서 로그인할 때 이 사용자 신원을 일부 수단에 의해 확인되어야 하는지를 나타냅니다.

**비보안 텔넷**
비보안 네트워크에서 로그인할 때 이 사용자 신원을 일부 수단에 의해 확인되어야 하는지를 나타냅니다.

**보안 FTP**
이 사용자가 비보안 네트워크에서 Firewall을 액세스하기 위해 FTP를 사용할 때 필요한 사용자 확인 수준을 지정합니다.

**비보안 FTP**
이 사용자가 비보안 네트워크에서 Firewall을 액세스하기 위해 FTP를 사용할 때 필요한 사용자 확인 수준을 지정합니다.

**보안 SOCKS**
Firewall의 보안 부분에서 시작된 SOCKS 클라이언트 연결에 대한 Socks V5 사용자 확인 방법을 지정합니다. 화살표를 눌러 선택사항 리스트에서 선택하십시오. 이는 86페이지의 『사용자 확인 방법』에서 설명됩니다.

**비보안 SOCKS**
Firewall의 비보안 부분에서 시작된 SOCKS 클라이언트 연결에 대한 Socks V5 사용자 확인 방법을 지정합니다. 화살표를 눌러 선택 사항 리스트에서 선택하십시오. 이는 86페이지의 『사용자 확인 방법』에서 설명됩니다.

**보안 HTTP**

아웃바운드 HTTP 프록시 요청에 대한 사용자 확인 방법의 사용자 ID/암호 유형을 지정합니다. 화살표를 눌러 선택 사항 리스트에서 선택하십시오. 이는 86페이지의 『사용자 확인 방법』에서 설명됩니다.

브라우저가 사용자 ID와 암호에 대한 프롬프트를 표시하므로, SDI를 사용중일 경우, 암호 프롬프트에 passcode를 채우십시오.

사용자 제공은 Socks/암호가 대화식 다이얼로그를 지원할 수없으며 이에 따라 활동할 수 없다는 것을 인식해야 합니다.

**보안 관리**

보안 인터페이스를 통해 구성 클라이언트에서 로그온할 때 사용되는 사용자 확인 방법을 지정합니다. 로컬적으로 로그온(로그온 패널에서 로컬을 선택해서)할 때 사용자는 항상 보안 환경에 있으므로 이 사용자 확인 방법을 사용하게 됩니다.

**비보안 관리**

비보안 인터페이스를 통해 구성 클라이언트에서 로그온할 때 사용되는 사용자 확인 방법을 지정합니다.

**SecureNet 키**

AssureNet Pathways SecureNet 키 카드를 가지고 있는 원격 사용자에 의해 입력된 문자 순서를 지정합니다. 키 카드를 준비하기 위해서도 가지고 있어야 하는 키 코드를 입력하십시오. 키 코드를 선택하고 설치하는 명령에 대해 SecureNet 키 정보를 참조하십시오.

**주:**

a. 이 필드는 SecurID 카드에 대해 사용되지 않습니다.

b. 각 사용자에 대해 고유한 임의의 키를 작성해야 합니다.

c. 키를 SecureNet 키 카드에 설치할 때 AssureNet Pathways 설치 프로시듀어를 사용하고 **모드 5**를 선택하십시오.

자세한 내용은 90페이지의 『사용자 확인 방법』을 참조하십시오.

## 사용자 확인 방법

사용자 확인에 대한 선택은 다음과 같습니다.

**모두 거부**

사용자는 거부된 액세스입니다.

**모두 허용**

사용자 확인이 필요 없습니다.

**NT 로그온 암호**

NT 로그온 암호는 Firewall 암호보다 보안 기능이 더 약합니다. 그

러나 사용자가 Windows NT 도메인에 이미 정의되어 있으면 복수의 암호가 필요하지 않도록 Windows NT 로그온 암호를 사용할 수 있습니다.

이 사용자 확인 방법을 선택하면, 사용자 ID와 암호는 로컬 Windows NT 사용자 데이터베이스에 비교하여 유효성이 검증됩니다. Firewall이 다른 Windows NT 서버를 수탁하도록 구성되면 이들 수탁된 서버에서 사용자 정의들이 탐색됩니다.

Windows NT Firewall과 위탁된 Windows NT 서버간의 위탁 관계가 설정되려면, 먼저 두 시스템간에 TCP/IP 통신 소통이 허용되도록 연결이 설정되어야 합니다.

다음 사전정의된 서비스를 사용하여 이 연결을 설정하십시오.

1. 도메인 제어기 사용자 확인 - 사용자 확인을 위한 도메인 제어기의 사용을 허용
2. NetBT 이름 서비스 브로드캐스트 - NetBIOS over TCP/IP 이름 서비스 브로드캐스트 허용

Windows NT 구성 유틸리티를 사용하여 위탁 관계를 정의하십시오.

**SecureNet 키**

사용자 확인은 AssureNet Pathways사의 SecureNet 키를 사용해서 이루어집니다.

SecureNet 키 필드에서 SecureNet 키 카드를 준비하기 위해서도 가지고 있어야 하는 키 코드를 입력하십시오.

**주:**

1. 각 사용자에 대해 고유한 임의의 키를 작성해야 합니다.
2. 임의의 키 범위는 8진수 값마다 1–377이어야 합니다.
3. 키를 SecureNet 키 카드에 설치할 때 AssureNet Pathways 설치 프로시듀어를 사용하고 **모드 5**를 선택하십시오.

자세한 내용은 90페이지의 『사용자 확인 방법』을 참조하십시오.

**SecurID 카드**

사용자 확인은 Security Dynamics사 SecurID 보안 카드 또는 핀패드 카드를 사용해서 이루어집니다. SecureNet 키 필드를 사용하지 *마십시오*. PIN은 이 사용자 확인 방법을 IBM Firewall과 함께 사용하기 전에 설정되어야 합니다.

FTP에 대해 SDI 신규 PIN 모드와 다음 토큰 모드가 지원되지 않습니다.

자세한 내용은 90페이지의 『사용자 확인 방법』을 참조하십시오.

**사용자 제공 사용자 확인 1, 2 및 3**

사용자 확인은 사용자에 의해 제공됩니다. Firewall에 세 개까지의 사용자 제공 사용자 확인 방법을 설치할 수 있습니다. 사용자 제공 사용자 확인을 위한 서브루틴을 작성하고 컴파일하는 데 대한 방법은 *IBM eNetwork Firewall 참조서*를 참조하십시오.

**Firewall 암호**

사용자는 유효한 암호를 위해 프롬프트되고 또한 이를 입력해야 합니다. 이 패널이 완료되면, IBM Firewall은 이 신규 사용자를 위해 암호를 지정하도록 프롬프트합니다.

Firewall 암호는 Windows NT 로그온 암호 보다 더 안전한 암호 및 암호 규칙을 허용하므로 권장되는 암호 선택사항입니다.

**사용자에게 변경 요청**

사용자가 확인되는 다음 번에 그 암호를 변경하도록 요청할지 여부를 지정하려면 예나 아니오를 누르십시오.

**암호 잠금**

암호 잠금 여부를 지정하려면 예나 아니오를 누르십시오. 최대 실패 로그인 회수가 초과되거나 잠금 이전 최대 시간에 지정된 주수에 이 암호가 사용되지 않았을 때 이 항목은 예로 설정됩니다.

관리자는 사용자가 암호 확인을 사용하지 못하도록 이 필드를 예로 설정할 수 있습니다.

**주:**

1. 암호는 대소문자를 구분합니다. 만일 대소문자가 혼합된 사용자 암호를 입력하면, 사용자는 암호를 정확하게 입력해야 합니다. 워크스테이션이 대문자로만 작업하는 경우에는 이런 사용자에 대한 암호를 대문자로 입력하십시오.
2. 운영체제가 암호 규칙을 정의할 수 있게 합니다. 이러한 암호 규칙은 사용자가 자신의 암호를 변경하지만 관리자는 암호 변경을 하지 않을 때에 적용됩니다. 암호 규칙은 다음과 같습니다.

   **만기 이전 경고 일 수(일 단위)**

   Firewall이 사용자에게 암호 변경 옵션을 제공하는 암호 만기 이전의 일 수.

   **만기 이전 최대 주 수**

   사용자에게 암호 변경을 요구하기 이전 주 수.

   **잠기기 이전 최대 주 수**

   암호가 잠기기 이전 사용되지 않는 주 수.

   **최대 허용 로그인 재시도 회수**

   암호가 잠기기 이전 허용되는 최대 실패 로그인 회수.

   **재사용 이전 암호**

   암호 이력 리스트에 저장된 암호의 수. 암호는 현재 이력 리스트에 있는 암호로는 변경될 수 없습니다. 이 매개변수는 암호 재사용 이전 주 수가 0으로 설정된 경우에만 유효합니다.

   **암호 재사용 이전 주 수**

   암호 이력 리스트에 암호가 보유되는 주 수. 암호는 현재 이력 리스트에 있는 암호로는 변경될 수 없습니다.

**최소 길이**
암호에 있는 최소 문자 수.

**최소 영문자 문자**
암호에 있는 최소 영문자 문자 수.

**최소 기타 문자**
암호에 있는 최소 비 영문자 문자 수.

**최대 반복 문자**
암호에서 한 문자가 반복될 수 있는 최대 회수.

**최소 다른 문자**
암호에 있는 다른 문자의 최소 수.

**Firewall 암호** 탭을 눌러 각 사용자에 대해 이러한 값들을 조정하십시오.

## 사용자의 액세스 변경

Firewall에 사용자를 추가한 후에는 **사용자 변경** 대화 상자에서 해당 사용자의 보안 속성을 변경할 수 있습니다.

1. **사용자** 대화 상자에서 변경하고자 하는 사용자를 선택하고 **열기**를 누르십시오.
2. **사용자 변경** 대화 상자가 나타나면, 해당 필드를 변경하십시오. 변경할 수 있는 사용자 속성 리스트에 대해 81페이지의 『IBM Firewall에 사용자 추가』를 참조하십시오.
3. 변경을 했으면, **확인**을 누르십시오.

## IBM Firewall에서 사용자 삭제

**주:** 사용자 `fwdfuser` 또는 `fwdfadm`을 삭제하지 마십시오.

사용자를 삭제하려면, **사용자 리스트** 패널에서 **삭제**를 누르십시오.

## 기능에 의한 관리자 권한 레벨

*1차 Firewall 관리자*만이 관리자를 작성하고 변경할 수 있으며, 이들에게 권한이 있는 Firewall 기능을 판별할 수 있습니다. 예를 들어, 사용자 및 로그 모니터 기능을 수행할 수 있는 권한만을 가지도록 특정 관리자를 제한할 수 있습니다.

**사용자 추가** 대화 상자에서, **권한 레벨** 필드에 Firewall 관리자를 선택하십시오. **사용자 추가** 대화 상자를 완료하는 데 대한 자세한 내용은 81페이지의 『IBM Firewall에 사용자 추가』를 참조하십시오.

그런 후, **사용자 추가** 대화 상자에서 **관리자** 탭을 선택하십시오. 관리자에게 사용 권한이 부여된 기능을 선택하십시오.

## 사용자 확인 방법

다음은 여러 가지 사용자 확인 방법입니다.

### 모두 거부

IBM Firewall은 서버를 액세스하지 못하도록 방지합니다.

### 모두 허용

사용자 확인이 필요하지 않습니다. 서버는 사용자를 확인하려고 하지 않지만 사용자가 외부 호스트를 액세스할 수 있도록 명령 프롬프트와 함께 진행합니다.

### Firewall 암호

서버는 사용자가 계속 진행할 수 있도록 먼저 Firewall 암호(표시되지 않음)를 요청합니다.

```
암호 :
```

Firewall 암호를 입력하십시오. 이는 사용자 이름이 Firewall에 추가될 때 사용된 것과 같은 암호입니다.

### SecurID 카드 확인

SecurID 카드를 가지고 있고 네트워크에서 Security Dynamics사 ACE/Server를 사용하면 이 방법을 사용하십시오.

프록시 서버는 사용자가 진행할 수 있게 하기 전에 PASSCODE(표시되지 않음)를 요구합니다.

```
PASSCODE 입력 :
```

이 시점에서 4-자리 SecurID PIN 코드, 쉼표 그리고 SecurID 카드의 코드 순으로 입력하십시오. 예를 들어, SecurID 카드가 코드 179091을 나타낼 때 PIN이 1234로 지정된 사용자 NEWUSER로 로그인하려면, 다음을 입력하십시오.

```
로그인 : NEWUSER
PASSCODE 입력 : 1234,179091
```

사용자가 처음으로 FTP를 사용하면, FTP에 암호 변경을 허용하는 옵션이 없기 때문에 SecurID 카드 사용자 확인이 실패할 것입니다. 사용자는 처음으로 PIN을 작성할 SecurID 카드 사용자 확인을 하려고 할때 텔넷을 사용해야 합니다. 사용자는 FTP, HTTP 등등과 같은 나중 사용자 확인에서 그 PIN을 계속 사용할 수 있습니다.

만일 SecurID 카드가 새로운 PIN 모드에 있으면,이 사용자 확인 방법을 IBM Firewall과 사용하기 전에 PIN을 설정해야 합니다.

## SecureNet 키 확인

Assurenet Pathways SecureNet카 카드를 가지고 있으면, 이 방법을 사용하십시오. SNK 카드를 초기화할 때는 다음을 사용하십시오.

- 표시 형식(16진수)
- ERASE 기능(on 또는 off)
- 한 자리 첼린지 기능(off)

프록시 서버는 사용자를 진행시키기 전에 SecureNet 키 카드에 의해 제공되는 응답을 요구합니다.

```
Use SNK for challenge
######## for user user_id
Ed:
```

첼린지 ########는 SecureNet 키 카드에 입력하는 8-자리 숫자입니다.

1. 이 프롬프트를 수신하면, SecureNet 키 카드를 활성화시키고 PIN 코드를 입력하십시오. PIN 코드는 카드와 함께 제공됩니다.
2. 서버가 제공한 대로 첼린지를 입력하십시오.

   예를 들어, 서버로 로그인하면, 서버는 다음과 같이 프롬프트합니다.

   ```
   Use SNK for challenge
      78987648 for user NEWUSER
   Ed:
   ```

   SecureNet 키 카드에 값 78987648을 입력하십시오. 그러면, 카드는 응답을 표시하고 이를 프록시 서버에 제공하게 됩니다.
3. 이 응답을 서버에 입력하십시오.

   만일 SecureNet 키 카드 8AE222A9가 챌린지의 응답으로 표시되면, 8AE222A9를 서버에 입력하십시오.

   ```
   logon: NEWUSER
      Use SNK for challenge 78987648 for user NEWUSER
   Ed:8AE222A9
   ```

AXENT** Technologies사에 의해 SecurNetKey(SNK)가 Defender Handheld Token**(DHT)으로 재명명되었습니다.

## NT 로그온 암호

이 사용자 확인 방법을 선택하면, 사용자 ID와 암호가 로컬 WIndows NT 사용자 데이터베이스에 비교하여 유효성이 검증됩니다. Firewall이 다른 Windows NT 서버를 수탁하도록 구성되면 이들 수탁된 서버에서 사용자 정의들이 탐색됩니다.

## 사용자 제공 사용자 확인 1, 2 그리고 3

FTP와 텔넷에 대해 사용자 제공 사용자 확인 방법을 사용할 수 있습니다. 자세한 내용은 *IBM eNetwork Firewall 참조서*를 참조하십시오.

# 제13장 프록시 서버 구성

이 장에는 보안 네트워크 안밖에서 워크스테이션의 프록시 서버를 구성하고 사용하는 방법에 대한 일반 정보가 들어 있습니다.

## HTTP 프록시

HTTP 프록시는 Web 브라우징에 대한 Socks 서버 없이 IBM Firewall을 통해 브라우저 요청을 효율적으로 처리합니다. 사용자는 내부 네트워크의 보안을 손상시키지 않고 또한 HTTP 프록시를 구현하기 위해 클라이언트 환경을 변경하지 않고 인터넷의 유용한 정보를 액세스할 수 있습니다.

HTTP 프록시는 서버가 아닙니다. 일반 사용자는 프록시의 파일을 다른 곳으로 로드하거나 프록시에 파일을 놓을 수 없습니다. 또한 이 프록시는 캐쉥 프록시도 아닙니다. HTTP 요청을 대신해 Firewall에 저장되는 것은 없습니다.

### 지속적 세션

지속적 세션은 클라이언트와 서버가 TCP 연결의 닫기를 신호하게 합니다. 이 신호는 연결 헤더 필드를 사용합니다.

IBM Firewall 프록시는 클라이언트와 프록시간의 지속적 세션을 지원합니다. *최대 지속적 요청* 조건과 *지속적 연결 시간종료* 조건은 얼마나 오래 연결이 존재할 지를 제어합니다. 이 조건들 중 하나가 발생하면, 프록시와 클라이언트간의 Socket 연결이 닫힐 것입니다. *최대 지속적 요청* 조건과 *지속적 연결 시간종료* 조건이 충족되지 않으면, 연결이 계속 열려 있을 것이며 언제 요청이 완료되는지를 결정하는 것은 클라이언트의 책임입니다.

잘 못 결정되었으면, 디스플레이가 통신량이 없을 때에 연결에 통신량을 표시할 수 있습니다. 이 예는 완전한 페이지가 로드되었을 지라도 계속해서 수행하는 브라우저의 애니메이트된 아이콘입니. 애니메이션을 멈추려면 **정지**를 누르십시오. 이 매개변수에 대한 정보는 96페이지의 『최대 지속적 요청』 및 96페이지의 『최대 연결 시간종료』를 보십시오.

### 구성 클라이언트를 사용하여 HTTP 프록시 구성

HTTP 프록시를 구성하려면, 다음과 같이 하십시오.

1. HTTP 프록시가 제대로 작업할 수 있기 전에 DNS 조회를 허용해야 합니다. 이를 쉽게 하는 방법은 구성 클라이언트 네비게이션 트리의 시스템 관리 폴더내에 있는 보안 규정을 누르고 DNS 조회 승인을 누르는 것입니다.
2. 필터를 활성화하십시오.
3. 연결을 추가하십시오. 네트워크의 비보안 측에서 연결을 설정하는 방법에 대한 예제는 57페이지의 『프록시 HTTP의 예제』를 참조하십시오.

4. HTTP 프록시를 구성하려면, 구성 클라이언트 네비게이션 트리에서 HTTP를 선택하십시오. IBM Firewall은 94페이지의 그림 24에서 보여 주는 바와 같이 **HTTP 프록시** 대화 상자를 표시합니다.


*그림 24. HTTP*

5. 프록시를 종료하려면 내 컴퓨터/제어판/서비스를 선택하십시오. IBM Firewall HTTP 프록시를 선택하고 *정지*를 누르십시오.

   실행 가능한 phttpd는 시스템 시작시 자동으로 시작하는 시스템 서비스입니다.

**HTTP 프록시** 대화 상자에서 매개변수를 구성하십시오. 매개변수를 변경하면, Firewall HTTP 프록시 서비스가 정지하고 다시 시작할 것입니다. 사용중인 프록시 사용자는 프록시가 재시작할 때까지 그들의 요청이 종료되게 합니다(수 초 정도).

### 프록시 포트 번호

이 매개변수를 사용해서 프록시가 요청을 연결대기해야 하는 포트 번호를 지정하십시오. 포트 번호를 변경하면, 포트를 통한 흐름을 허용하거나 또는 허용하지 않기 위해 필터를 구성해야 합니다. 1024보다 작은 포트 번호는 TCP/IP 응용 프로그램을 위해 예약됩니다. 프록시 웹 서버에 사용되는 공통 포트는 8080 및 8088입니다.

디폴트 필터 규칙은 포트 8080에서의 인바운드, 비보안 통신량을 불용하기 위해 설정되지만 동일한 포트에서 보안 통신량을 허용됩니다. 프록시는 비보안 프록시 요건만을 거부합니다. 디폴트는 8080입니다. 만일 이를 변경하면, 포트 번호도 이 구성에 대해 설정된 서비스에서 변경되어야 합니다. 이런 설정값을 변경하는 경우에는 phttpd 프로세스를 재시작해야 합니다.

### 최대 내용 버퍼 길이

서버가 생성한 동적 데이터에 대한 버퍼 크기를 설정하려면 이 매개변수를 사용하십시오. 동적 데이터는 CGI 프로그램, 서버−쪽 인클루드, 그리고 API 프로그램에서 출력됩니다. 이는 프록시에서 출력되지 않는 데이터입니다.

값을 킬로바이트 단위(K)로 지정하십시오. 디폴트는 50K입니다.

### 쓰레드 풀 크기

이 매개변수를 사용하여 한 번에 활성화시키려는 고정 쓰레드 수를 설정할 수 있습니다. 프록시는 다른 요청이 완료하고 쓰레드가 사용 가능해질 때까지 새로운 요청들을 보존합니다. 일반적으로, 시스템이 강력할수록 이 매개변수에 대해 더 큰 값을 사용해야 합니다. 만일 시스템이 메모리 교환과 같은 오버헤드 타스크에 너무 많은 시간을 쓰기 시작하면, 이 값을 줄이도록 하십시오. 60과 같은 정수를 지정하십시오. 디폴트 값은 200입니다.

### 사용자 레벨

이 매개변수는 확인할 사용자의 레벨을 프록시에게 알려줍니다. 값을 all, new 또는 none으로 지정하십시오. 디폴트는 none입니다. 값은 다음과 같습니다.

**all** 모든 브라우저는 사용자에게 사용자 ID와 암호를 입력하라는 메세지를 표시해야 함을 나타내기 위해 프록시 사용자 확인 응답을 전송하게 됩니다. 브라우저가 프록시 사용자 확인 응답을 지원하지 않으면 이를 나타내는 오류 페이지가 표시됩니다. 브라우저가 이를 지원하면 사용자 ID와 암호를 입력하라는 메세지가 표시됩니다.

**new** 이주 보조용으로 사용됩니다. 사용자 ID/암호 입력 메세지를 표시하도록 브라우저에게 지시하기 위해 자신을 HTTP/1.1 브라우저로 인식하는 클라이언트 브라우저에게 407 프록시 사용자 확인 응답만을 다시 전송합니다. HTTP/1.1 식별자를 가진 요청을 브로드캐스트하는 인터넷 익스플로러 4.0에 스위치를 설정할 수 있습니다. 넷스케이프와 다른 브라우저는 스스로를 HTTP/1.0 요청으로 구분합니다.

**none** 브라우저 요청을 점검하지 않습니다. 사용자 ID/암호를 입력하라는 메세지를 표시하지 않습니다.

### 시간종료

이 매개변수는 사용자가 재확인을 요청하기 전에 클라이언트 요청을 기다려야 하는 시간을 프록시에게 알려줍니다. 사용자는 이 유휴 시간 동안 초기의 사용자 확인시 제공된 특정 IP 주소와 사용자 ID로부터 확인됩니다. 시간을 분 단위로 지정하십시오. 디폴트 값은 60분입니다.

사용자가 활동적으로 찾기를 수행하는 한 이 시간 창은 만기되지 않습니다.

### 최대 지속적 요청

이 매개변수는 프록시가 HTTP/1.1 지속 연결에서 수신하는 최대 요청 회수를 지정합니다. 이것은 사용자 확인 시간종료에 직접 영향을 미치는 성능 툴입니다. 지속 세션이 끝날 때까지 사용자의 확인에 대한 검사는 수행되지 않습니다. 25와 같이 값을 지정하십시오. 디폴트 값은 5입니다.

### 최대 연결 시간종료

이 매개변수는 HTTP/1.1 준수 브라우저가 일단 프록시와의 세션을 시작하면 클라이언트 브라우저와의 HTTP/1.1 지속 연결을 유지해야 하는 시간을 초 단위로 지정합니다. 이것은 사용자 확인 시간종료에 직접 영향을 미치는 성능 툴입니다. 지속 세션이 끝날 때까지 사용자의 확인에 대한 검사는 수행되지 않습니다. 시간을 초 단위로 지정하십시오. 디폴트 값은 60입니다.

### HTTP 로깅 관리

이 매개변수는 프록시에게 시동/종료와 Firewall 로그에 대한 모든 프록시 요청을 기록하도록 지시합니다. 이는 로깅의 LOG_NOTICE 수준을 사용합니다. HTTP 요청 활동을 모니터하고 싶으면, 이를 켜짐으로 설정하십시오. 이벤트는 Firewall 로그 기능에 기록됩니다.

## 브라우저 구성

클라이언트 브라우저는 HTTP 프록시가 연결 대기중인 포트에 연결되도록 구성되어야 합니다.

또한 HTTPS 사용시 보안 프록시에 대해 IBM Firewall에 있는 HTTP 프록시를 가리키십시오.

Internet Explorer 브라우저를 프록시에게 HTTP/1.1 브라우저로 나타내고자 하는 경우, 다음을 수행하십시오.

- *열람* 풀다운을 여십시오.
- *인터넷 옵션*을 선택하십시오.
- *전진 탭*을 선택하십시오. .

- HTTP 1.1 설정으로 화면이동하여 스위치를 온(on)으로 설정하십시오.

### SSL 연결

HTTP 보안 연결에 대한 다른 서버로의 SSL 터널링이 지원됩니다. IBM Firewall은 이런 경우에 게이트웨이로 동작합니다. 터널은 클라이언트에서 Firewall을 통해 서버로 갑니다. 다음 예제에서처럼 HTTP 보안 연결에 대해 표준 포트 443을 사용하십시오.

```
https://www.ibm.com:443
```

또한 사전정의된 서비스 HTTPS 프록시 아웃 2/2를 사용하십시오.

또한 HTTPS 사용시 보안 프록시에 대해 IBM Firewall에 있는 HTTP 프록시를 가리키십시오.

자세한 내용은 57페이지의 『프록시 HTTP의 예제』를 참조하십시오.

### 지원되는 방법

HTTP 프록시는 다음과 같은 방법을 지원하는 데, 이는 인터넷에서 종류가 다른 찾기 방법입니다.

- FTP
- Gopher
- HTTP
- HTTPS
- WAIS

## HTTP 프록시에 대한 샘플 로깅 출력

다음은 HTTP 프록시 사용자 확인된 가져오기(get) 요구에 대한 로깅 출력의 샘플입니다.

```
Mar 06 14:04:50 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication UNSUCCESSFUL
for user <Unknown>, on 9.67.140.162, thru secure network ... RC:30.
Mar 06 14:04:50 1998 fire3: ICA2099i: httpd --> Status: 407 from client
9.67.140.162, who requested "GET http://9.67.128.69/ HTTP/1.1" for 0 bytes.
Mar 06 14:05:05 1998 fire3: ICA2024i: User fred successfully authenticated
using NT authentication from secure network:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2169i: User fred successfully authenticated
for HTTP Server using NT from secure network:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user (fred), on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:05 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/HTTP/1.1" for 2693 bytes.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user (fred), on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:06 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/Admin/lgsplash.gif HTTP/1.1"
for 211 bytes.
Mar 06 14:05:10 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user fred, on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:10 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/Admin/lgmast.gif HTTP/1.1"
for 211 bytes.
```

로깅 활동은 다음과 같이 설명됩니다.

- ICA2099i - 리턴 코드 407을 보여주며, 해당 가져오기(get) 요구에 대한 사용자 확인이 실패했음을 의미합니다.

  그러면 브라우저는 사용자에게 사용자 확인을 요구합니다. 브라우저는 사용자 ID와 암호를 요구합니다.
- ICA2140i - 사용자 Fred에 대한 사용자 확인이 성공했습니다.

사용자 확인은 웹 페이지 상의 모든 요수에 대한 가져오기(get) 요구가 발생할 때마다 이루어집니다.

## FTP

1. FTP 프록시를 사용해서 Firewall 호스트를 액세스하십시오. (Firewall에 대한 호스트명으로 ftp_gw.domain.net.com을 사용하게 됩니다).

   ```
   ftp ftp_gw.domain.net.com
   ```

   프록시 서버는 사용자명을 요구합니다.

   ```
   로그인 :
   ```
2. Firewall을 사용할 수 있는 권한을 받은 사용자명을 입력하십시오.

   ```
   login: jane_doe
   ```

서버는 사용자명이 Firewall에 추가되었을 때에 선택된 사용자 확인 스킴에 따라 사용자 신원의 유효성을 검증합니다(81페이지의 『IBM Firewall에 사용자 추가』 참조). 프록시 서버가 사용자를 확인하는 방법에 대해서는 90 페이지의 『사용자 확인 방법』을 참조하십시오.

사용자 확인이 끝난 후에 프록시 서버는 FTP 명령 프롬프트를 표시합니다.

```
ftp>
```

quote와 site FTP 명령을 사용해서 외부 호스트에 연결하십시오.

```
ftp> quote site forhost.network.outside.com
```

외부 호스트는 이제 사용자가 연결할 사용자명과 암호를 요구합니다. 이는 Firewall로의 FTP에서 사용한 사용자명 및 암호와는 다를 것입니다.

로그인에 대한 디폴트 시간 종료 값은 60초이며 유휴 프록시에 대한 디폴트 시간 종료 값은 7200초입니다. 디폴트 시간 종료 값을 변경하려면 100 페이지의 『FTP 및 텔넷 프록시에서 시간 종료 값 교체』를 참조하십시오.

## 가시적 FTP

Firewall을 통해 가시적으로 ftp할 수 있습니다. 가시적 프록시는 Firewall 사용자 확인이 필요 없으므로 가시적 프록시의 사용자는 Firewall 프록시 사용자처럼 정의될 필요가 없습니다. 가시적 프록시는 Firewall의 비보안쪽으로 송신되는 Firewall의 보안쪽에서만 허용됩니다. 가시적 프록시가 작동하기 위해서는 이를 보안 규정 구성 클라이언트 패널에서 선택해야 합니다.

1. ftp를 사용해서 Firewall 호스트를 액세스하십시오. (Firewall에 대한 호스트명으로 ftp_gw.domain.net.com을 사용하게 됩니다. )

   ```
   ftp ftp_gw.domain.net.com
   ```

2. 프록시 서버는 사용자명을 요구합니다.

   ```
   사용자:
   ```

3. 비보안 네트워크에서 사용자명을 입력하십시오.

   ```
   사용자: username@remote_site_host_name
   ```

4. 그러면 목표 호스트는 이전 단계에서 입력한 사용자 이름의 암호를 입력하라는 메세지를 표시합니다.

   ```
   암호 :
   ```

5. 암호를 입력하십시오.

로그인에 대한 디폴트 시간 종료 값은 60초이며, 유휴 프록시의 경우에는 7200초(2시간)입니다. 디폴트 시간 종료 값을 변경하려면 100페이지의 『FTP 및 텔넷 프록시에서 시간 종료 값 교체』를 참조하십시오.

## 텔넷

텔넷 프록시를 사용해서 Firewall 프록시 서버로 로그인하십시오. 호스트명이나 또는 인터넷 주소를 사용할 수 있습니다. 사용자의 신임이 확인된 후 Firewall에서 텔넷 명령을 사용해서 의도한 호스트로 로그인하십시오. 예를 들어, telnet_gw의 호스트명을 가지고 Firewall을 통해 보안 네트워크 내에 있는 텔넷을 사용하여 궁극적인 목적지인 forhost.network.outside.com을 액세스할 수 있습니다.

1. 프로세스를 시작하기 위해 텔넷을 사용하여 Firewall 호스트를 액세스하십시오. (Firewall에 대한 호스트명으로 telnet_gw.domain.net.com을 사용하게 됩니다. )

   ```
   telnet telnet_gw.domain.net.com
   ```

2. 프록시 서버는 사용자명을 요구합니다.

   ```
   로그인 :
   ```

3. Firewall을 사용할 수 있는 권한을 받은 사용자명을 입력하십시오.

   ```
   login: jane_doe
   ```

서버는 사용자명이 Firewall에 추가되었을 때에 선택된 사용자 확인 스킴에 따라 사용자 신원의 유효성을 검증합니다(81페이지의 『IBM Firewall에 사용자 추가』 참조). 프록시 서버가 사용자를 확인하는 방법에 대해서는 90페이지의 『사용자 확인 방법』을 참조하십시오.

oneact 쉘을 사용하게 됩니다. IBM Firewall 프록시 텔넷 디먼으로, 모든 통신이 Firewall을 통과합니다.

oneact 쉘을 사용하는 경우 사용자 확인이 끝난 후에 프록시 서버는 다음을 표시합니다.

```
ENTER DESIRED HOST:
```

유형

```
telnet forhost.network.outside.com
```

외부 호스트는 호스트에 알려진 대로 사용자 이름과 암호를 입력하도록 요청합니다. 이는 Firewall 프록시 서버에서 사용한 사용자명 및 암호와는 다를 수 있습니다.

로그인에 대한 디폴트 시간 종료 값은 60초이며 유휴 프록시에 대한 디폴트 시간 종료 값은 7200초입니다. 디폴트 시간 종료 값을 변경하려면 100 페이지의 『FTP 및 텔넷 프록시에서 시간 종료 값 교체』를 참조하십시오.

## 가시적 텔넷

Firewall을 통해 가시적으로 텔넷할 수 있습니다. 가시적 프록시는 Firewall 사용자 확인이 필요 없으므로 가시적 프록시의 사용자는 Firewall 프록시 사용자처럼 정의될 필요가 없습니다. 가시적 프록시는 Firewall의 비보안 쪽으로 송신되는 Firewall의 보안 쪽에서만 허용됩니다. 가시적 프록시가 작동하기 위해서는 이를 보안 규정 구성 클라이언트 패널에서 선택해야 합니다.

1. 텔넷을 사용해서 Firewall 호스트를 액세스하십시오. (호스트명으로 `ftp_gw.domain.net.com`을 사용하게 됩니다. )

   ```
   telnet telnet_gw.domain.net.com
   ```

2. 프록시 서버는 사용자명을 요구합니다.

   로그인:

3. 비보안 네트워크에서 사용자명을 입력하십시오.

   ```
   Login@remote_host
   ```

외부 호스트는 호스트에 알려진 대로 사용자 이름과 암호를 입력하도록 요청합니다. 이는 Firewall 프록시 서버에서 사용한 사용자명 및 암호와는 다를 수 있습니다.

로그인에 대한 디폴트 시간 종료 값은 60초이며 유휴 프록시에 대한 디폴트 시간 종료 값은 7200초입니다. 디폴트 시간 종료 값을 변경하려면 100 페이지의 『FTP 및 텔넷 프록시에서 시간 종료 값 교체』를 참조하십시오.

## FTP 및 텔넷 프록시에서 시간 종료 값 교체

FTP와 텔넷은 모두 로그인과 유휴 대기에 대한 시간 종료 값을 가집니다. 디폴트로 로그인과 사용자 확인중에 60초마다 적어도 한 번씩 세션 활동이 있어야 합니다. 이것은 loginTimeout으로 알려져 있습니다.

일단 로그인이 성공적으로 완료되면 7200초마다 적어도 한 번씩 세션에 활동이 있어야 하며 그렇지 않은 경우 세션은 단절됩니다.

ROOTDIR\config 디렉토리에 fwTimeout.cfg 파일을 작성하고 새로운 시간 종료 값을 초 단위로 지정하여 이러한 디폴트를 대체할 수 있습니다. fwTimeout.cfg 파일의 형식은 다음과 같아야 합니다.

텔넷
```
proxyTimeout=7200
loginTimeout=60
```

```
ftp
proxyTimeout=7200
loginTimeout=60
```

# 제14장 Firewall 로깅 모니터

이 장에서는 실시간으로 경보의 로깅을 모니터하는 방법을 설명합니다. 구성된 임계값이 위반되면 경보가 생성됩니다.

IBM Firewall은 사용자 정의 임계값에 따른 잠재적인 위기 상황의 경우 Firewall 로그에 전송된 메시지를 모니터합니다. 임계값 위반이 발생하면, Firewall은 Firewall 관리자가 지정한 방식으로 경보를 전달합니다.

## 임계값 정의

임계는 계수와 시간 매개변수로 구성됩니다. 지정된 시간 (분) 중에 계수 (특정 이벤트의 수)를 초과하면, 임계를 위반하게 되고 경보 메세지가 생성됩니다.로그 모니터는 4가지 유형의 임계를 인식합니다.

1. 총 사용자 확인 실패
2. 특정 사용자 ID에 대한 사용자 확인 실패
3. 특정 호스트에서 시작하는 사용자 확인 실패
4. 로그에서의 메세지 태그의 발생

모든 임계값은 구성 클라이언트나 또는 명령 행 인터페이스를 사용해서 구성될 수 있습니다. 임계값 정의에 대한 변경사항은 IBM Firewall에서 자동으로 선택됩니다.

## 경보 메세지

임계에 도달하면, IBM Firewall이 경보 메세지를 생성합니다. 경보 메세지의 전달은 4가지 형태로 일어날 수 있습니다.

1. 로그 파일의 입력항목.
   - 구성 클라이언트나 명령 행을 통해 구성할 수 있는 경보 로그 기능을 통해.
   - Firewall 로그에서
2. 사용자 리스트로 전자 우편 메세지를 송신하십시오
3. 구성된 대로 호출기. 105페이지의 『호출기 알림 지원』을 참조하십시오.
4. 경보 메세지가 첫번째 매개변수인 사용자-정의 명령의 실행.

경보 메세지는 특정 임계값 위반과 관련된 정보를 가지고 있습니다. 예를 들면, 다음과 같습니다.

```
ICA0001e: ALERT – 사용자 확인 실패 20.
ICA0002e: ALERT – 사용자 루트에 대한 사용자 확인 실패 10.
ICA0003e: ALERT – 호스트 56.67.78.89의 사용자 확인 실패 15.
ICA0004e: ALERT – 3개의 입력항목이 있는 태그 ICA1234e.
```

경보 메세지와 로그 모니터에 의해 시작된 기타 메세지는 모니터되지 않습니다.

## 구성 클라이언트를 사용하여 로그 모니터 구성

본 섹션은 실시간 로그 모니터를 구성하기 위해 구성 클라이언트를 사용하는 방법에 대해 설명합니다. 구성 클라이언트 네비게이션 트리에서 시스템 로그를 선택하십시오. 파일 폴더를 두 번 눌러서 보기를 확장하십시오. **로그 모니터 임계값**을 누르십시오.

**로그 모니터 임계값 관리** 대화 상자에서, 임계값 정의를 추가, 변경 또는 삭제할 수 있습니다.

### 로그 모니터 추가

임계값 정의를 추가하려면, **로그 모니터 임계값 관리** 대화 상자에서 **신규**를 선택하고 **열기**를 누르십시오. **로그 모니터 추가** 대화 상자가 나타납니다. 다음 필드를 채우십시오.

1. **클래스 유형** 화살표를 눌러 클래스 유형 리스트에서 선택하십시오. 등급 유형은 다음과 같습니다.
   - 전자우편 통지
   - 명령 실행
   - 사용자 확인 실패 임계값당
   - 총 사용자 확인 실패 임계값
   - 호스트 사용자 확인 실패 임계값당
   - 메세지 임계값
2. 만일 전자우편 통지의 등급 유형을 선택했다면, 전자우편 주소를 입력하십시오. 복수 전자우편 통지 등급을 정의할 수 있습니다.

   모든 임계값 위반 메세지는 지정된 전자우편 주소로 송신됩니다.
3. 만일 명령 실행의 등급 유형을 선택했다면, 명령 파일명을 채우십시오.

   로그 모니터는 첫번째 매개변수로 경보 메세지와 함께 이 명령을 실행합니다. 오로지 한 개의 명령 실행 등급만 정의할 수 있습니다.
4. 만일 메세지 임계값의 등급 유형을 선택했다면, 모니터하고 싶은 IBM Firewall 로그 메세지에서 표준 태그인 메세지 태그를 채우십시오.
5. 만일 임계값 등급 중 하나를 선택했다면, 임계값 계수 필드를 채우십시오.

   임계값 계수는 지정된 시간 기간에 허용되는 실패한 이벤트의 최대 수입니다.
6. 만일 임계값 등급 중 하나를 선택했다면, 임계 시간 필드를 채우십시오.

   임계 시간은 이벤트의 첫 발생에서 시작하는 분의 수입니다.
7. 만일 임계값 등급 중 하나를 선택했다면, 호출기 알림의 활성화 여부를 나타내기 위해 예 또는 아니오를 누르십시오.

8. 주석을 채우는 것은 선택적입니다.
9. **확인**을 누르십시오.

### 임계값 정의 변경

임계값 정의를 변경하려면, **로그 모니터 임계값 관리** 대화 상자에서 변경될 항목을 선택한 후 **열기**를 누르십시오. **로그 모니터 변경** 대화 상자가 나타납니다.

1. 임계값 계수에 대한 변경과 임계 시간 필드를 입력하십시오.

   임계 계수는 지정된 시간 기간 내에 감지되어야 하는 실패한 사용자 확인 메세지의 최대 수입니다. 임계 시간은 이벤트의 첫 발생에서 시작하는 분의 수입니다.
2. **확인**을 누르십시오.

### 임계값 정의 삭제

임계값 정의를 삭제하려면, **로그 모니터 임계값** 대화 상자에서 삭제될 항목을 선택하고 **삭제**를 누르십시오. 삭제를 확인하도록 요구됩니다. **예**를 눌러 확정하십시오. 삭제는 로그 파일로부터의 삭제를 의미하지 않는다는 것에 유의하십시오. 이는 정의의 삭제를 의미합니다.

## 호출기 알림 지원

Firewall은 Firewall에 침입 경보가 있을 때 관리자의 호출기로 메세지를 보내 시스템 관리자를 호출할 수 있습니다. 호출기 알림 지원을 설정하려면 다음의 세 가지 호출기 구성요소를 구성해야 합니다.

1. 명령 조정 - 이 구성요소는 구성 클라이언트를 사용하여 작성되고 수정되어야 합니다. 이것은 로그 모니터에서 사용되어 명령 행에서 사용할 수 있는 호출기 명령에 대한 디폴트를 설정합니다. 이 구성요소에는 호출기 환경을 정의하는 고유한 항목이 들어 있습니다. 이 구성요소를 정의하고 조정하는 것에 대해서는 107페이지의 『명령 조정』을 참조하십시오.
2. 반송자(carrier) 관리 - 모뎀을 연결하기 전에 적합한 반송자를 정의해야 합니다. 이 구성요소에는 미국에서 사용되는 디폴트 반송자 리스트가 들어 있습니다. 사용중인 반송자가 이 리스트에 있는 것이 아니면 이 구성요소에 사용하는 반송자를 추가하십시오. 더 자세히 알고 싶으면, 108페이지의 『반송자 관리』를 참조하십시오.

   반송자로부터 기존 전화번호를 사용하여 반송자에 대해 이러한 전화 번호의 유효성을 검증하십시오. 반송자와 통신할 때 구매한 특정 서비스에 대해 유효한 반송자의 모뎀 전화번호와 기타 설정을 확인하십시오.
3. 모뎀 관리 - 모뎀을 연결하기 전에 적합한 모뎀 정의를 작성해야 합니다. 이런 정의는 호출기 알림 지원이 사용하는 모든 관련 모뎀 정보를 가지고 있습니다. 이 구성요소에는 선택할 수 있는 모뎀 리스트가 들어 있

습니다. 이 리스트에 모뎀을 추가할 수도 있으나 일부 모뎀은 반송자가 지원하는 것과 호환되지 않을 수 있습니다. 모뎀 정의 유지보수에 대해서는 110페이지의 『모뎀 관리』를 참조하십시오.

**주:** IBM Firewall은 호출기 알림 지원을 위한 Tele-AlphaNumeric Protocol (TAP) 통신 프로토콜을 지원합니다.

### 지원되는 반송자 및 모뎀

반송자 데이터베이스 파일에는 반송자와 관련 전송 매개변수의 리스트가 들어 있습니다. 다른 반송자를 추가할 수 있습니다. 반송자명과 모뎀 전화번호를 제외한 일부 매개변수는 다음과 같습니다.

- 문자형 호출기에 대한 최대 메세지 길이와 숫자형 호출기에 대한 최대 자리수
- 보오드율, 패리티, 데이터 및 정지 비트 길이

특정 반송자를 사용하기 전에, 반송자가 TAP 프로토콜을 사용하는지 확인하십시오.

호출기 코드는 디폴트 모뎀 정의와 함께 제공됩니다. 이는 다음과 같습니다.

- IBM MOD 448 14400 bps
- IBM 5853 2400 bps
- IBM 7852 28800 bps
- IBM 7855 2400 bps
- 일반 Hayes 호환 가능
- US Robotics Courier 9600 bps
- Zoom V.34

## 호출기 알림 지원 구성

호출기 설정은 명령 조정 파일을 구성하고 반송자와 모뎀을 유지보수하기 위해 사용됩니다. 호출기를 사용중이면, 로그 모니터를 사용하기 전에 호출기 환경을 조정하기 위해 호출기 설정을 사용해야 합니다.

시작하기 전에, 올바른 모뎀 전화번호, 호출기 ID 및 반송자의 모뎀 매개변수를 확보해야 합니다.

호출기 알림 지원을 구성하려면, 구성 클라이언트 네비게이션 트리에서 시스템 관리를 선택하십시오. 파일 폴더를 두 번 눌러서 보기를 확장하십시오. **시스템 로그**를 선택하십시오. 파일 폴더를 두 번 눌러서 보기를 확장하십시오. **호출기 설정**을 선택하십시오.

## 명령 조정

**호출기 설정**을 선택하면 사용할 반송자와 모뎀을 선택하고 호출 메세지를 쓸 수 있습니다.

### 명령 조정 설정값

네비게이션 트리에서 **호출기 설정**을 선택하면, 107페이지의 그림 25에 나와 있는 대화 상자와 유사한 명령 조정 설정값이 들어 있는 **호출기 설정** 대화 상자가 표시됩니다.


*그림 25. 호출기 설정*

입력 필드에 추가될 값을 입력하거나 또는 선택하십시오.

1. 호출기 ID를 입력하십시오. 이것은 대개 반송자 회사가 사용자의 호출기에 지정한 고유한 PIN이 됩니다.
2. 호출기 메세지를 입력하십시오. 이것은 사용자가 전송하려는 디폴트 메세지를 포함하는 문자열입니다. 숫자형 호출기에 대해 이는 숫자만이어야 합니다. 문자형 호출기에 대해 이는 텍스트 메세지일 수 있습니다. 반송자 설정에 지정된 최대 메세지 길이를 초과하지 않도록 하십시오. 그렇지 않으면 메세지는 잘립니다. 콜론(:)을 사용하지 마십시오.만일 사용하면, 이는 공백 문자로 대체됩니다.
3. 반송자명이 없는 경우에는 **선택**을 눌러 반송자를 정의하십시오. **호출기 반송자(carrier) 관리** 대화 상자가 표시될 것입니다. 이 패널을 채우는 데 대한 자세한 내용은 108페이지의 『반송자 관리』를 보십시오.

4. 모뎀명이 없는 경우에는 **선택**을 눌러 모뎀을 정의하십시오. **호출기 모뎀 관리** 대화 상자가 표시됩니다. 이 패널을 채우는 데 대한 자세한 내용은 110페이지의 『모뎀 관리』를 보십시오.
5. **확인**을 누르십시오.

### 명령 조정 변경

네비게이션 트리에서 호출기 설정을 선택하면, 명령 조정 설정값이 들어 있는 **호출기 설정** 대화 상자가 표시됩니다.

1. 입력 필드에 값을 입력하거나 또는 선택하여 기존의 조정 입력 필드의 값을 변경하십시오.
2. **확인**을 누르십시오.

### 명령 조정 삭제

1. 리스트에서 항목을 선택하고 **삭제**를 두 번 눌러 **호출기 반송자(carrier) 관리** 대화 상자나 **호출기 모뎀 관리** 대화 상자의 항목을 삭제할 수 있습니다.

   삭제를 확인하도록 요구됩니다.
2. **예**를 눌러 삭제를 확정하거나 **아니오**를 눌러 **호출기 설정** 대화 상자로 되돌아 가십시오.

만일 조정 항목이 없으면, 호출기 알림 지원이 호출을 송신할 수 없게 됩니다.

## 반송자 관리

**호출기 설정** 대화 상자에서, 반송자(carrier) 명 필드로 가서 **선택**을 누르십시오. 109페이지의 그림 26에 표시된 것과 유사한 **호출기 반송자(carrier) 관리** 대화 상자가 표시됩니다.


*그림 26. 호출기 반송자 관리*

## 반송자 추가

새로운 반송자를 추가하려면, **호출기 반송자 (carrier) 관리** 대화 상자에서 **신규**를 선택하고 **열기**를 누르십시오. 해당 입력 필드에 값을 입력하거나 또는 선택하십시오.

1. 반송자명을 입력하십시오. 이것은 고유한 이름이면 어떤 이름이나 무방하며 사용자가 반송자를 인식하는 데 필요한 충분한 정보를 제공합니다.
2. 음성 호출 또는 기타 서비스 번호와는 대조되는 것으로 반송자 회사의 모뎀에 대한 전화번호인 반송자 전화번호를 입력하십시오. 이것은 사용자가 계약한 호출 장치와 서비스가 요구하는 지역 또는 국가 적용범위에 적절하며 숫자형 또는 문자형 호출기에 적절한 모뎀 번호여야 합니다.
3. 호출 방법에 대해 TAP를 입력하십시오. 값만 허용됩니다.
4. 반송자가 허용하거나 요구하는 암호를 입력하십시오.
5. 문자형 호출기에 대한 최대 메세지 길이와 숫자형 호출기에 대한 최대 자리수를 입력하십시오.
6. 보오드율을 입력하십시오. 화살표를 누르고 리스트에서 값을 선택하십시오.
7. 패리티 필드에 대해 **짝수**, **홀수** 또는 **없음**을 누르십시오.
8. 디폴트 데이터 비트를 선택하십시오. **7** 또는 **8**을 누르십시오.
9. 디폴트 정지 비트를 선택하고 **1** 또는 **2**를 누르십시오.
10. **확인**을 누르십시오.

### 반송자 변경

1. **호출기 반송자(carrier) 관리** 대화 상자에서 변경하려는 반송자를 선택한 후 **열기**를 누르십시오.
2. 변경할 수 있는 필드의 설명에 대해서는 109페이지의 『반송자 추가』를 참조하십시오. 반송자명 자체는 변경될 수 없습니다. 이 필드는 사용 중단됩니다.
3. 원하는 변경을 수행하십시오.
4. **확인**을 누르십시오.

### 반송자 삭제

1. **호출기 반송자(carrier) 관리** 대화 상자에서 삭제하려는 반송자를 선택한 후 **삭제**를 누르십시오.
2. 삭제를 확인하도록 요구됩니다. **예**를 눌러 확정하십시오.

   **주:** 반송자 데이터베이스에는 최소한 하나의 반송자가 항상 들어 있어야 합니다. 만일 정의된 반송자가 없으면 호출기 알림 지원은 실패합니다.

## 모뎀 관리

모뎀 설명서에는 모뎀을 초기화하는 방법에 대한 관련 정보가 들어 있습니다. 반송자를 사용하여 모뎀 설정을 조정해야 할 수도 있습니다. 일반적으로 표준 모뎀 명령을 사용하는 Hayes 호환 모뎀만 지원됩니다.

**호출기 설정** 대화 상자에서, 모뎀 명 필드로 이동한 후 **선택**을 누르십시오. 110페이지의 그림 27에 표시된 것과 유사한 **호출기 모뎀 관리** 대화 상자가 표시됩니다.

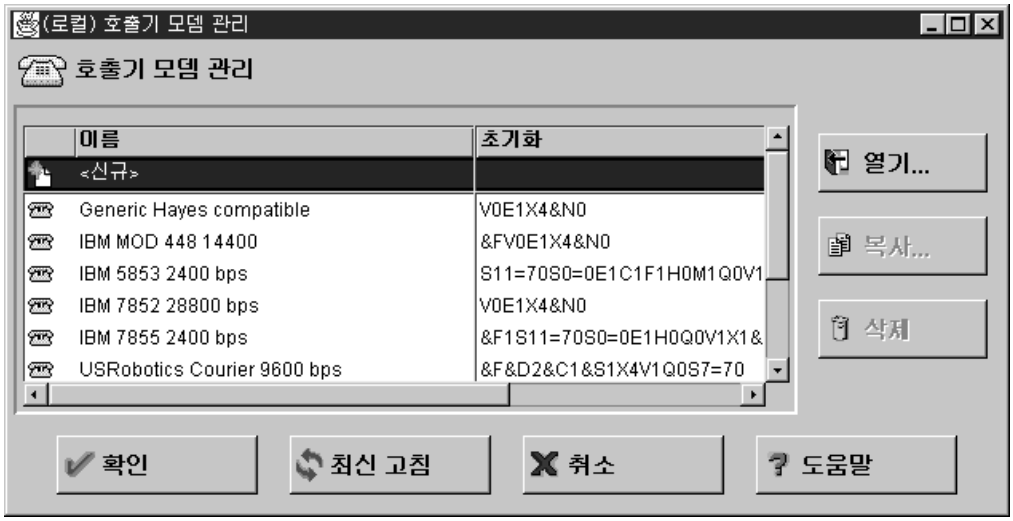


*그림 27. 호출기 모뎀 관리*

이 대화 상자를 사용하여 여러 가지 모뎀을 추가, 변경 또는 삭제할 수 있습니다.

### 모뎀 추가

새로운 모뎀 정의 파일을 추가하려면, **호출기 모뎀 관리** 대화 상자에서 **신규**를 선택한 후 **열기**를 누르십시오. **모뎀 추가** 대화 상자에서, 입력 필드에 값을 입력하거나 선택하십시오.

1. 모뎀명을 입력하십시오. 이것은 다른 정의중에서 고유하다면 어떤 이름이나 무방하며 사용자가 모뎀을 인식하는 데 필요한 충분한 정보를 제공할 수 있습니다.
2. 모뎀이 접속되는 직렬 COM 포트를 정의하는 COM 포트 번호를 입력하십시오. 10보다 작은 숫자를 입력하십시오. 이 포트에 하드웨어로 구성되어야 하나, Windows NT로 정의되어서는 안 됩니다. 이 경우, 호출기 기능으로 인해 포트에 대한 액세스가 거부됩니다. 모뎀이 하드웨어 설정과 일치하지 않으면, 호출기 코드는 오랜 시간 동안 재시도하게 되며 결국 실패하게 됩니다.
3. X 레벨4에서 반향(echo)을 가지며 로컬 사이트에 의해 정의된 고정 보오드율을 가진 데이터 모뎀으로 해당 모뎀을 정의해주는 초기화 문자열을 입력하십시오. AT 명령은 포함시키지 않도록 하십시오. 호출기 기능은 초기화 문자열 맨 앞에 이 명령을 추가하게 됩니다.
4. 외부 회선 접두어를 입력하십시오. 이것은 회사 외부로 가기 위해 다이얼하는 번호입니다.
5. **확인**을 누르십시오.

### 모뎀 변경

1. **호출기 모뎀 관리** 대화 상자에서 모뎀명을 선택하고 **열기**를 눌러 모뎀 정의 파일을 변경하십시오.

   **모뎀 변경** 대화 상자에서, 모뎀 정의에 대해 변경할 수 있는 필드의 리스트가 표시됩니다. 이런 필드에 대해서는 111페이지의 『모뎀 추가』를 참조하십시오.

2. **확인**을 누르십시오.

### 모뎀 삭제

1. **호출기 모뎀 관리** 대화 상자에서 모뎀명을 선택하고 **삭제**를 눌러 모뎀 정의 파일을 삭제하십시오.
2. 삭제를 확인하도록 요구됩니다. **예**를 눌러 확정하십시오.

## 호출기 알림 로깅

호출기 알림 프로세스는 Firewall 로그 유틸리티를 사용하여 출력 로그를 기록합니다. 모든 호출 메세지와 오류는 일반 Firewall syslog 기능에 기록됩니다. Firewall 로그 파일을 설정하여 사용하는 방법에 대해서는 113페이지의 『제15장 로그 및 아카이브 파일 관리』를 참조하십시오.

### 호출기 설정 검사

호출기 명령을 사용하여 호출기 설정을 검증할 수 있습니다. 세부사항에 대해서는 *IBM eNetwork Firewall 참조서*를 참조하십시오. 설정을 정의하거나 변경할 경우 언제든지 호출기 명령을 사용하여 시스템, 모뎀, 반송자 및 호출 장치가 모두 서로 제대로 통신하고 있으며 호출 내용이 실제로 송수신될 수 있는지 확인하십시오.

## 명령 실행

경보 임계값에 도달할 때마다 기동되는 프로그램을 지정할 수 있습니다. 프로그램을 지정하려면 다음과 같이 하십시오.

1. **로그 모니터 관리**를 누르고 **신규**를 두 번 누르십시오.

   **로그 모니터 추가** 대화 상자가 나타납니다.

2. **클래스 유형** 드롭 다운 상자에서, **명령 실행**을 선택하십시오. 이는 패널의 **명령 파일명** 필드를 작동가능하게 합니다.

3. **명령 파일명** 필드에서, 경보 임계값에 도달될 때 기동하고자 하는 프로그램의 완전 경로명을 입력하십시오.

   로그 모니터에서 실행한 명령에 대한 작업 디렉토리는 \winnt\system32 입니다. 명령 쉘이 시스템 프로세스에서 수행되므로, 시스템 환경 변수만 설정됩니다. 사용자 환경 변수는 설정되지 않습니다. 일반적으로, 수행된 프로그램은 경로 변수에 의존하기 보다는 완전히 규정된 파일명을 사용해야 합니다.

   Firewall이 다음과 같이 프로그램의 첫번째 매개변수로서 전체 경보 메세지를 전달할 것입니다.

   ```
   총 사용자 확인 실패 경보: ICA0001e
   사용자 당 사용자 확인 실패 경보: ICA0002e
   호스트 당 사용자 확인 실패 경보: ICA0003e
   메세지 임계값 경보: ICA0004e
   ```

이들 메세지의 전체 설명은 *IBM eNetwork Firewall 참조서*를 보십시오.

# 제15장 로그 및 아카이브 파일 관리

본 장은 구성 클라이언트를 통해 로그 기능을 사용하는 방법에 대해 설명합니다. 사용자가 여러 가지 IBM Firewall 서버를 통해 호스트에 액세스하려고 할 때, IBM Firewall에서는 IBM Firewall 로깅 서비스에 의해 유지보수되는 로그 파일에 항목을 기록합니다.

IBM Firewall은 Firewall을 구성하는 방법에 따라 로깅 정보의 큰 볼륨을 생성할 수 있습니다. 로그 항목은 Socks 및 Expert 필터와 같은 다양한 장소에서 나올 수 있습니다. 추가적으로, 로그 파일은 가령, *디버그, 정보* 또는 오류 등의 다양한 심각도 레벨로 로그 파일이 쓰여질 수 있습니다. 또한, 이 장에서는 로그 관리 및 로그 아카이브 관리 기능을 사용하여 로그 및 아카이브 파일의 크기를 관리하는 방법을 알려줍니다.

## 구성 클라이언트를 사용한 로그 파일 작성 및 아카이브

로그 관리 및 로그 아카이브 관리에 구성 클라이언트를 사용할 수 있습니다. 사용 가능한 디스크 공간이 모든 로그 정보를 저장할 수 있을 만큼 충분하다고 간주됩니다. Firewall은 Firewall 로그 기능에 대한 루틴 디버그 및 오류 정보를 생성합니다. 1차 Firewall 관리자만이 Firewall 로그 기능에 액세스할 수 있습니다. 경보 메세지는 경보 로그 기능으로 이동합니다. 관리 감사 로그 정보는 감사 로그 기능으로 이동합니다.

제대로 기능을 수행하는 보고서 유틸리티의 경우, Firewall 로그 메세지만이 그 입력 파일에 표시되는 것은 중요합니다. 다른 어떠한 기능도 Firewall 로그와 동일한 파일에 지정되어서는 안되므로, Firewall 로깅을 적절하게 설정하십시오.

주 구성 클라이언트 패널에서 경보를 보려면, 경보 로그 기능으로 지정된 파일에 경보를 지정해야 합니다. 그 파일에 대해 그 외의 어떠한 것도 지정되어서는 안됩니다.

다음의 우선순위 레벨은 대부분의 정보를 캡쳐하는 *디버그*와 함께 누적됩니다. *심각*은 가장 심각한 Firewall 이벤트만 캡처합니다.

- 디버그
- 정보
- 경고
- 오류
- 심각

Firewall 프로시듀어가 안정될 때까지 *정보* 레벨로 시작하는 것이 좋습니다. 그런 다음 *경고* 또는 *오류*로 변경하여 로깅 활동과 시스템 로그 크기를 줄일 수 있습니다.

우선순위 레벨은 메세지 태그 접미어 *(i,e,w,s..)*. 일부 메세지를 종료*(shut off)* 하는 방법을 판별하려면 테스트가 필요할 수도 있습니다.

## 로그 기능 추가

구성 클라이언트 네비게이션 트리에서 보기를 확장하기 위해 시스템 관리 파일 폴더 아이콘을 두 번 누르십시오. 시스템 로그 파일 폴더 아이콘을 두 번 눌러서 보기를 확장하십시오. 로그 기능을 선택하십시오. **로그 기능** 대화 상자가 현재 작동되는 로그 기능 세트를 표시하면서 나타납니다.

1. **로그 기능** 대화 상자에서 **신규**를 선택하고 **열기**를 눌러 현재 사용 가능한 것들에 syslog 항목을 추가하십시오.

   114페이지의 그림 28에서 보여 주는 바와 같이 **로그 기능 추가** 대화 상자가 나타납니다.


*그림 28. 로그 기능 추가*

2. **유형** 화살표를 눌러 유형을 선택하십시오. 유형은 파일명입니다.

3. 로그 기능은 기록되는 정보의 유형과 출발지를 판별합니다. **기능** 화살표를 눌러 다음 로그 기능들 중 하나를 선택하십시오.
   - Firewall 로그 - 필터 로깅을 포함한 일반 Firewall 로그
   - 경보 로그 - 경보 화면에 상주하기 위해 사용되는 로그 모니터 디먼 상태 및 임계값 위반 경고
   - 전자우편 로그
4. **우선순위** 화살표를 눌러 우선순위를 선택하십시오. 로깅 우선순위는 심각도의 증가 순으로 나열됩니다. 선택한 우선순위는 기록되는 최소 레벨이 됩니다.
5. 로그 파일명을 채우십시오. 로그 파일명은 절대 경로(드라이브와 백슬래쉬 \로 시작하는)를 가져야 하며 파일명으로의 경로가 존재해야 합니다.
6. 아카이브 관리는 오로지 *파일명* 유형 로그 기능과 함께 사용될 수 있습니다. 사용 가능해지면, 로그 파일 크기가 정기적으로 줄여질 수 있습니다. 아카이브 관리를 작동 가능하게 하면 `fwlogmgmt` 명령이 의존하는 매개변수를 설정한다는 것을 의미합니다. 116페이지의 『로그 아카이브』를 참조하십시오. 아카이브 관리 매개변수를 사용할 수 있게 하거나 또는 사용할 수 없게 만들 수 있습니다.
7. 활동중인 로그에 있는 레코드가 아카이브되어야 할 때까지의 일수를 선택하십시오. 이 값은 0이거나 0보다 커야 합니다. `fwlogmgmt -l` 명령이 이 기준에 맞는 로그 레코드를 발견할 때에 아카이브가 일어납니다. 로그 관리는 로그 레코드 보존 일수를 계산할 때 현재 날짜를 포함하지 않습니다.
8. 아카이브 파일명과 완전 경로를 입력하십시오. IBM Firewall은 디렉토리를 사용하는 디폴트 아카이빙 기능을 제공합니다. 그러나 원하는 경우, 플러그인 아카이브 기능을 사용할 수 있습니다.
9. 활동중인 로그 파일에 아카이브로부터 삭제되어야 할 때까지의 일수를 선택하십시오. 이 값은 0이거나 0보다 커야 합니다. `fwlogmgmt -e` 명령이 이 기준에 맞는 아카이브 파일을 발견할 때에 정리(퍼지)가 일어납니다. 로그 관리는 아카이브 파일 보존 일수를 계산할 때 현재 날짜를 포함하지 않습니다.
10. **확인**을 누르십시오.

## 로그 기능 변경

1. **로그 기능** 대화 상자에서 변경하려는 Firewall 로깅 항목을 선택한 후, **열기**를 누르십시오.

   **로그 기능 변경** 대화 상자가 나타날 것입니다.
2. 원하는 필드를 변경하십시오. 필드에 대한 설명은 114페이지의 『로그 기능 추가』를 참조하십시오.
3. **확인**을 누르십시오.

### 로그 기능 삭제

1. **로그 기능** 대화 상자에서 현재 사용 가능한 것으로부터 Firewall 로깅 항목을 선택한 후, **삭제**를 누르십시오.

   **삭제 경고** 패널이 나타납니다.
2. 삭제를 계속하려면 **확인**을 누르십시오. 마음이 바뀌었으면 **취소**를 누르십시오. 이는 실제 로그 파일을 삭제하지 않습니다.

## 로그 아카이브

아카이브 프로세스

- 사용중 로그로부터 자격이 있는 레코드를 삭제합니다.
- 이들을 별도의 파일에 놓습니다.
- 결과 파일을 비교합니다.
- 새로운 파일을 아카이브 디렉토리에 놓습니다.

로그 관리 프로그램을 시작하여 누적된 로그를 아카이브하는 데, 다음의 두 가지 옵션을 사용할 수 있습니다.

1. 때때로 명령 행에서 `fwlogmgmt -l` 명령을 수행하십시오.
2. NT 스케줄 서비스로 `fwlogmgmt -l` 명령을 설정하십시오.

로그 아카이브를 정리(퍼지)하는 일은 자격있는 아카이브 파일을 아카이브 디렉토리로부터 삭제하는 일로 이루어 집니다.

아카이브 파일을 삭제하려면, 두 개의 옵션이 있어야 합니다.

1. 때때로 명령 행에서 `fwlogmgmt -a` 명령을 수행하십시오.
2. NT 스케줄 서비스로 `fwlogmgmt -a` 명령을 설정하십시오.

114페이지의 『로그 기능 추가』에서 기술된 대로 로그 기능 정의에 지정된 값에 의해 자격있는 레코드 및 파일들이 결정됩니다.

로그 관리 프로세스를 수행하는 가장 효율적이고 편리한 방법은 이를 NT 스케줄 서비스로 설정하는 것입니다. 제어판의 서비스 오브젝트를 사용하여 시작하십시오.

예를 들어 로그 관리 아카이빙 프로세스가 매일 오전 3시에 실행되도록 설정하려면 다음을 입력하십시오.

```
at 3:00 /every:M,T,W,Th,F,S,Su fwlogmgmt -l
```

### 플러그인 DLL

Firewall 디폴트 DLL 대체시 사용하는 로그 아카이버 (archiver) 플러그-인 DLL에 대해 알고 싶으면, *IBM eNetwork Firewall 참조서*를 참조하십시오.

## 로그 관리 출력

로그 관리 기능은 로그 관리 활동을 진행시키기 전에 일부 예비 완전성 검사를 수행합니다. 문제가 발생하면, 명령 행에서 `fwlogmgmt` 명령을 수행할 때 진단이 Firewall 로그 기능으로 전송됩니다.

전자우편 또는 관리 감사(local0) 로그 기능은 다른 기능보다는 다른 아카이브 규칙에 따라 달라집니다. 모든 로그 기능에 있어서, 아카이브가 되려면 아카이브가 사용 가능 상태에 있어야 합니다. 그러나 *전체* 전자우편이나 감사 로그 파일이 매번 아카이브 되는데 반해, Firewall(local4)과 경보(local1) 로그 레코드들은 날짜가 아카이브 프로세스가 실행될 때 기능 정의에 지정된 기준을 넘어선 경우에만 아카이브됩니다. 또한 전자우편 로그의 정보는 디버그용이며, 아카이브할만한 가치는 없습니다. 일반적으로 더 유용한 다른 전자우편 정보는 Firewall(local4) 로그에 기록되어 있습니다.

## 보고서 유틸리티

보고서 유틸리티 기능을 사용하여 현재 또는 아카이브 로그 파일로부터 보고서를 생성하는 데 도움을 얻을 수 있습니다. 보고서 유틸리티는 관계형 데이터베이스 표로 쉽게 대응될 수 있도록 구성되고 서식화된 표로 작성된 관리 정보 파일을 생성합니다. 이들 표는 Firewall 관리자가 다음을 분석하는 데 도움을 줍니다.

- Firewall의 일반 사용법
- Firewall 프로세스에 있는 오류
- 보안 네트워크로의 허가 받지 못한 액세스 시도

유틸리티와 Firewall 로그를 사용하면, 관리자가 메세지의 일반적인 텍스트 파일을 작성할 수 있습니다. 또한 표로 작성된 파일은 생성되어 DB2 제품 계열과 같은 관계형 데이터베이스 시스템의 표로 반입될 수 있습니다. 그러면 관리자는 구조화 조회 언어(SQL)를 사용하여 데이터를 조회하고 보고서를 생성할 수 있습니다.

보고서 유틸리티는 Firewall 설치의 일부로서 설치됩니다. 이들은 또한 개별적으로 설치되고 비-Firewall 호스트에서 실행될 수 있습니다. 구성 클라이언트는 이를 Firewall에서 수행하기 위해 사용될 수 있습니다. 비-Firewall 시스템에서는 명령 행을 사용하십시오.

제대로 기능을 수행하는 보고서 유틸리티의 경우, `Firewall` 로그 메세지만이 그 입력 파일에 표시되는 것은 중요합니다. 다른 어떠한 기능도 `Firewall` 로그와 동일한 파일에 지정되어서는 안되므로, Firewall 로깅을 적절하게 설정하십시오.

AIX용 IBM Firewall V3R1 이전 버전의 로그 파일에 대해서는 보고서 유틸리티를 사용하지 않도록 하십시오. 그러나 AIX V3R1용 IBM Firewall에서 가져온 로그 파일을 처리하는 데는 보고서 유틸리티를 사용할 수 있습니다. 이를 사용하여 AIX su 로그도 처리할 수 있습니다. 보고서 유틸리티에 대한 세부사항은 *IBM eNetwork Firewall 참조서*를 보십시오.

## 구성 클라이언트를 사용해서 보고서 유틸리티 수행

구성 클라이언트 네비게이션 트리에서 보기를 확장하기 위해 시스템 관리 파일 폴더 아이콘을 두 번 누르십시오. 시스템 로그 파일 폴더 아이콘을 두 번 눌러서 보기를 확장하십시오. **보고서 유틸리티**를 선택하십시오. 118 페이지의 그림 29에서 보여 주는 바와 같이 **보고서 유틸리티** 대화 상자가 나타납니다.

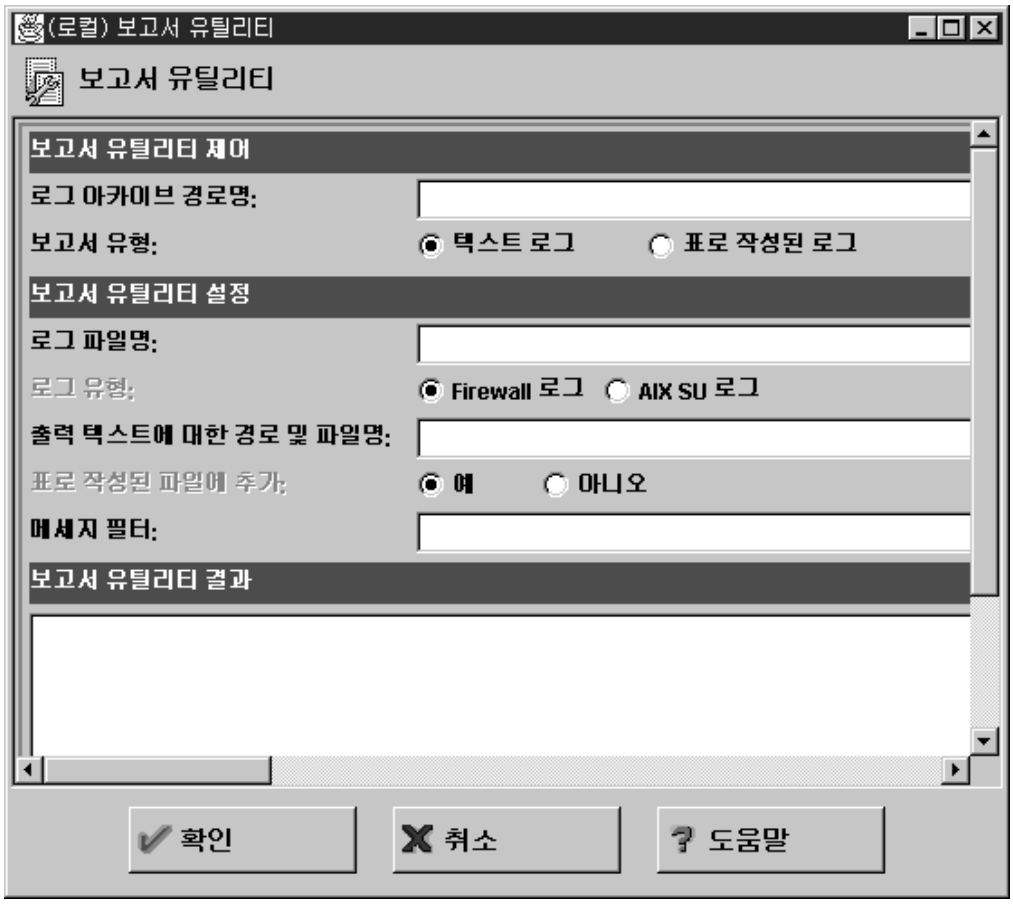


*그림 29. 보고서 유틸리티*

1. IBM Firewall과 함께 제공되는 디폴트 아카이브 프로그램의 경우, 로그 아카이브 경로 이름은 압축된 로그 파일이 들어 있는 디렉토리입니다. 로그 아카이브 경로명 필드에 **로그기능** 대화 상자의 아카이브 디렉토리 필드에서 지정한 디렉토리를 입력하십시오. 아카이브 디렉토리로의 절대 경로명을 입력하십시오. 만일 아카이브되지 않은 로그 파일을 열람하고 싶으면, 이 필드를 공백으로 남겨 놓으십시오.
2. **보고서 유형**을 선택하십시오. 확장된 로그 메세지 텍스트를 생성하려면 **텍스트 로그**를 선택하십시오. DB2 사용법에 대한 표로 작성된 파일을 작성하려면, **표 로그**를 선택하십시오. 만일 결과 파일을 DB2로 반입하면, SQL 조회를 로그 데이터에서 수행할 수 있습니다. 더 자세한 정보는 *IBM eNetwork Firewall 참조서*를 보십시오.

3. 로그 파일명은 압축된 아카이브 로그 파일 또는 다른 유효한 Firewall 로그 로그 또는 AIX su 로그 파일의 이름 중 하나입니다. 로그 아카이브 디렉토리 필드에 입력한 경우 **로그 파일명** 화살표를 눌러 작업할 로그를 선택할 수 있습니다. 단계 1에서 로그 아카이브를 입력하지 않은 경우 여기에 입력한 로그 파일명은 유효하고 압축해제된 Firewall 로그 파일이거나 AIX su 로그 파일이어야 합니다. 전체 경로를 지정해야 합니다.
4. **로그 유형**, **Firewall** 또는 **AIX su**를 선택하십시오.
5. **출력 텍스트에 대한 경로 및 파일명**을 입력하십시오.
6. 표 로그 요청의 결과를 기존의 표로 작성된 파일에 첨부하기 위해 **예**를 선택하거나 또는 기존의 파일을 대체하기 위해 **아니오**를 선택하십시오.
7. 이 필드는 출력 텍스트 파일에 놓여질 메세지의 특정 유형을 선택할 수 있게 합니다. 이 필드의 내용은 표준 Windows NT Find 명령안에 놓여지는 매개변수로 취급됩니다. 예를 들어, 필드에 ″ICA0″을 입력하면(인용 표시를 해야 합니다), 이느 마치 다음 명령을 수행하는 것과 같을 것입니다.

   ```
   fwlogtxt < my.log | find "ICA0"
   ```

   다음은 이 필드에 넣을 수 있는 몇가지 예제 항목 및 그 결과입니다.

   | 필터 | 결과 |
   |---|---|
   | "ICA0" | 로그 모니터 임계값 경보 메세지를 나열합니다 |
   | "ICA3" | Socks 관련 메세지(#ICA3000 - 3999)를 나열합니다 |
   | "ICA2010" | ICA2010 메세지의 발생만을 나열합니다 |
   | /V "ICA3" | Socks 메세지를 제외한 모든 메세지를 나열합니다 |
   | /C "ICA001" | ICA0001 메세지 수를 셉니다 |

8. **확인**을 누르면 Firewall 시스템상의 지정된 출력 디렉토리에 요청된 파일을 생성합니다.
9. 보고서 유틸리티 결과 영역은 수행된 보고서 유틸리티로부터의 오류 메세지를 보여줍니다. 텍스트 로그 보고서 유형으로부터 야기된 로그 텍스트를 보려면, 주 Firewall 구성 클라이언트 패널에서 **로그 표시기**를 누르고 완전한 자격의 출력 파일명을 입력하십시오. *IBM eNetwork Firewall 참조서*를 참조하십시오.

# 제16장 네트워크 주소 변환하기

인터넷 사용 인구가 폭발으로 성장함에 따라 IP 주소의 부족은 중요한 문제로 대두되었습니다. 네트워크 주소 변환 (NAT)은 주소 재사용을 기초로 IP 주소 부족 문제 해결책을 제공합니다.

개인 네트워크에 있는 주소는 매우 큰 주소 공간에서 지정될 수 있습니다 (일반적으로, 10.0.0.0 클래스 A 주소 공간). 이런 주소는 개인용이며 인터넷에서 노출되지 않습니다. 그러므로, 다른 IP 네트워크에서 이런 주소를 다시 사용할 수 있습니다. 등록된 IP 주소 하나는 여러 개의 개인 네트워크 주소를 숨기기 위해 사용됩니다. NAT는 등록되지 않은 주소와 포트 번호를 등록되고 유효한 인터넷 주소와 포트 번호로 변환합니다. 인바운드 방향 NAT는 등록된 인터넷 주소와 포트 번호를 등록되지 않은 주소와 포트 번호로 다시 변환합니다. 개인 또는 위법의 주소를 사용하는 네트워크가 NAT를 통해 인터넷의 호스트와 통신하여 더 많은 공간을 개인 네트워크에 효과적으로 제공할 수 있는 점이 NAT의 장점입니다.더군다나, NAT를 사용하면, 개인 네트워크에서 주소를 외부로부터 숨길 수 있으므로 보안 레벨을 하나 더 추가할 수 있게 됩니다.

보안 호스트가 생성한 TCP/UDP 패킷에서는 출발지 주소가 등록된 인터넷 주소로 대체됩니다. 보안 호스트의 포트는 고유한 포트 번호로 변환됩니다. 모든 아웃바운드 패킷의 출발지 주소는 같지만 포트 번호는 고유합니다. 이런 형태의 변환은 다-대-일(many-to-one) 변환이라고 하며, 하나의 주소로 여러 보안 호스트를 숨길 수 있습니다. IP 헤더와 TCP/UDP 허위 헤더의 패킷 체크섬이 갱신됩니다. 최대 동시 연결 수는 포트 0–1023이 예약되어 있기 때문에 64536 (실제로 64512)으로 제한됩니다. 인바운드 연결은 정적 (동적보다) 변환 테이블 항목으로 지원됩니다. 예를 들어, 호스트 193.5.8.2는 195.9.5.2 to 10.1.1.1을 맵하는 NAT 변환 테이블에 정적 항목만 있을 때 호스트 10.1.1.1의 TCP 연결을 시작합니다 (글로벌 주소 195.9.5.2 사용).

TCP/UDP 어플리케이션으로 생성된 모든 패킷은 변환됩니다. IP 패킷의 어플리케이션 데이터에 IP 주소가 있으면 어려워집니다. 주소 변환시 특히 문제가 되는 어플리케이션 하나는 FTP 입니다. FTP 제어 연결은 메세지에 ascii로 코드화된 IP 주소가 있는 ″PORT″ 명령 또는 ″PASV″ 응답을 발행합니다. 이런 경우 NAT는 IP 헤더의 주소뿐만 아니라 자료부분의 ascii 주소와 포트 번호도 수정해야 합니다.

이번의 APAR 릴리스에서 NAT의 다-대-일과 MAP 변환 옵션을 사용하면 인바운드 및 아웃 바운드 ICMP 패킷을 변환할 수 있습니다. 인바운드 ICMP 응답 패킷 (ping, 시간소인, 주소 마스크)과 모든 오류 패킷 (도달할 수 없는 목적지, 출발지 제지, 경로 재지정, 시간 초과 그리고 나쁜 패킷 메세지)은 기존의 변환 테이블 항목에 경로 재지정 예외가 있을 때만 변환됩니다. ICMP 경로 재지정은 변환되지 않은 NAT를 통과합니다. ICMP 경로 재지정 허용 또는 거부는 사용자의 필터 규칙에 달려 있습니다.

아웃바운드 조회/응답 ICMP 패킷 (ping 요청/응답, 시간 소인 요청/응답, 주소 마스크 요청/응답)은 다른 보안 호스트의 ICMP 패킷이 등록된 하나의 주소를 공유할 수 있도록 패킷 보안 주소 변환과 ICMP 조회 식별자에 의해 지원됩니다.

관리자는 보안 및 비보안 네트워크에서, 특히 주소 마스크/응답 및 경로 재지정과 같은 특정 ICMP 패킷을 전달할 때에는 신중해야 합니다. ICMP 통신량이 Firewall을 통과할 때 생길 수 있는 보안 위험에 대해서는 참고 서적 중 하나인 *NT 3.2용 IBM eNetwork Firewall을 사용한 게이트 보호*를 참조하십시오.

## IBM eNetwork Firewall NAT 구현

IBM Firewall NAT 구현은 다음과 같은 경고와 함께 앞에서 설명된 대로 기본 주소 변환을 지원합니다.

- 자료부분에 IP 주소 정보가 있는 TCP/UDP 어플리케이션 (나중에 설명된 대로 FTP 제외)에서는 앞에서 설명된 대로 패킷 헤더 필드만 변환됩니다. 이는 DSN 또는 SNMP와 같은 UDP 어플리케이션의 자료부분에 있는 주소 정보가 변환되지 않는다는 것을 의미합니다.
- FTP PORT 명령은 완전히 변환됩니다. 그러나, PASV 응답 패킷에 삽입된 주소는 변환되지 않습니다.
- ICMP 요청/응답 및 암호화 메세지는 변환됩니다. 이로서, 예를 들어, 아웃바운드 ping뿐만 아니라 TCP 경로 MTU 검색이 올바로 작동할 수 있습니다.
- NAT는 TCP 단절을 감지하기 보다는 동적 변환 테이블 항목을 제거하고 사용가능한 주소 풀에 등록된 IP 주소를 다시 삽입하기 전에 구성가능한 유휴 시간 초과에 의존합니다.

## NAT, 필터, 및 터널간의 상호작용 예

IPSec ESP 터널이 Firewall 9.67.23.2와 204.96.140.2 사이에서 수작업으로 설정되었다고 가정하십시오. NAT는 이 보안 네트워크가 개인 주소를 사용하므로 9.67.23.2. Firewall에서만 활성화됩니다. 터널의 다른 쪽 끝에 있는 보안 네트워크는 NAT를 사용하지 않습니다. 기본 NAT 변환을 설명하는 것외에 (왼쪽에서부터 두 번째 패킷의 양 필드는 아웃바운드 주소 변환 중에 수정된 패킷의 필드를 설명합니다), 0페이지의 는 또한 호스트의 변환된 패킷이 변환되지 않은 IP 패킷에서 포장됨을 설명합니다.

일반적으로, 필터링은 NAT에 앞서 아웃바운드 패킷에 적용되고 NAT 변환 이후에 인바운드 패킷에 적용됩니다. 그러므로, 필터 규칙은 변환되지 않은 주소를 기초로 합니다. NAT 및 터널이 관련될 경우, 필터 규칙은 또한 NAT가 활성화된 Firewall에서 변환되지 않은 주소를 기초로 합니다. 터널의 다른 쪽 끝에서 (이 Firewall에서 NAT가 활성화되지 않았다고 가정), 인바운드 패킷에 대한 필터 규칙은 변환된 출발지와 목적지 주소를 기초로 합니다 (인

바운드와 아웃바운드의 경우마다). NAT가 터널의 양쪽 끝에서 활성화되면, 앞에서 이루어진 설명은 양쪽 방향에 다 적용됩니다.

0페이지의 에서 설명된 시나리오를 예로 사용하고 보안 호스트 10.1.1.1의 터널을 통한 보안 호스트 204.96.145.9와의 통신을 목표로 잡았다고 했을 때, 10.1.1.1에 접속된 Firewall에는 10.1.1.1이 터널을 통해 204.96.145.9와 통신할 수 있도록 허용하는 필터 규칙이 있어야 합니다. 목적지 호스트에 연결된 다른 Firewall 쪽에서는 터널을 통한 9.67.23.1과 204.96.145.9의 통신을 허용하는 필터 규칙이 필요합니다.

## NAT의 추가 정보

다음 경우를 가능케 하려면 NAT를 사용하십시오.

- Firewall으로 보안 시스템의 주소를 보호하면서 그 시스템에서 비보안 사이트를 직접 액세스하는 경우.
- 등록된 주소가 없는 여러 시스템이 인터넷의 사이트에 다을 수 있도록 등록된 주소를 공유하는 경우.
- 비보안 위치의 기타 시스템이 Firewall으로 보호된 서버를 액세스하는 경우.

ISP에서 NAT에 대해 등록된 주소를 확보하십시오. NAT에 사용되는 모든 주소는 다른 목적으로 사용될 수 없습니다.

NAT에 대해서는 4가지 옵션이 있습니다.

**다-대-일(Many-to-One)**
: 많은 (최대 65536) 내부 주소가 등록된 하나의 IP 주소를 공유할 수 있도록 패킷 보안 주소와 포트 번호의 변환이 일어납니다. 공유되는 이 하나의 등록된 IP 주소는 로컬 주소를 숨기지만, 이 외에도, Firewall의 비보안 주소에 대해 또 다른 등록된 인터넷 주소가 필요합니다. NAT 구성은 다-대-일 항목이 관련된 포트 변환에서 사용되는 등록된 인터넷 주소를 식별합니다.

**변환**
: 변환될 보안 주소의 리스트 작성시 사용됩니다.

**제외**
: 변환되지 않을 보안 주소 리스트 작성시 사용됩니다.

**맵**
: 특정 보안 주소에 대해 등록된 특정 주소를 예약하기 위해 사용됩니다.

## 구성 클라이언트를 사용하는 네트워크 주소 변환 구성하기

1. 구성 클라이언트 네비게이션 트리에서 주소 변환 파일 폴더 아이콘을 두 번 눌러 뷰를 확장하십시오. NAT 파일 폴더 아이콘을 두 번 눌러 뷰를 확장하십시오.
2. **NAT 설정**을 선택하여 네트워크 주소 변환 모듈을 구성하십시오.
3. NAT 구성 파일에 있는 네트워크 주소 변환 항목은 이 대화 상자에 표시됩니다. NAT 항목을 추가, 변경, 또는 삭제할 수도 있습니다.

## NAT 항목 추가

1. **네트워크 주소 변환 리스트**에서 **신규**를 선택하고 **열기**를 눌러서 새로운 항목을 NAT 구성 파일에 추가하십시오.

   **NAT 추가** 대화 상자가 나타납니다.

2. **NAT 추가** 대화 상자의 NAT 유형 필드에서 화살표를 누르고 다음에서 선택하십시오.
   - 다-대-일의 등록된 네트워크 주소. 지정된 IP 주소를 예약된 IP 주소에 추가합니다. 매개변수는 예약된 IP 주소와 변환 테이블과 관련된 시간-초과입니다.
   - 보안 네트워크 주소 변환. 네트워크 주소 변환이 일어나야 하는 보안 IP 주소의 범위를 지정합니다.
   - 보안 네트워크 주소 제외. 네트워크 주소 변환에서 제외되어야 하는 보안 IP 주소의 범위를 지정합니다.
   - 보안 네트워크 주소 맵. 일대일 보안-대-등록 IP 주소 정적 변환을 정의합니다.

## 등록된 다-대-일 네트워크 주소

등록된 다-대-일 주소 항목은 많은 (최대 65536) 내부 주소가 하나의 등록된 IP 주소를 공유할 수 있도록 패킷의 보안 주소와 포트 번호를 변환합니다. 그러므로, 등록된 하나의 IP 주소를 가지고 많은 로컬 주소를 숨길 수 있습니다. (Firewall 비보안 주소에 대해 등록된 인터넷 주소를 하나 추가해야 합니다).

보안 호스트가 패킷을 비보안 네트워크로 송신하면, 등록된 IP 주소 하나가 할당됩니다. 이 고유한 IP 주소는 IBM Firewall와 보안 네트워크 밖에 있는 시스템 사이에서 IP 프레임을 전송하기 위해 사용됩니다.

NAT 추가 화면에서 다-대-일을 선택하는 경우에는 다음 값을 입력하십시오.

**등록된 IP 주소**

이를 ISP에서 확보하십시오. 이 주소는 모든 보안 주소가 숨을 수 있는 점이 찍힌 십진수 IP 주소입니다.

**선택**을 눌러 네트워크 오브젝트를 선택하여 **네트워크 오브젝트 선택** 대화 상자를 가져오십시오. 네트워크 오브젝트를 선택하고 **확인**을 누르십시오. 네트워크 오브젝트는 **NAT 구성 추가** 대화 상자의 네트워크 오브젝트 필드에 추가됩니다. 또는 네트워크 오브젝트를 아직 작성하지 못했다면, 필드에 직접 값을 입력하십시오.

**시간종료 값**

NAT가 등록된 IP 주소를 해제시킬 때까지 주소 변환이 유휴 상태로 남아 있어야 하는 시간 길이(분)를 입력하십시오. 이 시간종료 값은 이 항목에 의해 지정된 IP 주소 범위내의 등록된 IP 주소를 사용하는 주소 변환에만 적용됩니다.

디폴트 값은 15분입니다. 값의 범위는 5에서 45까지입니다.

## 보안 네트워크 주소 변환

보안 IP 주소 변환 항목은 IP 주소 변환시 NAT가 필요한 보안 네트워크 주소 세트를 정의합니다. 디폴트로 NAT는 보안 IP 주소 변환 세트에서 모든 보안 IP 주소에 주소 변환을 수행합니다.

NAT 추가 화면에서 변환을 선택한 경우 다음 값을 입력하십시오.

**보안 IP 주소**

네트워크 주소 변환이 일어나야 하는 보안 IP 주소 범위를 식별하는 점이 찍힌 십진수 IP 주소를 지정합니다.

**선택**을 눌러 네트워크 오브젝트를 선택하여 **네트워크 오브젝트 선택** 대화 상자를 가져오십시오. 네트워크 오브젝트를 선택하고 **확인**을 누르십시오. 네트워크 오브젝트는 **NAT 구성 추가** 대화 상자의 네트워크 오브젝트 필드에 추가됩니다. 또는 네트워크 오브젝트를 아직 작성하지 못했다면, 필드에 직접 값을 입력하십시오.

**보안 IP 주소 마스크**

IP 주소 범위 식별시 사용되는 보안 IP 주소에서 비트를 지정하는 서브네트 마스크와 같은 마스크를 지정합니다. 이런 마스크에서 0으로 설정된 비트는 0 또는 1이 있는 비트 위치가 IP 주소 범위에 포함된다는 것을 나타냅니다. 그러므로, 마스크에서 255.255.255.255를 지정하면 이 변환 항목에 오로지 하나의 보안 IP 주소가 포함된다는 것을 나타내는 반면, 255.255.255.0의 마스크는 클래스 C IP 주소에 주소 변환이 필요하다는 것을 나타냅니다.

## 보안 네트워크 주소 제외

보안 IP 주소 제외 항목은 IP 주소 변환시 NAT가 필요 없는 보안 네트워크 주소 세트를 정의합니다. 디폴트로 NAT는 보안 IP 주소 변환 세트에서 모든 보안 IP 주소에 주소 변환을 수행합니다.

**NAT 추가** 대화 화면에서 제외를 선택한 경우 다름 값을 입력하십시오.

**보안 IP 주소**

네트워크 주소 변환에서 제외되어야 하는 보안 IP 주소 범위를 식별하는 점이 찍힌 십진수 IP 주소를 지정합니다.

**선택**을 눌러 네트워크 오브젝트를 선택하여 **네트워크 오브젝트 선택** 대화 상자를 가져오십시오. 네트워크 오브젝트를 선택하고 **확인**을 누르십시오. 네트워크 오브젝트는 **NAT 구성 추가** 대화 상자의 네트워크 오브젝트 필드에 추가됩니다. 또는 네트워크 오브젝트를 아직 작성하지 못했다면, 필드에 직접 값을 입력하십시오.

**보안 IP 주소 마스크**

IP 주소 범위 식별시 사용되는 보안 IP 주소에서 비트를 지정하는 서브네트 마스크와 같은 마스크를 지정합니다. 이런 마스크에서 0으로 설정된 비트는 0 또는 1이 있는 비트 위치가 IP 주소 범위에 포함된다는 것을 나타냅니다. 그러므로, 마스크에서 255.255.255.255를 지정

하면 이 항목에서 오로지 하나의 보안 IP 주소가 지정된다는 것을 나타내는 반면, 255.255.255.0의 마스크는 클래스 C IP 주소에 주소 변환에서 제외된다는 것을 나타냅니다.

### 보안 네트워크 주소 맵

보안 IP 주소 맵 항목은 보안 IP 주소에서 등록된 IP 주소로의 일대일 맵핑을 정의합니다. 이 일대일 IP 주소 맵핑을 사용하면, FTP 또는 텔넷 클라이언트와 같은 외부 어플리케이션 클라이언트가 보안 네트워크에 상주하는 서버 시스템을 사용하여 TCP 세션을 설정할 수 있습니다. 보안 IP 주소 맵 항목의 등록된 IP 주소는 등록된 IP 주소 예약 항목으로 지정된 IP 주소 공간 위에 중복될 수 있습니다.

**NAT 구성 추가** 대화 상자에서 맵을 선택한 경우 다음 값을 입력하십시오.

**보안 IP 주소**
등록된 지정 IP 주소로 변환되어야 하는 점이 찍힌 십진수 IP 주소.

**선택**을 눌러 네트워크 오브젝트를 선택하여 **네트워크 오브젝트 선택** 대화 상자를 가져오십시오. 네트워크 오브젝트를 선택하고 **확인**을 누르십시오. 네트워크 오브젝트는 **NAT 구성 추가** 대화 상자의 네트워크 오브젝트 필드에 추가됩니다. 또는 네트워크 오브젝트를 아직 작성하지 못했다면, 필드에 직접 값을 입력하십시오.

**등록된 IP 주소 필드**
지정된 보안 IP 주소가 변환되어야 하는 점이 찍힌 십진수 IP 주소.

**선택**을 눌러 네트워크 오브젝트를 선택하여 **네트워크 오브젝트 선택** 대화 상자를 가져올 수 있습니다. 네트워크 오브젝트를 선택하고 **확인**을 누르십시오. 네트워크 오브젝트는 **NAT 구성 추가** 대화 상자의 네트워크 오브젝트 필드에 추가됩니다.

## NAT 항목 변경

**NAT 구성** 대화 상자에서 기존의 NAT 항목을 선택하고 **열기**를 눌러서 NAT 구성 파일의 네트워크 변환 항목을 변경하십시오.

## NAT 항목 삭제

1. **NAT 구성** 대화 상자에서 기존의 NAT 항목을 선택하고 **삭제**를 눌러 NAT 구성 파일에서 네트워크 변환 항목을 제거하십시오.

   확인 대화 상자가 나타납니다.
2. 예 또는 아니오를 선택하십시오.

## NAT 활성화

1. 구성 클라이언트 네비게이션 트리에서 주소 변환 파일 폴더 아이콘을 두 번 눌러 뷰를 확장하십시오. NAT 파일 폴더 아이콘을 두 번 눌러 뷰를 확장하십시오.
2. **NAT 활성화**를 선택하십시오.
3. 다음 중 하나를 선택하고 **실행**을 누르십시오.
   - 지정된 NAT 구성 파일에 있는 네트워크 주소 변환 항목의 유효성을 검증하십시오.
   - 구성을 활성화/갱신하여 NAT 모듈에서 현재 사용 중인 네트워크 주소 변환 항목을 표시하십시오.
   - NAT를 비활성화시켜서 네트워크 주소 변환을 사용할 수 없게 만드십시오.
   - 로깅을 사용가능하게 만들어서 네트워크 주소 변환 로깅을 작동시키십시오.
   - 로깅을 사용할 수 없게 만들어서 네트워크 주소 변환 로깅의 작동을 막으십시오.

## 로깅

NAT는 NAT 로깅과 필터 로깅이 둘 다 작동한다는 조건하에서 다양한 오류 조건을 기록합니다. NAT 로깅은 **NAT 활성화** 패널을 통해 또는 **fwnat** 명령 사용으로 작동됩니다. 필터 로깅은 **필터 로깅** 패널을 통해 또는 **fwlog** 명령 사용으로 작동됩니다.

다음 활동은 Firewall 로그 기능에 기록됩니다.

- 관리자에 의한 NAT 테이블 갱신 (예를 들어, 정적 또는 MAP 항목)
- NAT 변환 테이블에 대한 동적 갱신
- 오류 메세지
- 패킷 포기를 초래하는 실패한 변환 시도
- NAT가 활성화 및 비활성화되는 각 시간

## NAT에 대한 필터 규칙 작성

NAT 구성을 완료한 후 NAT를 사용하는 연결에 대해 필터 규칙을 작성해야 합니다. 47페이지의 『제8장 Firewall을 통해 통신량 조절』을 검색하고 직접 연결에 대한 사전정의된 서비스를 사용하십시오. 직접 연결을 위한 사전정의된 서비스의 예는 다음과 같습니다.

- HTTP 직접 아웃
- 텔넷 직접 아웃

더 자세히 알고 싶으면, 48페이지의 『사전정의된 서비스를 사용해서 연결 구축』을 참조하십시오.

네트워크에서 한 서비스를 직접 사용하려면, 이를 작성해야 합니다. 그 작성 방법에 대해서는 71페이지의 『서비스를 작성하기 위해 구성 클라이언트 사용』을 참조하십시오.

# 부록. 주의사항

이 책에서 언급하는 IBM 제품, 프로그램 또는 서비스가 IBM이 영업중인 모든 나라에서 반드시 제공되는 것은 아닙니다. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서, IBM의 제품, 프로그램 또는 서비스만을 사용해야 한다는 의미는 아닙니다. IBM의 지적 재산권이나 기타 법적으로 보호받는 권한을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. IBM에서 명시한 제품이 아닌 제품과의 결합에 따른 운영상의 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 출원중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 사용권을 부여하는 것은 아닙니다. 특허 사용권에 대한 문의는 다음 주소로 하시기 바랍니다.

150-010

서울특별시 영등포구 여의도동 25-11, 한진빌딩

한국 아이.비.엠 주식회사

지적 재산권부

T: 02-781-6028

사용권 소유자가 (i) 독자적으로 작성된 프로그램과 다른 프로그램(이 프로그램을 포함하여)간의 정보 교환이나 (ii) 교환될 정보의 상호이용등과 같은 목적으로 정보를 필요로 하는 경우에는 소프트웨어 상호운영 담당자에게 문의하실 수 있습니다. 기타 자세한 문의사항은 아래 주소를 이용하시기 바랍니다.

150-010

서울특별시 영등포구 여의도동 25-11, 한진빌딩

한국 아이.비.엠 주식회사

소프트웨어 사업본부

T: 02-781-7777

이러한 정보는 사용료등을 비롯한 해당 기간 및 조건에 따라 사용이 가능합니다.

이 책에 기술된 사용권 프로그램과 여기에 사용할 수 있는 모든 사용권 자료는 IBM 고객 협의하에 IBM에서 제공합니다.

이 책은 제품 사용을 위한 것이 아니며, 어떠한 종류의 보증도 없이 있는 그대로 제공되므로, 판매 가능성을 보장하거나 특정 목적에 적합한지 여부에 대해서는 책임질 수 없습니다.

이 제품에는 캘리포니아 주립 대학, Berkeley 및 그 연구진들에 의해 개발된 소프트웨어가 포함됩니다.

## 등록상표

다음 용어는 미국과 다른 나라에서 영업 중인 IBM사의 등록상표입니다.

- Common User Access
- DB2
- eNetwork
- IBM
- OS/2

Microsoft, Windows, Windows NT 그리고 Windows 95 로고는 Microsoft사의 등록상표입니다.

Java 및 HotJava는 Sun Microsystems, Inc.의 등록상표입니다.

이중 별표(**)가 붙은 다른 회사, 제품 및 서비스 이름은 타사의 등록상표이거나 서비스 표시입니다.

# 참고 문헌

인터넷상의 보안에 대한 추가 정보를 보려면, **http://www.software.ibm.com/enetwork/firewall**에서 IBM eNetwork Firewall 홈 페이지를 찾아보십시오.

## IBM 서적에 포함된 정보

Firewall, 인터넷 보안 및 일반 보안 항목에 대한 정보와 관련된 기타 IBM 소스는 여기에 나열되어 있습니다.

### Firewall 주제항목

다음 문서는 IBM Firewall CD-ROM과 IBM eNetwork Firewall 홈 페이지에서 사용할 수 있습니다.

- *IBM eNetwork Firewall 사용자 안내서*, GC31-8658
- *IBM eNetwork Firewall 참조서*, SC31-8659
- *NT 3.2용 IBM eNetwork Firewall을 사용한 게이트 보호*, SG24-5209

### 인터넷 및 월드 와이드 웹

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694
- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

### 일반 보안 주제항목

- *The Basics of IP Network Design*, SG24-2580
- *Elements of Security: AIX V4.1*, GG24-4433
- *Enterprise-Wide Security Architecture and Solutions Presentation Guide*, SG24-4579
- *HACMP/6000 Customization Examples*, SG24-4498
- *IBM Global Network (IGN) Security Policy*, GC34-2206
- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC24-8135
- *IBM Systems Monitor: Anatomy of a Smart Agent*, SG24-4398
- *Security Overview of Open Systems Networking*, GG24-3815
- *Systems Monitor for AIX User's Guide*, SC31-8173
- *TCP/IP Tutorial and Technical Overview*, GG24-3376

## 산업 서적에 포함된 정보

이러한 산업 출판물은 TCP/IP 및 UNIX에 관련된 것입니다.

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail*. O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration*. O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)
- Nemeth, Snyder, et al. *UNIX System Administration Handbook*. Prentice Hall. (ISBN: 0-13-151051-7

이러한 산업 출판물은 인터넷상의 Firewall과 보안에 관련된 것입니다.

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)
- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, Willam R., and Steven M. Bellovin. *Firewalls and Internet Security*. New York: Addison-Wesley, 1994. (ISBN: 0201633574)
- Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995. (ISBN: 1562054716)
- Curry, David. *UNIX System Security: Guide for Users and Systems Administrators*. Sebastopol, CA: O'Reilly and Associates, 1994. (ISBN: 0201563274)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX Security*. Sebastopol, CA: O'Reilly and Associates, 1991. (ISBN: 0937175722)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX and Internet Security*. Sebastopol, CA: O'Reilly and Associates, 1996. (ISBN: 1565921488)
- Hare, Chris, and Karanjit Siyan. *Internet Firewalls and Network Security*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562056328)
- Randall, Neil. *Teach Yourself the Internet in a Week*. Indianapolis, IN: Sams.Net, 1995. (ISBN: 0672307359)
- Stallings, William. *Internet Security Handbook*. Foster City, CA: IDG Books, 1995. (ISBN: 0077092546)
- Stevens, W. Richard. *TCP/IP Illustrated*. Reading, MA: Addison-Wesley, 1994. (ISBN: 0201634953)

# 용어

**http://www.networking.ibm.com/nsg/nsgmain.htm**에서 IBM 소프트웨어 용어집에 액세스할 수 있습니다.

# 색인

## [ 아 ]



## [ 자 ]



## [ 차 ]



## [ 카 ]



## [ 타 ]



## [ 파 ]



## [ 하 ]



## D



## E



## F



## H

# I



# M



# N



# S



# T



# U

Printed in Korea

GC31-8658-01