Windows NT용 IBM eNetwork Firewall

참조서

버전 3 릴리스 2.1.1

SC31-8659-01

Windows NT용 IBM eNetwork Firewall

참조서

버전 3 릴리스 2.1.1

SC31-8659-01

주

이 책과 이 책에서 지원하는 제품을 사용하기 전에 143페이지의 『주의사항』을 읽으십시오.

재판 (1998년 6월)

이 책은 Windows NT용 IBM eNetwork Firewall 버전 3 릴리스 2.1.1에 적용됩니다 (제품 번호 5765-C16). 이는 SC31-8659-00 대신 사용됩니다.

목차

이 책에 관하여

이 책은 Windows NT** 시스템에서 IBM eNetwork Firewall 버전 3.2를 설치, 관리 및 사용하는 네트워크 또는 시스템 보안 관리자를 위한 참조서로 고안되었습니다. 텔넷 또는 FTP와 같은 클라이언트 프로그램을 사용하려면, TCP/IP 클라이언트 프로그램에 대한 사용자 안내서를 참조하십시오.

사전 지식

IBM eNetwork Firewall을 설치하고 구성하기 전에 TCP/IP 및 네트워크 관리에 대해 적절한 지식을 갖추는 것이 중요합니다. 사용자 네트워크 내부 및 외부의 액세스를 제어하는 Firewall을 설정 및 구성하게 되므로, 우선 네트워크가 작동되는 방법을 이해해야 합니다. 특히, IP 주소, 완전 규정 이름 및 서브네트 마스크의 기초를 이해해야 합니다.

netstat, arp, ifconfig, ping, nslookup, DNS, sendmail, 경로지정 및 더 많은 정보가 다루어지는 TCP/IP에 대한 가장 좋은 책은 *TCP/IP Network Administration* 입니다. 자세한 내용은 *참고 문헌*을 참조하십시오.

TCP/IP 및 경로지정, 네트워크 하드웨어, DNS 및 sendmail의 개요가 나와 있는 UNIX 관리 수행을 위한 좋은 책은 *UNIX System Administration Handbook* 입니다. 자세한 내용은 *참고 문헌*을 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 프로토콜 버전 5를 통한 회선 레벨 게이트웨이, 인터넷 표준
3. 필터링—통신량이 허용되거나 거부될 수 있는 확장된 일련의 강력한 기준. 기준에는 TCP/IP 주소, 포트, 프로토콜, 방향, 어댑터(보안/비보안) 등이 포함됩니다.

   다수의 사전정의된 서비스는 설정을 신속하게 만듭니다.

Socks 프로토콜 버전 5

그 단순성 및 융통성 외에도, Socks 프로토콜 버전 5에는 다음과 같은 장점이 있습니다.

- 사용자 확인 및 암호화 방법의 쉬운 전개
- UDP 기반의 프록시 회선을 통과를 위한 가상 프록시 회선을 작성하는 UDP 연합.
- 실시간 socks 성능 정보를 표시하는 Socks V5 감시자

네트워크 주소 변환

인터넷 사용자의 폭발적인 증가로 IP 주소 부족은 중요한 문제로 대두되고 있습니다. 네트워크 주소 변환(NAT)은 주소 재사용을 기초로 IP 주소 감소 문제에 대한 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 Firewall로 액세스를 더 제어할 수 있는 다른 레벨의 권한 레벨이 지정될 수 있습니다. 이처럼 이해하기 쉬운 단일 그래픽 사용자 인터페이스(GUI)는 Windows NT Firewall과 AIX Firewall을 관리하는 데 사용할 수 있습니다.

NT 안정화

Firewall이 설치되면, TCP/IP 이외의 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 데이터베이스 엔진으로 반출된 후 시스템 로그에 대해 다시 SQL 조회를 실행할 수 있습니다.

경보, 모니터 및 기록

확장된 상세한 로깅에는 TCP/IP 주소, 사용자 ID, TOD, 파일명, 포트 번호를 포함하는 모든 Firewall 활동이 포함됩니다. 또한 로그 모니터가 들어 있어 의심스러운 활동을 감시하고 임계값이 초과될 때 경고를 보냅니다.

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 한자, 정체 한자, 이탈리아어, 스페인어 및 브라질 포르투갈어에 대해 제공됩니다.

IP 주소 입력

Firewall을 구성하는 경우, IP 주소를 입력하도록 요구합니다. 완전한 점으로 구분된 IP 주소를 모두 4개의 8진수를 사용하여 다음과 같은 형식으로 입력해야 합니다.

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

여기서 각각의 nnn은 범위 000–255 사이의 3 숫자 세트입니다.

IBM 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). 전화 번호는 1-800-237-5511 입니다.

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

제1장 IBM Firewall 명령 행 인터페이스 사용

이 장에서는 IBM eNetwork Firewall 명령 행에서 사용할 수 있는 명령을 설명합니다.

다음 정보는 명령에 적용됩니다.

- 이 책에 나열된 명령은 다음과 같은 구문을 사용합니다.
  - 밑줄은 이것이 사용자 입력 데이터임을 지시합니다.
  - []는 매개변수가 선택적임을 나타냅니다.
  - {}는 매개변수 선택사항이 있음을 나타냅니다.
  - |는 선택사항을 구분합니다.
- 모든 매개변수는 `keyword=value` 형식을 사용합니다.
- 하나의 매개변수가 복수의 값을 갖는 경우 값을 큰 따옴표로 묶거나 공백으로 구분해야 합니다. 예를 들면 다음과 같습니다.

  ```
  secaddr="11.22.33.1 11.22.33.2"
  ```

- 큰 따옴표로 묶이지 않은 경우 매개변수내에 공백을 포함시키지 마십시오.
- 하나 이상의 필수 매개변수를 생략하는 경우, 명령 행 유틸리티가 누락된 매개변수를 나열합니다.
- 매개변수에 대한 잘못된 값을 입력하는 경우, 명령 행 유틸리티에서 오류를 보고합니다.
- 일부 Firewall 서비스는 그 구성 파일 변경시 그 동작을 동적으로 갱신합니다. 일부는 갱신(update) 하위 명령을 필요로 합니다. `update` 하위 명령은 명령어를 필요로하는 Firewall 서비스에 제공됩니다.
- 1차 Firewall 관리자만이 명령 행에서 프로그램을 실행할 수 있습니다.
- 복잡성 및 파일 상호 의존성으로 인해, **임의의 구성 파일을 직접 편집하지 마십시오.**

구성 서버

`fwcfgsrv` 명령은 구성 서버의 옵션을 나열하거나 변경합니다. 관리자는 이 명령을 실행하기 위해 통신 제어 기능을 관리할 수 있는 권한 레벨을 가져야 합니다.

구성 서버 옵션을 나열하려면, 다음 명령을 발행하십시오.

```
fwcfgsrv cmd=list
```

`fwcfgsrv` 명령의 출력 결과는 다음과 같이 나타납니다.

```
localonly = yes/no
encryption = none/ssl
sslfile = filename if one is defined
```

구성 서버 옵션을 변경하려면, 다음 명령을 발행하십시오.

```
fwcfgsrv cmd=change
         [localonly={yes|no}]
         [encryption={none|ssl}]
         [sslfile=]
```

매개변수는 다음과 같이 정의됩니다.

localonly
Firewall이 로컬 시스템에 의해서만 관리될 수 있는지 여부를 지정합니다. 유효한 값은 yes 또는 no입니다.

encryption
SSL을 통해 수신 데이터가 암호화될지 여부를 지정합니다. 유효한 값은 none 또는 ssl입니다.

sslfile SSL 암호화에 사용될 SSL 키 파일명을 지정합니다. 59페이지의 『제 6장 Make Key File 유틸리티 사용(MKKF)』을 참고하십시오.

도메인 이름 서비스

도메인 이름 서비스(DNS)는 보안 네트워크 안에 있는 호스트에 완전한 도메인 이름 서비스를 제공하는 반면 보안 네트워크 외부의 호스트에는 최소한의 정보를 제공합니다. 이를 이루기 위해서는 3개의 도메인 이름 서버가 필요합니다.

- Firewall에 있는 하나의 서버
- 하나는 보안 네트워크 내에서
- 보안 네트워크 외부에 있는 하나의 서버.

자세한 내용은*IBM eNetwork Firewall 사용자 안내서*를 참고하십시오.

주:

1. x.x.x.x는 점으로 구분된 십진수 형식의 IP 주소입니다.
2. secaddr 및 remaddr 매개변수의 값은 하나의 IP 주소이거나 IP 주소 리스트일 수 있습니다. IP 주소 리스트를 지정하는 경우, 리스트는 공백으로 구분되어야 하며 큰 따옴표로 묶여야 합니다.
3. 중복된 주소가 감지되었으며 오류로 표시됩니다.
4. 맨 처음 DNS를 구성하면, `fwdns cmd=change`가 새로운 파일을 작성합니다. Firewall은 항상 정확히 하나의 구성 레코드만을 갖습니다. 값은 비어 있을 수도 있습니다. 변경 하위 명령으로 DNS 레코드의 임의의 또는 모든 값을 변경할 수 있습니다.

다음 명령은 현재 DNS 구성을 나열합니다.

```
fwdns cmd=list
```

DNS 구성 항목을 변경하고 새로운 파일을 작성하려면, 다음을 사용하십시오.

```
fwdns cmd=change
    secdomain=SecureDomainName
    secaddr=x.x.x.x | "x.x.x.x  x.x.x.x  x.x.x.x"
    remaddr=x.x.x.x | "x.x.x.x  x.x.x.x  x.x.x.x"
```

매개변수는 다음과 같이 정의됩니다.

secdomain=*SecureDomainName*
내부, 보안 네트워크의 도메인 이름

secaddr=*SecureDNSaddr[,...]*
보안 도메인 이름 서버의 IP 주소

remaddr=*NonSecureDNSaddr[,...]*
인터넷 연결 서비스 제공자가 제공하는 보안된 네트워크 외부에 있는 도메인 이름 서버의 IP 주소.

필터

fwfilter 명령을 사용하면, 필터를 활성화 또는 비활성화할 수 있습니다.

```
fwfilter cmd=update | verify | list | shutdown | startlog |
stoplog
```

매개변수는 다음과 같이 정의됩니다.

fwfilter cmd=update
구성을 재작성하고 해당 규칙 세트를 활성화합니다.

fwfilter cmd=verify
구성에 대한 "검사 작성" 을 수행하지만 변경사항을 활성화하지는 않습니다.

fwfilter cmd=list
가장 최근에 작성된 구성을 나열합니다.

fwfilter cmd=shutdown
필터 메카니즘을 비활성화합니다.

fwfilter cmd=startlog
Firewall 로그 기능에 선택한 통신량을 기록합니다.

fwfilter cmd=stoplog
Firewall 필터 로깅을 중지합니다.

HTTP 프록시

HTTP 프록시는 Web 브라우징에 대한 Socks 서버 없이 IBM Firewall을 통해 브라우저 요청을 효율적으로 처리합니다. 사용자는 그 인터넷 네트워크의 보안을 위협하지 않으며 HTTP 프록시를 구현할 그 클라이언트 환경을 변경하지 않고 인터넷에서 유형한 정보에 액세스할 수 있습니다.

fwhttp 명령은 현재 HTTP 프록시 구성을 나열하거나 변경합니다.

현재 HTTP 프록시 구성을 나열하려면, 다음 명령을 사용하십시오.

```
fwhttp cmd=list
```

현재 HTTP 프록시 구성을 변경하려면, 다음 명령을 사용하십시오.

```
fwhttp cmd=change
       [port=]
       [maxcontentlengthbuffer=]
        [minactivethreads=]
        [maxactivethreads=]
        [idlethreadtimeout=]
        [logging=]
        [authenticate=]
        [authenticatetimeout=]
        [maxpersistrequests=]
        [persisttimeout=]
```

매개변수는 다음과 같이 정의됩니다.

port HTTP 프록시 서비스가 연결대기를 수행하는 포트.

maxcontentlengthbuffer
목차 길이 헤더의 추가 내용의 반환을 허용하는 문서를 반환하기 위해 필요한 최대 버퍼 크기.

minactivethreads
초기화시에 시작하여 수행시에 활동 상태를 유지하는 최소 작업 쓰레드 수.

maxactivethreads
언제든지 실행될 수 있는 최대 작업 쓰레드 수.

idlethreadtimeout
유휴 쓰레드를 사용 가능 상태로 유지하는 시간.

logging
HTTP 활동에 대한 로깅을 수행할지 여부를 지정합니다. 해당 값은 on 또는 off입니다.

authenticate
확인할 사용자의 레벨. 해당 값은 all, none 또는 new입니다.

authenticatetimeout
지속 연결을 설정한 후에 클라이언트 요청을 대기하는 시간.

maxpersistrequests
지속 연결 상에서 수신할 최대 요청 수.

persisttimeout
지속 연결을 유지하는 시간.

인터페이스

보안 인터페이스는 내부 네트워크에 있는 호스트의 네트워크인 보호하려는 네트워크에 IBM Firewall 호스트를 연결합니다. **Firewall이 작동되게 하려면 하나 이상의 보안 인터페이스가 있어야 합니다.** 비보안 인터페이스는 하나 이상의 외부 네트워크 또는 인터넷에 IBM Firewall을 연결합니다. IBM Firewall에는 최소한 하나의 비보안 인터페이스가 있어야 합니다.

이 명령을 실행하면 Firewall의 네트워크 인터페이스가 나열됩니다. 관리자는 이 명령을 실행하기 위해 인터페이스 기능을 관리할 수 있는 권한 레벨을 가져야 합니다.

```
fwinterface cmd=list
       [addr=x.x.x.x]
```

관리자 권한 레벨에 대한 자세한 내용은 *IBM eNetwork Firewall 사용자 안내서*의 관리자 장을 참고하십시오.

매개변수는 다음과 같이 정의됩니다.

addr=x.x.x.x

Firewall에 대해 구성되어 있는 모든 네트워크 인터페이스를 나열하고 각각을 보안 또는 비보안 인터페이스로 구분합니다. 이름도 식별될 수 있습니다. 선택적인 addr 매개변수를 지정하면 해당 어댑터만 나열됩니다. addr에 대해 점분리 십진 IP 주소가 제공되면 이 IP 주소가 Firewall에 대해 구성되었다고 할 때 그 주소, 상태 및 지정된 주소의 이름만 이 리스트에 포함됩니다.

이 명령을 실행하면 Firewall에 대해 네트워크 인터페이스를 정의할 수 있습니다. 관리자는 이 명령을 실행하기 위해 인터페이스 기능을 관리할 수 있는 권한 레벨을 가져야 합니다.

```
fwinterface cmd=change
           addr=x.x.x.x
           [state={secure|nonsecure}]
           [name=]
```

매개변수는 다음과 같이 정의됩니다.

addr=x.x.x.x

변경될 인터페이스의 주소가 점분리 십진수로 포함됩니다. 해당 인터페이스가 Firewall에 대해 정의되어 있지 않으면 오류가 보고됩니다.

state={secure|nonsecure}

지정된 인터페이스에 접속된 네트워크를 분류하는 두 키워드 "보안" 또는 "비보안" 중 하나가 포함됩니다.

name 인터페이스나 이 인터페이스가 연결된 네트워크를 나타내는 의미있는 이름입니다. 큰 따옴표가 붙여 있으면 공백도 포함될 수 있습니다.

state 및 name 매개변수가 모두 생략 가능하지만 둘 중 하나는 반드시 지정되어야 합니다.

로그 아카이버

다음 명령은 아카이브하도록 구성된 로그 기능을 유지보수하기 위해 로그 파일 아카이버를 호출합니다.

```
fwlogmgmt -1 or fwlogmgmt -a
```

이 명령을 Windows NT 예정 서비스(Scheduled Service)에 넣는 것이 좋습니다. 자세한 내용은*IBM eNetwork Firewall 사용자 안내서*를 참고하십시오.

로그파일 관리

로그 파일 관리는 로그 및 아카이브 파일을 정의하고 관리합니다. fwlog 명령은 로그 기능을 추가, 변경 및 삭제합니다.

로그 기능을 추가하려면, 다음 명령을 발행하십시오.

```
fwlog cmd=add
      facility=Facility
      priority=Priority
      logfile=LogFileName
       [arcfile=ArchivePath
      logtime=DaysToKeepInLog
      arctime=DaysToKeepInArchive
```

기능에 대하여 유효한 값은 다음과 같습니다:

- Firewall (local4) - 필터 로깅을 포함한 일반 Firewall 로그
- alert (local1) - 경보 화면에 상주하는 데 사용되는 로그 모니터 디먼 상태와 임계값 위반 경고
- adminaudit (local0) - 관리 감사 로그
- mail - 전자우편 로그

우선순위에 대하여 유효한 값은 다음과 같습니다:

- debug
- info
- warning
- error
- crit

logfile 매개변수는 Firewall 로깅 항목이 송신될 위치를 지정합니다. 유효한 logfile 값은 로그 항목이 기록될 파일을 나타내는 완전한 규정화 파일명(형식 drive:\directory를 가짐)입니다.

주: 경보 로그 또는 Firewall 로그 기능에 대해 식별되는 파일은 서로 달라야 하며, Firewall 기능이 이들 파일을 처리하는 데 사용될 경우 또다른 로그 기능에 대한 파일과 달라야 합니다.

Firewall 로그 메세지만이 보고서 유틸리티에 대한 파일 입력에 표시되는 것은 중요합니다. 다른 어떤 기능도 Firewall 로그나 경보 로그와 동일한 파일에 지정되어서는 안됩니다.

arcfile, logtime 및 arctime 매개변수는 생략 가능하며 logfile 매개변수가 파일명을 지정할 때만 유효합니다. 어떤 것을 지정하든지 세 매개변수가 모두 지정되어야 합니다. 이러한 매개변수는 로그 아카이브(archival)를 제어합니다. 실제 아카이브(archival)를 발행하려면, `fwlogmgmt` 명령을 정기적으로 수행하십시오. 6페이지의 『로그 아카이버』를 참고하십시오.

디폴트로, Firewall은 이들 매개변수를 사용하여 아카이브 로그 레코드를 저장하는 위치와 아카이브가 발생하는 회수를 나타냅니다. 아카이브를 작동하기 위해서는 이들 세 가지 매개변수를 지정해야 합니다.

아카이브 기능은 플러그인을 아카이브하는 Firewall을 작성하여 대체할 수 있습니다. 49페이지의 『제4장 로그 아카이버 플러그인 소프트웨어 개발 키트』를 참고하십시오.

arcfile 매개변수에는 완전히 규정된 경로가 들어 있어야 합니다.

logtime 매개변수는 Firewall 로깅 항목이 아카이브로 이동되기 전에 로그 파일에 남아 있는 최소 일 수를 나타냅니다.

arctime 매개변수는 Firewall 로깅 레코드가 삭제되기 전에 아카이브에 남아 있는 최소 일 수를 나타냅니다.

로그 기능을 변경하려면, 다음 명령을 발행하십시오.

```
fwlog cmd=change
        index=Index
        [facility=Facility]
        [priority=Priority]
        [logfile=LogFileName]
        [arcfile=ArchiveFileName]
        [logtime=DaysToKeepInLog]
        [arctime=DaysToKeepInArchive]
```

수행한 변경(특히 초기 인스턴스의 경우)이 올바른 구문의 구성 파일을 작성하는 데 실패하면 (예를 들어 작성된 로그 파일 구성에 누락된 필드가 있는 경우) 경고가 나타나고 Firewall은 데이터를 기록하지 않게 됩니다.

로깅을 수행하지만 아카이브는 수행하지 않으려는 경우, **facility**, **priority** 및 **logfile** 매개변수만이 필요합니다. 일단 시작된 로그 아카이브를 사용불가로 만들려면 **archive**, **logtime** 및 **arctime** 매개변수를 비워 두십시오. 아카이브(archival) 작업을 예정에 넣은 경우, 이를 삭제하십시오.

현재 로그 파일 구성 데이터를 나열하려면, 다음 명령을 발행하십시오.

```
fwlog cmd=list
```

fwlog cmd=list 명령에서 항목에 대하여 반환된 인덱스 번호에 지정된 Firewall 로그 항목을 삭제하려면, 다음 명령을 발행하십시오.

```
fwlog cmd=delete
      index=삭제할 항목의 인덱스
```

로그모니터

로그 모니터 명령을 사용하면, 경보를 트리거하는 시기와 방식을 로그 모니터에게 알려 줄 수 있습니다. 이 명령(또는 해당 구성 클라이언트 패널)에 지정된 임계값이 지정된 시간 간격에 도달할 경우 경보가 발생합니다. 경보가 발생하면 다음이 실행됩니다.

1. 레코드가 Firewall 경보 기능 및 Firewall 로깅 기능에 쓰여집니다.
2. 지정된 명령이 수행됩니다.
3. 알림이 하나 이상의 사용자 ID(들)에게 송신됩니다.
4. 메세지가 호출 디바이스로 송신됩니다.

마지막 세 조치는 여기에 지정된 값을 적절히 구성하여 제어할 수 있습니다.

로그 모니터 설정 나열

```
fwlogmon cmd=list
```

경보 발생시 전자우편 통지를 수신하는 사용자 ID 지정

경보가 발생할 때(사용자가 추가한 각 ID에 알림이 송신될 때) 전자우편 통지를 수신하는 사용자 ID를 지정하려면, 다음을 수행하십시오.

```
fwlogmon cmd=add|delete
         type=id
         username=
         [comment=]
```

경보 발생시 수행할 명령 지정

```
fwlogmon cmd=add|change
         type=command
         command=
         [comment=]

fwlogmon cmd=delete
         type=command
```

성공하지 못한 로그인 시도 수에 기초하여 경보가 트리거되는 임계값 지정

```
fwlogmon cmd=add
         type=single|multi|host
         count=
         time=
         pager=
         [comment=]

fwlogmon cmd=change
         type=single|multi|host
         [count=]
         [time=]
         [pager=]
         [comment=]
```

```
fwlogmon cmd=delete
         type=single|multi|host
```

지정된 Firewall 메세지 ID의 발생 수에 기초하여 경보가 트리거되는 임계값 지정

```
fwlogmon cmd=add
         type=msg
         tag=
         count=
         time=
         pager=
         [comment=]

fwlogmon cmd=change
         type=msg
         tag=
         [count=]
         [time=]
         [pager=]
         [comment=]

fwlogmon cmd=delete
         type=msg
         tag=
```

매개변수는 다음과 같이 정의됩니다.

type 추가 또는 변경 중인 로그 모니터 명령 특성의 유형을 식별합니다.

허용된 값은 id, command, msg, single, multi 및 host입니다.

id 알림을 송신할 사용자 ID에 영향을 줍니다.

command
실행될 명령을 지정합니다.

msg 특정 로그 메세지의 모니터에 영향을 줍니다.

single 단일 사용자 ID에 기반한 모니터링에 영향을 줍니다. 카운터는 실패한 시도를 가진 각 ID에 대해 유지됩니다. 임의 ID의 카운터가 이 명령에 지정된 임계값에 도달하면, 경보가 트리거됩니다.

multi 복수 사용자 ID에 기반한 모니터링에 영향을 줍니다. 실패한 시도를 가진 모든 사용자 ID에 대한 모든 카운터의 총 수가 이 명령에 지정된 임계값에 도달하면, 경보가 트리거됩니다.

host 호스트명에 기반한 모니터링에 영향을 줍니다. 카운터는 실패한 시도가 발생한 각 호스트명에 대해 유지됩니다. 임의 호스트명의 카운터가 이 명령에 지정된 임계값에 도달하면, 경보가 트리거됩니다.

username
임의 경보를 통지받는 Firewall 관리자 또는 다른 사용자의 전자우편 ID. 보안 전자우편 서버를 적절히 구성한 경우에만 경보 통지가 성공적으로 전송됩니다.

command
임의 경보가 발생할 때 실행되는 명령의 이름입니다. 이것은 실행 파일의 완전한 경로명이어야 합니다. 이는 .bat 파일이 될 수 있으며, 그 파일 안에서 복수 명령의 실행을 허용할 수 있습니다. 그런데 .bat 파일이 다른 파일에 대한 참조를 작성하면 그 참조도 완전한 경로명 참조이어야 합니다.

count 경보가 사용될 때 실패 수의 임계값 또는 특정 로그 메세지의 발생을 설정합니다.

time 분 단위의 시간 간격을 설정합니다. count는 이벤트의 트리거를 위해 첫 번째 발생으로부터 이 시간 간격 안으로 도달되어야 합니다. 지금으로부터 이 간격보다 오래된 발생은 count에서 삭제됩니다.

pager 관련 임계값이 경보를 트리거할 때 페이지 사용 여부를 지정합니다. 활성 호출기 구성은 페이지를 송신하는 데 사용됩니다.

tag 모니터되는 로그 메세지 태그(ICA라는 접두사를 가진 메세지의)입니다. 로그 모니터 메세지(1000개 이하의 ICA 태그)는 모니터할 수 없습니다.

전자우편

fwmail 명령을 사용하면 공용 및 보안 전자우편 도메인을 대응할 수 있습니다.

```
fwmail cmd=list

fwmail cmd=add
        secdomain=
        mail=
        remdomain=

fwmail cmd=change
        secdomain=
        [mail=]
        [remdomain=]

fwmail cmd=delete
        secdomain=
```

매개변수는 다음과 같이 정의됩니다.

secdomain
설명되고 있는 전자우편 도메인에 대해 Firewall의 보안 부분에 있는 사용자가 알고 있는 이름입니다.

mail 전자우편 서버의 주소입니다.

remdomain
설명되고 있는 전자우편 도메인에 대해 Firewall의 비보안 부분에 있는 사용자가 알고 있는 이름입니다.

네트워크 주소 변환

네트워크 주소 변환(NAT)은 보안된 IP 네트워크 내부의 주소를 다른 IP 네트워크에서 다시 사용할 수 있도록 함으로써 IP 주소 감소 문제에 대한 해결책을 제공합니다.

NAT는 4 가지 유형의 구성을 지원합니다.

- 다-대-일의 등록된 주소 - 다-대-일 변환에서는 많은 (최대 65536) 내부 주소가 하나의 등록된 IP 주소를 공유할 수 있도록 패킷의 보안 주소와 포트 번호를 변환하는 작업이 일어납니다. 이 공유된 하나의 IP 주소는 로컬 주소를 숨기지만, 이 외에도 Firewall만을 위한 또 하나의 등록된 인터넷 주소가 필요합니다.
- 보안된 IP 주소 변환 - 보안된 IP 주소 변환 항목은 IP 주소 변환을 수행하기 위하여 NAT를 필요로하는 보안된 네트워크 주소 세트를 정의합니다. 기본적으로, 네트워크 주소 변환 프로그램은 모든 보안된 IP 주소에 관한 주소 변을 수행합니다.
- 보안된 IP 주소 제외 - 보안된 IP 주소 제외 항목은 IP 주소 변환을 수행하기 위해 NAT를 필요로하지 않는 보안된 네트워크 주소 세트를 정의합니다. 기본적으로, 주소가 보안된 IP 주소 제외 항목에서 지정하는 범위 안에 있지 않은 경우 네트워크 주소 변환 프로그램은 모든 보안된 IP 주소에 관하여 주소 변환을 수행합니다.
- 보안된 IP 주소 대응 - 보안된 IP 주소 대응 항목은 보안 IP 주소에서 등록된 IP 주소로의 일대일 대응을 정의합니다. 이러한 일대일 IP 주소 대응을 사용하여 FTP 또는 텔넷 클라이언트와 같은, 외부 응용 프로그램 클라이언트가 보안된 네트워크내에 거주하는 서버 시스템과의 TCP 세션을 설정할 수 있습니다.

NAT 명령의 구문은 다음과 같습니다.

```
fwnat
cmd=list | update | verify |shutdown | startlog | stoplog
```

매개변수는 다음과 같이 정의됩니다.

fwnat cmd=list
현재 NAT 구성을 나열합니다.

fwnat cmd=update
NAT 엔진을 최신으로 고칩니다.

fwnat cmd=verify
구성을 구문 검토합니다.

fwnat cmd=shutdown
모든 주소 변환을 중지합니다.

fwnat cmd=startlog
각 변환된 패킷 로깅을 시작합니다.

fwnat cmd=stoplog
각 변환된 패킷 로깅을 중지합니다.

다-대-일 항목을 NAT 구성에 추가하려면, **type=many-to-one**을 사용하십시오.

```
fwnat cmd=add
       type=many-to-one
       addr=Addr
       [timeout=minutes]
```

매개변수는 다음과 같이 정의됩니다.

type=many-to-one
다-대-일(many-to-one) 항목을 추가합니다.

addr=*Addr*
등록된 주소 풀에 추가된 등록된 IP 주소의 범위를 식별하는 주소입니다.

timeout=*minutes*
NAT가 등록된 IP 주소를 해제시킬 때까지 주소 변환이 유휴 상태로 남아 있어야 하는 시간 길이 (분). 디폴트 값은 15이고 범위는 5–45입니다.

NAT 구성에서 다-대-일 항목을 수정하려면, 다음 구문을 사용하십시오.

```
fwnat cmd=change
       index=
       [addr=Addr]
       [timeout=minutes]
```

매개변수는 다음과 같이 정의됩니다.

색인 fwnat cmd=list를 실행할 때 특정 NAT 항목의 왼쪽 컬럼에 숫자가 있습니다. 색인 매개변수로 특정 NAT 항목에 대한 숫자를 사용하십시오.

addr=*Addr*
등록된 주소 풀에 추가된 등록된 IP 주소의 범위를 식별하는 주소입니다.

timeout=*minutes*
NAT가 등록된 IP 주소를 해제시킬 때까지 주소 변환이 유휴 상태로 남아 있어야 하는 시간 길이 (분). 디폴트 값은 15이고 범위는 5–45입니다.

NAT 구성에 변환 항목을 추가하려면 **type=translate**를 사용하고, NAT 구성에서 항목으 제외하려면 **type=exclude**를 사용하십시오.

```
fwnat cmd=add
       type={translate|exclude}
       addr=Addr
       mask=Mask
```

매개변수는 다음과 같이 정의됩니다.

type=translate
translate 항목을 추가합니다.

type=exclude
exclude 항목을 추가합니다.

addr=*Addr*
변환을 요구하는 보안된 IP 주소 범위를 식별하는 IP 주소입니다.

mask=*Mask*
IP 주소 범위를 식별합니다.

NAT 구성 파일의 변환 또는 제외 항목을 변경하려면, 다음과 같은 구문을 사용하십시오.

```
fwnat cmd=change
       index=
       [addr=Addr]
       [mask=Mask]
```

매개변수는 다음과 같이 정의됩니다.

색인 fwnat cmd=list를 실행할 때 특정 NAT 항목의 왼쪽 컬럼에 숫자가 있습니다. 색인 매개변수로 특정 NAT 항목에 대한 숫자를 사용하십시오.

addr=*Addr*
변환을 요구하는 보안된 IP 주소 범위를 식별하는 IP 주소입니다.

mask=*Mask*
IP 주소 범위를 식별합니다.

NAT 구성에 대응 항목을 추가하려면 **type=map**을 사용하십시오.

```
fwnat cmd=add
      type=map
      secaddr=SecureAddr]
      remaddr=RegisteredAddr]
```

매개변수는 다음과 같이 정의됩니다.

type=map
map 항목을 추가합니다.

secaddr
지정된 등록된 주소로 변환되어야 하는 IP 주소

remaddr
지정된 보안 주소가 변환될 등록된 주소

NAT 구성에서 맵 항목을 변경하려면 다음과 같은 구문을 사용하십시오.

```
fwnat cmd=change
       index=
      [secaddr=SecureAddr]
      [remaddr=RegisteredAddr]
```

매개변수는 다음과 같이 정의됩니다.

색인 fwnat cmd=list를 실행할 때 특정 NAT 항목의 왼쪽 컬럼에 숫자가 있습니다. 색인 매개변수로 특정 NAT 항목에 대한 숫자를 사용하십시오.

secaddr
지정된 등록된 주소로 변환되어야 하는 IP 주소

remaddr
지정된 보안 주소가 변환될 등록된 주소

호출

호출기 알림 지원을 활성화하여 Firewall에서 침입 경보가 있을 때 관리자의 호출기에 메세지를 전송함으로써 시스템 관리자가 Firewall 페이지를 갖도록 할 수 있습니다. 적절히 기능하게 하려면, fwpgr, fwcarrier및 fwmodem 명령을 사용하여 호출기, 반송자 서비스 및 모뎀을 구성해야 합니다.

호출기 구성

fwpgr 명령은 Firewall이 신호를 발신하는 활성 호출기의 매개변수를 설정합니다.

호출기를 나열하려면, 다음 명령을 발행하십시오.

```
fwpgr cmd=list
```

호출기를 추가하려면, 다음 명령을 발행하십시오.

```
fwpgr cmd=add
          carrier=
        modem=
        pagerid=
        message=
```

호출기를 변경하려면, 다음 명령을 발행하십시오.

```
fwpgr cmd=change
        [carrier=]
        [modem=]
        [pagerid=]
        [message=]
```

매개변수는 다음과 같이 정의됩니다.

carrier
반송자 서비스의 이름이며, 반송자 데이터베이스에 정의되어 있습니다(fwcarrier 명령을 통해).

modem
모뎀의 이름이며, 모뎀 데이터베이스에 정의되어 있습니다(fwmodem 명령을 통해).

pagerid
호출 디바이스의 반송자 할당된, 고유한 식별 번호 또는 이름입니다.

message

호출 디바이스로 송신되는 또는 그 위에 표시되는 메세지입니다. 반송자가 제공 중인 서비스에 따라 숫자 또는 텍스트가 됩니다. 반송자에 대한 길이 설정의 작은 부분 또는 200자를 초과할 경우 잘려집니다.

반송자

fwcarrier 명령을 사용하면 사용자가 사용하는 임의 호출 서비스의 매개변수를 설정할 수 있습니다.

반송자를 나열하려면, 다음 명령을 발행하십시오.

```
fwcarrier cmd=list
          carrier=
```

반송자를 추가하려면, 다음 명령을 발행하십시오.

```
fwcarrier cmd=add
          carrier=
          dial=
          method=
          [password=]
          length=
        baud=
        parity=
        databits=
        stopbits=
```

반송자를 변경하려면, 다음 명령을 발행하십시오.

```
fwcarrier cmd=change
          carrier=
          [dial=]
          [method=]
          [password]
          [length=]
          [baud]
        [parity=]
        [databits=]
        [stopbits=]
```

반송자를 삭제하려면, 다음 명령을 발행하십시오.

```
fwcarrier cmd=delete
          carrier=
```

매개변수는 다음과 같이 정의됩니다.

carrier

반송자의 이름.

dial 사용자가 계약한 TAP 서비스용 반송자의 모뎀 전화 번호를 지정해야 합니다.

method

값은 TAP이어야 합니다.

password
반송자 서비스에 필요하지 않을 경우 옵션입니다.

length 반송자 서비스에 허용되는 최대 메세지 길이입니다.

baud 반송자 서비스가 지원하는 가장 신뢰성 있는 보오드율을 지정합니다.

parity 반송자 서비스가 지원하는 패리티 점검 유형입니다. TAB 프로토콜의 경우 이것은 보통 짝수 패리티입니다.

databits
반송자 서비스가 지원하는 데이터 비트수입니다. TAB 프로토콜의 경우 이것은 보통 7입니다.

stopbits
반송자 서비스가 지원하는 정지 비트수입니다. TAB 프로토콜의 경우 이것은 보통 1입니다.

모뎀 구성

호출기 알림 지원을 설정하려면, 모뎀을 구성해야 합니다.

호출기 요청을 호출기 반송자에 송신할 모뎀을 구성하려면, 모뎀 명령을 사용하십시오.

모뎀을 나열하려면, 다음 명령을 발행하십시오.

```
fwmodem cmd=list
        modem=
```

모뎀을 추가하려면, 다음 명령을 발행하십시오.

```
fwmodem cmd=add
        modem=
        comport=
        initsting=
        outsideline=
```

모뎀을 변경하려면, 다음 명령을 발행하십시오.

```
fwmodem cmd=change
        modem=
        [comport=]
        [initstring=]
        [outsideline=]
```

모뎀을 삭제하려면, 다음 명령을 발행하십시오.

```
fwmodem cmd=delete
        modem=
```

매개변수는 다음과 같이 정의됩니다.

modem
모뎀의 이름입니다.

comport

모뎀이 접속되는 직렬 COM 포트입니다. 이 COM 포트의 모뎀은 Windows NT 시스템에 정의되어선 안됩니다.

initstring

모뎀에 대한 초기화 문자열입니다. 스트링 안의 매개변수는 AT 모뎀 명령에 적합해야 하지만, AT는 스트링의 일부로 포함되어선 안됩니다. 지정된 매개변수는 반송자 모뎀의 통신 필요조건으로 조정되어야 합니다.

outsideline

외부 회선으로 연결하기 위한 다이얼 번호입니다.

호출기 구성 검사

활성 호출기를 올바르게 구성했는지 확인하려면, 다음 명령을 사용하십시오.

```
pager
         carrier=
        modem=
    ID=
    msg=
```

매개변수 정의는 fwpgr 명령의 경우와 동일합니다.

복수 호출기

여러분의 활성 호출기를 정기적으로 변경해야 할 경우, 다음을 실행하십시오.

- 필요한 반송자 및 모뎀을 모두 정의했는지 확인하십시오.
- fwpgr 또는 구성 클라이언트를 사용해서 호출기 구성을 정의 및 저장하십시오.
- ROOTDIR\config\pager.cfg 파일을 복사하고, 구별할 수 있는 이름을 제공하십시오.
- 다른 호출기 구성을 정의하고 필요한 pager.cfg 파일의 사본을 모두 얻을 때까지 계속해서 복사하십시오.
- 활성화하려는 구성 파일을 다시 ROOTDIR\config\pager.cfg로 복사하십시오.

시프트 변경을 처리하려 할 경우, 각 시프트 시작에서 마지막 불릿을 자동적으로 반복하도록 명령에서 Windows NT를 사용하여 예정된 작업을 설정하십시오.

사용자

이 명령은 새로운 사용자를 추가하거나 기존의 Firewall 사용자의 하나 이상의 속성을 변경합니다. 특정 환경에서 모든 매개변수가 디폴트 값을 사용하거나 필요하지 않습니다. cmd=add의 경우, 디폴트 값이 저장됩니다; cmd=change의 경우, 기존 값이 보존됩니다.

```
fwuser cmd={add|change}
username=LoginName
[fullname="UsersRealName"]
[password={yes|no}]
[pwdvalue=Password]
[level={proxy|admin}]
       [secftp=SecureFTPauthentication]
       [remftp=NonSecureFTPauthentication]
       [secauth=SecureTelnetAuthentication]
       [remauth=NonSecureTelnetAuthentication]
       [secadmin=SecureAdminAuthentication]
       [remadmin=NonSecureAdminAuthentication]
       [secsocks=SecureSocks]
       [remsocks=NonSecureSocks]
       [sechttp=SecureHTTP]
[key="SecureNet Key Code"]
[histexpire=HistoryExpiration]
[histsize=HistorySize]
[loginretries=LoginRetries]
[maxage=MaxAge]
[maxexpired=MaxExpiredAge]
[maxrepeats=MaxRepeatChars]
[minalpha=MinAlphaChars]
[mindiff=MinDifferentChars]
[minlen=MinLength]
[minother=MinNonAlphaChars]
[pwdwarntime=PasswordWarnTime]
       [userchng={yes|no}]
       [pwlocked={yes|no}]
[fg_all={yes|no}]
[fg_dns={yes|no}]
[fg_interfaces={yes|no}]
[fg_logmonitor={yes|no}]
[fg_logs={yes|no}]
[fg_mail={yes|no}]
[fg_netobjs1={yes|no}]
[fg_netobjs2={yes|no}]
[fg_pagers={yes|no}]
[fg_proxyserver={yes|no}]
[fg_user={yes|no}]
[fg_traffic={yes|no}]
```

기본 매개변수

username

해당 사용자의 로그인 이름.

fullname

해당 사용자에 대해 보유하는 사용자의 전체 이름 또는 몇 가지 그 밖의 간단한(한 행으로된) 정보. 이 값에 공백이 포함되는 경우, 값을 큰 따옴표로 묶어야 합니다.

level 디폴트 값은 프록시이며, 작성 중인 사용자가 단순한 프록시 또는 Socks 사용자임을 나타냅니다. 관리 기능 그룹 및 관리 확인은 프록시 사용자에게는 적용되지 않습니다.

key 사용자의 Digital Pathways SecureNet 키 카드 확인에 사용되는 키. 이 값은 공백을 포함해야 하므로, 큰 따옴표로 묶어야 합니다.

사용자 확인

다음은 사용자 확인 스트링이며 그 해당 사용자 확인 메소드입니다. `fwuser` 명령의 다양한 매개변수에 대한 사용자 확인 스트링 용법은 아래와 같습니다.

- permit–모두 허용
- deny–모두 거부
- password–Firewall 암호
- NT–NT 로그온 암호
- snk–SNK
- sdi–SDI
- user–사용자 제공 확인
- userauth2–사용자 제공 확인
- userauth3–사용자 제공 확인

secftp 보안 인터페이스로부터 FTP 로그인에 사용할 사용자 확인 방법. 유효한 값은 deny, permit, password, NT, snk, sdi, user, userauth2 및 userauth3입니다. 디폴트는 deny입니다.

remftp
비보안 인터페이스로부터 FTP 로그인에 사용할 사용자 확인 방법. 유효한 값은 deny, permit, password, NT, snk, sdi, user, userauth2 및 userauth3입니다. 디폴트는 deny입니다.

secauth
보안 인터페이스로부터 텔넷 로그인에 사용할 사용자 확인 방법. 유효한 값은 deny, permit, password, NT, snk, sdi 및 user입니다. 디폴트는 deny입니다.

remauth
비보안 인터페이스로부터 telnet 로그인에 사용할 사용자 확인 방법. 유효한 값은 deny, permit, password, NT, snk, sdi, user, userauth2 및 userauth3입니다. 디폴트는 deny입니다.

secadmin
보안 인터페이스로부터 Firewall 구성 클라이언트 로그인에 사용할 사용자 확인 방법. 유효한 값은 deny, permit, password, NT, snk, sdi, user, userauth2 및 userauth3입니다. 1차 Firewall 관리자의 프록시 사용자 및 NT의 경우 디폴트는 deny입니다.

remadmin

비보안 인터페이스로부터 Firewall 구성 클라이언트 로그인에 사용할 사용자 확인 방법. 유효한 값은 deny, permit, password, NT, snk, sdi, user, userauth2 및 userauth3입니다. 1차 Firewall 사용자의 프록시 사용자 및 NT의 경우 디폴트는 deny입니다.

secsocks

Firewall의 보안측에서 나온 Socks 클라이언트 연결에 대한 Socks5 사용자 확인 방법입니다. 유효한 값은 deny, permit, password, NT, snk, sdi, user, userauth2 및 userauth3입니다.

Socks5 서버가 CRAM(Challenge Response Authentication) 대신에 사용자 ID/암호 형태 확인 방법에 대해 구성되어 있으면, SNK는 Socks5 사용자 ID/암호 프로토콜이 SNK 챌린지(challenge)를 표시하지 않으므로 작동되지 않습니다.

디폴트는 deny입니다.

remsocks

Firewall의 비보안측에서 나온 Socks 클라이언트 연결에 대한 Socks5 사용자 확인 방법입니다. 유효한 값은 deny, permit, password, NT, snk, sdi, user, userauth2 및 userauth3입니다.

Socks5 서버가 CRAM(Challenge Response Authentication) 대신에 사용자 ID/암호 형태 확인 방법에 대해 구성되어 있으면, SNK는 Socks5 사용자 ID/암호 프로토콜이 SNK 챌린지(challenge)를 표시하지 않으므로 작동되지 않습니다.

디폴트는 deny입니다.

sechttp

보안 인터페이스의 HTTP 요청에 대한 사용자 확인 방법. 유효한 값은 deny, permit, password, NT, sdi, user, userauth2 및 userauth3입니다.

SNK는 SNK 챌린지가 사용자에게 표시되는 방법을 제공하지 않으므로, HTTP 프로토콜에서 지원되지 않습니다. SDI가 지원되지만, 사용자에게는 SDI passcode 대신에 암호를 입력하라는 프롬프트가 표시됩니다. 사용자는 그 SDI passcode를 입력해야 합니다.

주: `fwdfuser`에는 그 사용자 확인 방법 필드에 SNK 또는 Firewall 암호 세트가 없습니다.

Firewall 암호 매개변수

password

사용자에게 암호를 입력하도록 프롬트되는지 여부를 나타냅니다. 기본적으로, 사용자 확인 방법이 지정되었는지 또는 디폴트 암호를 허용할 것인지 여부를 프롬트합니다.

pwdvalue

대부분 스크립트 프로그래밍에 사용되며, 이 매개변수를 사용하여 명

령 행에서 매개변수 값을 지정할 수 있습니다. 이 값은 순수하게 텍스트로 입력되며 eavesdroppers로부터 항상 명백합니다. 디폴트는 없습니다.

userchng

사용자 데이터베이스에서 관리자 변경 플래그가 설정되는 방식을 결정합니다. 값 yes를 사용하면 사용자가 처음 로그온할 때 암호를 변경할 것을 요구하도록 관리자 변경 플래그가 설정됩니다. No가 디폴트입니다. 이 매개변수는 password=yes 및 pwdvalue=″ 매개변수가 제공될 경우에만 유효합니다.

pwlocked

암호가 잠겨지는지 여부를 지정합니다. 이 매개변수는 최대 실패 로그인 회수가 초과되거나 암호가 잠금 이전 최대 시간에 지정된 주수에 사용되지 않은 경우에 yes로 설정됩니다.

histexpire

사용자가 암호를 재사용할 수 없는 시간 주수를 정의합니다. 값은 정수 스트링입니다. 유효한 값은 0 - 52입니다. 값 0은 시간 제한이 설정되어 있지 않음을 나타냅니다. 디폴트 값은 0입니다.

histsize

사용자가 재사용할 수 없는 이전 암호의 수를 정의합니다. 값은 정수 스트링입니다. 유효한 값은 0 - 20입니다. histexpire=0의 경우에만 유효합니다. 디폴트 값은 5입니다.

loginretries

시스템이 계정을 잠그기 전에 마지막으로 성공한 계정 이후 허용되는 성공하지 않은 로그인 시도 수를 정의합니다. 값은 정수 스트링입니다. 유효한 값은 0 - 20입니다. 디폴트 값은 10입니다. 0 또는 음수 값은 제한이 존재하지 않음을 나타냅니다. 일단 사용자 계정이 잠기면, 시스템 관리자가 pwlocked를 no로 설정할 때까지, 사용자는 로그인할 수 없습니다.

maxage

암호의 최대 수명(주 단위)을 정의합니다. 암호를 이 시간에 따라 변경해야 합니다. 값은 정수 스트링입니다. 유효한 값은 0 - 52입니다. 값 0은 최대 수명이 설정되어 있지 않음을 나타냅니다. 디폴트는 13입니다.

maxexpired

사용자가 만료된 암호를 변경할 수 있는 maxage 값 이후 최대 시간(주 단위)을 정의합니다. 이 정의된 시간이 끝나면, 관리 사용자만이 암호를 변경할 수 있습니다. 값은 정수 스트링입니다. 유효한 값은 -1 - 26입니다. maxexpired 속성이 0인 경우, maxage 값이 일치될 때 암호가 만료됩니다. maxage 속성이 0인 경우, maxexpired 속성이 무시됩니다. 디폴트는 3입니다.

maxrepeats

새 암호에서 반복할 수 있는 한 문자의 최대 회수를 정의합니다. 유

효한 값은 0 - 8이지만, 값 0은 의미가 없습니다. 값 8은 최대 회수가 없음을 나타냅니다. 디폴트는 2입니다.

minalpha
새 암호에 존재해야 하는 영문자의 최소 회수를 정의합니다. 값은 정수 스트링입니다. 유효한 값은 0 - 8이지만, 값 0은 의미가 없습니다. 디폴트는 4입니다.

mindiff
기존 암호에는 없는 새 암호에서 필요한 문자의 최소 회수를 정의합니다. 값은 정수 스트링입니다. 유효한 값은 0 - 8이지만, 값 0은 의미가 없습니다. 디폴트는 3입니다.

minlen
암호의 최소 길이를 정의합니다. 값은 정수 스트링입니다. 유효한 값은 0 - 8이지만, 값 0은 의미가 없습니다. 디폴트는 8입니다.

minother
새 암호에 존재해야 하는 영문이 아닌 문자의 최소 회수를 정의합니다. 값은 정수 스트링입니다. 유효한 값은 0 - 8이지만, 값 0은 의미가 없습니다. 디폴트는 1입니다.

pwdwarntime
암호를 변경해야 하는 것을 시스템이 경고하기 전 일 수를 정의합니다. 값은 정수 스트링입니다. 유효한 값은 0 - 30입니다. 0 또는 음수 값은 메세지가 실행되지 않음을 나타냅니다. 디폴트 값은 5입니다.

관리 기능 그룹

fg_all 해당 관리자가 모든 Firewall 요소를 관리할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_dns
해당 관리자가 도메인 이름 서비스를 관리할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_interfaces
해당 관리자가 Firewall 인터페이스를 정의할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_logmonitor
해당 관리자가 로그 모니터 임계값을 관리할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_logs
해당 관리자가 로그 기능을 관리할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_mail
해당 관리자가 Firewall 게이트웨이를 관리할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_netobjs1
해당 관리자가 네트워크에 대한 기본 관리를 수행할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_netobjs2
해당 관리자가 네트워크 오브젝트에 대한 고급 관리를 수행할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_pagers
해당 관리자는 호출기 설정을 관리할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_proxyserver
해당 관리자가 Firewall 프록시 디먼을 구성할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_traffic
해당 관리자가 통신량 조절을 관리할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

fg_user
해당 관리자가 Firewall 사용자를 관리할 수 있는 경우 yes를 입력하십시오. 디폴트는 no입니다.

모든 Firewall 사용자나 한 명의 지정된 Firewall 사용자의 모든 속성을 나열하려면, 다음을 사용하십시오.

```
fwuser cmd=list
       [username=username]
       [type={short|long}]
```

type={short|long}
사용자 이름을 사용하는 경우 디폴트 유형은 long입니다. 사용자 이름을 사용하지 않는 경우, 디폴트는 short입니다.

Firewall에서 사용자를 삭제하려면:

```
fwuser cmd=delete
       username=username
```

제2장 보고서 유틸리티 사용

이 장에서는 IBM Firewall의 보고서 유틸리티 사용에 관하여 설명합니다. 보고서 유틸리티의 1차적인 목적은 Firewall 로그 파일에서 관리 정보의 표로 작성된 파일을 생성하기 위한 것입니다.

표로 작성된 텍스트 파일은 DB2/6000 또는 DB2/2와 같은 데이터베이스 시스템에서 표로 생성되고 반입될 수 있습니다. 그러면 관리자는 SQL(Structured Query Language)을 사용하여 데이터를 조회하고 보고서를 생성할 수 있습니다. 또한, 유틸리티를 사용하여 관리자는 Firewall 로그 메세지의 읽을 수 있는 텍스트 파일을 작성할 수도 있습니다.

보고서 유틸리티는 다음 프로그램과 파일로 구성됩니다.

fwlogtxt
: Firewall 로그 파일에서 완전 텍스트 메세지를 생성하기 위한 프로그램

fwlogtbl
: Firewall 로그 및 su 로그로부터 DEL(분리) 형식으로 데이터베이스 반입 파일을 생성하는 프로그램.

  fwlogtbl 프로그램과 DDL, DML 및 DEL 파일을 사용하려면, 관계형 데이터베이스 및 해당 관계형 데이터베이스 제품 사용에 대한 얼마간의 지식이 있어야 합니다.

fwschema.ddl
: 데이터베이스 테이블을 정의하는데 적합한, SQL 데이터 정의 언어(DDL) 명령문으로된 파일

fwimport.dat
: 데이터베이스 테이블로 DEL 파일을 반입하는데 적합한, DB2 반입 명령문으로된 파일

fwqrysmp.dml
: 예제 보고서를 생성하는데 적합한 SQL 데이터 처리 언어(DML) 명령문으로된 파일

fwlogcvrt
: Windows NT Firewall 로그 형식을 AIX Firewall 로그 형식으로 변환하는 프로그램입니다. 이를 사용하여 다른 벤더의 보고 툴은 새로운 메세지가 인식되지 않을 수 있다는 점을 제외하고는 전과 같이 조작됩니다.

DDL 및 DML 파일은 DB2 계열에 특정적이지만, 다른 데이터베이스 관리 시스템에서 사용하기 위해 수정할 수 있습니다. DEL 형식 파일은 쉽게 DB2/6000, DB2/2 및 그밖의 데이터베이스 및 파일 시스템으로 반입(로드)될 수 있습니다. 간단한 형식으로 필요에 따라 다른 형식으로 변환할 수 있어야 합니다.

보고서 유틸리티 사용법

이 정보에는 명령행에서 보고서 유틸리티를 사용하는 방법에 대한 설명이 담겨 있습니다. 구성 클라이언트로부터 보고서 유틸리티를 사용하는 방법에 대해서는 *IBM eNetwork Firewall 사용자 안내서*를 참고하십시오.

명령 행에서 Firewall 로그 파일을 보려면, **fwlogtxt** 유틸리티를 사용하십시오. 자세한 정보는 27페이지의 『Firewall 로그 파일로부터 메세지 생성』을 참조하십시오.

로그 정보에 따라 보고서를 생성하려면:

1. 관계형 데이터베이스 제품을 설치하십시오.
2. 비어있는 데이터베이스를 작성하십시오.
3. 데이터베이스에 비어있은 Firewall 로그표를 작성하십시오.
4. 표로 작성된 파일을 생성하려면 명령행에서 **fwlogtbl**을 실행하십시오.
5. 로그 데이터를 사용하여 데이터베이스 테이블을 채우려면 결과 파일을 반입하십시오.
6. SQL문 또는 SQL 프로그램을 사용하여 보고서를 생성하십시오.

주: 처음 세 가지 단계는 한번만 수행해야 하며, 나머지 단계는 새로운 로그 데이터가 사용가능할 때마다 반복됩니다.

IBM Firewall 로그 형식

각 방화벽 로그 파일 항목의 형식은 다음과 같습니다.

```
Date Time Firewall_name:year;pid:Amsg_num; msg_ID;var_1;...;var_n;
```

여기서,

- 처음 3개의 필드 **date, time 및 Firewall-name**은 Firewall 로깅 기능에 의해 추가됩니다.
- **year**는 4자로된 연도입니다.
- **pid**는 항목이 적용되는 쓰레드 ID입니다.
- **Amsg_num**는 보고서 유틸리티에서 fw_log.cat 파일로부터 적합한, 변환된 메세지 텍스트에 액세스하는 데 사용하는 순차적인 정수입니다. 숫자 msg_num는 로그 레벨 표시자 문자 (A) 바로 다음에 나옵니다. 이 표시자는 로그가 시작된 플랫폼과 로그 형식 안의 차이점을 구별해 줍니다.
- **msg_ID**는 메세지의 외부 숫자(ICA0001e와 같은)입니다.
- **var_1-n**는 메세지 변수값을 나타내며, 여기서 **n**은 메세지 정의에 있는 변수의 수입니다.

주: Firewall 로그와 동일한 파일에 다른 레코드를 지정하지 마십시오. 그러한 레코드는 보고서 유틸리티에서 요구하는 형식을 따르지 않으며 결과를 예상할 수 없습니다.

fwlogcvrt 명령을 사용해서 이 Windows NT 릴리스의 로그 형식을 AIX 로그의 형식으로 변환하십시오. AIX용 IBM Firewall 로그를 지원하는 기타 벤터 보고 툴을 사용하려면 이를 실행해야 할 수 있습니다. 변환은 msg_num 앞에 나오는 'A' 로그 레벨 표시자를 삭제하고 Firewall_name과 year 사이의 콜론 주변에 두 공백 문자를 삽입합니다.

매개변수는 다음과 같습니다.

input Windows NT Firewall 로그로부터 경로를 재지정한 표준 입력입니다.

output
파일로 경로를 재지정할 수 있는 표준 출력입니다.

fwlogcvrt 구문

```
fwlogcvrt
```

예:

```
fwlogcvrt < fw980212.log >logcvrt.out
```

Firewall 로그 파일로부터 메세지 생성

명령 **fwlogtxt**를 사용하여 Firewall 로그 파일의 항목으로부터 읽기 가능한 메세지를 생성할 수 있습니다.

매개변수에는 다음이 포함됩니다.

input Firewall 로그 파일로부터의 표준 입력입니다.

output
표준 출력입니다.

fwlogtxt 구문

```
fwlogtxt
```

예:

```
fwlogtxt < fw980212.log >logtxt.out
fwlogtxt < my.log | find "ICA0"
```

fwlogtxt에는 매개변수가 없으며; 표준 입력으로부터 정보를 취하여 표준 출력으로 결과를 내보냅니다.

데이터베이스 반입 파일 생성

명령 **fwlogtbl**을 사용하여 사용자가 보고서를 생성하기 위하여 데이터베이스 테이블을 채울 수 있는 표로 작성된 파일을 작성하거나, 기록하거나, 추가할 수 있습니다.

매개변수에는 다음이 포함됩니다.

input Firewall 로그 파일.

output

파일명:

a_alert.tbl
f_rule.tbl
f_info.tbl
f_match.tbl
f_stat.tbl
interfaces.tbl
nat_info.tbl
p_info.tbl
p_ftp.tbl
p_http.tbl
p_info.tbl
p_login.tbl
p_stat.tbl
server_info.tbl
session.tbl
s_ftp.tbl
s_info.tbl
ssl_info.tbl

fwlogtbl 구문

```
fwlogtbl  -w [-d OutDir]  [-su]LogName
                |
               -a

예:

             fwlogtbl -a  -d :c\reports fw961031.log
```

-w 기존 출력 파일을 대체하도록 지정합니다. 파일이 존재하지 않는 경우, fwlogtbl이 작성합니다.

-a 생성된 파일을 기존 출력 파일에 추가하도록 지정합니다. 파일이 존재하지 않는 경우, fwlogtbl이 작성합니다.

-d 출력 디렉토리를 식별합니다.

OutDir

모든 출력 파일을 저장할 디렉토리를 지정합니다. 디렉토리를 지정하지 않은 경우, 출력 파일이 현재 디렉토리에 저장됩니다.

-su LogName이 AIX su 로그 파일의 이름임을 지정합니다. 따라서 Windows NT Firewall에서 더 이전의 AIX Firewall으로부터 Firewall과 su 로그 파일을 모두 처리할 수 있습니다.

LogName
Firewall 로그 파일 또는 AIX su 로그 파일을 지정합니다.

출력 파일명이 사전정의되어 있지만 fwlogtbl 실행후 복사하거나 재명명할 수 없습니다. 출력 파일은 문자열 구분자 없이, ASCII(DEL) 파일 형식을 구분하며, 콜론 구분자로 세미콜론(;)을 사용합니다.

메세지에 관한 자세한 정보는, 77페이지의 『부록A. 메세지』를 참조하십시오.

보고서 유틸리티를 사용한 데이터베이스 사용

이 절에서는 데이터베이스를 작성하고, 정보를 데이터베이스로 반입하며, 보고서를 조회하기 위하여 Firewall에서 제공하는 파일을 설명합니다. DB2가 있는 경우, db2 명령을 이들 파일에 사용할 수 있습니다. (db2 명령과 유사한 기능이 다른 데이터베이스 관리 프로그램에 존재할 수 있습니다. 파일이 그러한 기능에 사용할 대체방안을 요구할 수도 있습니다.)

db2 명령을 실행하려면, DB2가 설치되고 'instance'가 정의되어야 합니다. DB2 설치 설명서를 참고하십시오. 초기적으로, DB2의 데이터베이스 작성 명령을 사용하여 비어있는 데이터베이스를 작성해야 합니다. ('fwlog'로 칭하도록 제안합니다.) 이를 수행하려면, 명령 행에 다음과 같이 입력하십시오.

```
db2cmd
```

그런 다음 나타나는 DB2 명령 창에 다음을 입력하십시오.

```
db2 create database fwlog
```

다음에는 fwlog 데이터베이스로 연결해야 합니다.

```
db2 connect to fwlog
```

그런 다음 db2 명령의 -vf 옵션을 다음과 같이 사용할 수 있습니다.

```
             db2 -vf fwschema.ddl > schema.out
db2 -vf fwimport.dat > import.out
             db2 -vf fwqrysmp.dml > report.out
```

이들 단계에 대해서는 다음 절에서 좀더 상세히 설명합니다. 각각의 경우, 사용자는 표준 출력(각각의 예제에서 파일로 경로 재지정된)을 주의하여 확인해야 합니다. 반입의 경우, 또한 각각의 개별적인 반입 명령문에서 생성한 .msg 파일을 확인해야 합니다.

테이블 작성

명령 **db2 -vf fwschema.ddl > schema.out**은 필요한 모든 테이블과 인덱스를 작성합니다. 이 명령은 Firewall 설치 후 즉시, 한번만 실행하십시오. 이

예제를 실행할 때 현재 사용자 ID가 테이블의 작성자 ID가 됩니다. 이 ID는 작성자 ID로 실행되지 않는 경우, 나중에 SQL문에서 테이블명 규정자(reatorid.tableName과 같은)로 사용되어야 할 수도 있습니다. 따라서, 작성자 ID를 사용 중이 아닌 경우, 사용자는 각각의 테이블명 앞에 작성자 ID를 위치시키려면 fwimport.dat 및 fwqrysmp.dml 파일을 편집해야 합니다.

ROOTDIR\sample\report\fwschema.ddl 파일에는 **fwlogtbl**에 의해 표로 작성된 파일로부터 레코드를 수용하는 데 필요한 데이터베이스 테이블을 작성할 DDL문이 들어 있습니다. *ROOTDIR*은 설치 프로세스 동안에 IBM Firewall의 목표 위치로 여러분이 선택한 디렉토리입니다. 조작이 성공했는지 결정하려면 schema.out을 조사해야 합니다. fwschema.ddl 파일에 나오는 명령문들은 있는 그대로 사용되거나 다양한 데이터베이스 시스템에 맞도록 수정될 수 있습니다. (사용자는 테이블과 컬럼명을 변경하지 않아야 합니다.)

데이터 반입

db2 –vf fwimport.dat > import.out 명령은 모든 DEL 파일에서 데이터를 **db2-vf fwschema.ddl** 명령에 의해 작성된 테이블로 로드됩니다.

ROOTDIR\sample\report\fwimport.dat 파일에는 *.tbl 파일에서 DB2 데이터베이스로 데이터를 반입하는 샘플 명령문이 들어 있습니다. 29페이지의 『테이블 작성』에 언급된 대로, 반입 사용자가 테이블 작성자가 아닌 경우, 작성자 ID가 각각의 테이블명 앞에 위치해야 합니다.

각 반입 명령문은 표준 출력으로, tblname.msg 파일에 추가 정보를 생성하며, 여기서 tblname은 각 반입 명령문에 특정합니다. 반입이 성공했는지 결정하려면 사용자는 출력 양식을 둘 다 확인해야 합니다. 이 파일에 있는 모든 반입 명령문을 DB2와 같은 프로그램으로 실행 중인 경우, 사용자는 표준 출력을 파일로 지정한 다음, 해당파일과 각 .msg 파일을 확인해야 합니다. 각각의 반입 명령 중 하나가 개별적인 .msg 파일을 생성합니다. 또한, 사용자는 데이타베이스에서 새로운 로그가 반영될 때마다 **db2 –vf fwimport.dat > import.out** 명령을 재발행해야 합니다.

대용량 로그 파일을 반입하는 경우, 추가 메모리나 디스크 공간에 대한 필요성을 나타내는 설명과 함께 SQL 오류 코드를 수신할 수도 있습니다. 예를 들어, 메세지는 힙(heap) 공간이 충분하지 않습니다 또는 트랙잭션 로그 공간입니다일 수 있습니다. 이들 오류는 데이터베이스 제품 또는 fwlog 데이터베이스에 대한 매개변수 설정을 조정하도록 요구합니다. 자세한 정보는 DB2 문서를 참조하십시오. DB2 매개변수 설정을 조정하기 위한 임시 대체 방안은 대용량 로그나 대용량 표로 작성된 파일을 보다 작은 파일로 쪼개는 것입니다.

샘플 조회 실행하기

db2 -vf fwqrysmp.dml > report.out 명령은 샘플 조회를 수행합니다. ROOTDIR:\sample\report\fwqrysmp.dml 파일에는 일부 조회 요구사항에 따라 유용한 보고서 데이터를 제공할 수 있는 샘플 SQL문이 들어 있습니다. 자

체 보고서를 작성하기 위하여 이들 예제를 사용할 수 있습니다. 29페이지의 『테이블 작성』에 언급된 대로, 반입 사용자가 테이블 작성자가 아닌 경우, 작성자 ID가 각각의 테이블명 앞에 위치해야 합니다.

명령 행에서 조회를 실행하면, DB2는 각각의 출력 열에 필요한 최대 공간을 할당합니다. 이것은 읽기 어려운 보고서를 생성할 수 있습니다. 각 조회에 보다 적은 열을 요청하거나 표시를 보다 잘 제어할 수 있는 프로그램에 이들 조회 명령문을 포함시켜서 보다 만족스런 결과를 달성할 수도 있습니다.

보고서 유틸리티에 대한 사용자 인터페이스

보고서 유틸리티는 Firewall 설치의 일부로 설치되어 있습니다. 이들은 또한 개별적으로 설치되고 비-Firewall 호스트에서 실행될 수 있습니다. 구성 클라이언트나 `fwlogtbl` 명령은 Firewall에서 보고서 유틸리티를 실행하는 데 사용될 수 있습니다. 비Firewall에서는 명령행을 사용하십시오.

SQL 테이블

이 절에서는 SQL 표의 개요에 대해 설명합니다.

각 Firewall 로그 메세지 또는 AIX su 로그 메세지는 다음 SQL 표 중 하나로 대응됩니다.

```
ADMIN_ALERT
FILTER_INFO
FILTER_MATCH
FILTER_ACTIVE_RULE
FILTER_STATUS
INTERFACES
NAT_INFO
PAGER_INFO
PROXY_FTP
PROXY_HTTP
PROXY_INFO
PROXY_LOGIN
PROXY_STATUS
SERVER_INFO
세션
SOCKS_FTP
SOCKS_INFO
SSL_INFO
SU
TUNNEL_CONTEXT
TUNNEL_POLICY
TUNNEL_STATUS
```

테이블과 컬럼 이름을 변경해서는 안됩니다. 그러나 그 값 중 일부가 절단되고 있다는 것을 발견한 경우, char 컬럼의 폭을 늘릴 수 있습니다.

인덱스

특정 Firewall 이벤트가 데이터베이스에서 한번만 나타나야 함을 나타내는 로그 레코드. 관리자가 같은 표로 작성된 테이블을 여러 번 반입하거나 같은 로그 파일에서 유도된 또다른 표로 작성된 파일이 반입된 경우, 로그 레코드가 두번 이상 나타날 수 있습니다.

이러한 문제를 방지하기 위하여, 데이터베이스 정의 샘플 파일, fwschema.dll은 다음과 같은 세 가지 필드를 사용하여 각각의 테이블에 고유한 인덱스를 정의합니다.

- 해당 레코드의 소스인 로그 파일의 파일명(LOG_FILE)
- 그 로그 파일에서 해당 레코드의 행 번호(LINE_NUM)
- syslog '마지막 메세지가 n번 반복되었음' 메세지에 따라, 해당 행의 반복 회수(REPEAT_NUM)

이 인덱스는 같은 명명된 파일에서 두번 이상 같은 행 번호를 로드하지 않도록 합니다. 이것은 로그 파일명에 대한 주의깊은 관리와 결합하여, 데이터베이스의 로그 이벤트 중복을 방지해야 합니다.

다른 인덱스를 데이터베이스에 추가하여 가장 공통적인 조회의 성능을 향상시킬 수도 있습니다. 자세한 정보는 데이터베이스 문서를 참조하십시오.

테이블 설명

이 절에서는 Firewall 로그 메세지를 테이블과 열에 대응하고 보고서에 대하여 조회하려는 정보를 나타냅니다. 특정 테이블에 대응된 모든 메세지가 테이블 끝에 있는 주석에 나열됩니다. 특정 열에 대한 데이터를 제공하는 메세지가 해당 열 설명에 나열됩니다. 이 테이블에는 AIX용 IBM Firewall의 메세지와 NT용 IBM Firewall의 메세지 및 두 Firewall에 공통적인 메세지가 있습니다.

Firewall 로그 메세지에 관한 자세한 정보는, 77페이지의 『부록A. 메세지』를 참조하십시오.

다음 설명의 데이터 유형 열에서, 'int'는 DB2의 SMALLINT 열 유형을 나타내며; 'long int'는 DB2 INTEGER 유형을 나타냅니다. 날짜-시간 데이터 유형은 DB2 TIMESTAMP를 나타냅니다. 시간소인에서, 마이크로초 값은 항상 ″000000″입니다.

설명이 *필수*로 표시된 경우, 테이블에 레코드를 입력하도록 값을 지정해야 하는 것을 의미합니다.

정의가 동일하며 일반적으로 조회할 이유가 없으므로 고유한 인덱스 및 열로 작용하는 세 개의 열을 이들 테이블 설명에서 생략합니다.

표 1. ADMIN_ALERT. 이 테이블은 a_alert.tbl 테이블의 위반 경고와 관련된 메세지를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
사용자 ID	char(16)	사용자 ID (ICA0001, ICA0002, ICA0003, ICA0004, ICA2001, ICA2002, ICA2003, ICA2026, ICA2043, ICA2068, ICA2167, ICA2168, ICA 2170, ICA2173, ICA3001, ICA3012, ICA3018)
조치	char(7)	연결 (ICA3012) 또는 바인드 (ICA3018)
NUM_COUNT	int	사용자 확인 실패 회수(ICA0001, ICA0002, ICA0003); TAG_MSG_NUM에 대한 로그 입력 회수(ICA0004); 일 수 (ICA9000)
TAG_MSG_NUM	char(8)	태그 메세지 번호(ICA0004)
SRC_IP	char(15)	출발지 IP 주소(ICA2001, ICA2028, ICA2079, ICA2167, ICA3012, ICA3018)
DST_IP	char(15)	목적지 IP 주소(ICA2028, ICA2079, ICA3012, ICA3018)
AUTH_METHOD	char(20)	사용자 확인 방법(ICA2002, ICA2167, ICA2170)
네트워크	char(25)	네트워크 이름(ICA2001, ICA2002, ICA2167)
HOST_NAME	char(100)	호스트명(ICA0003, ICA2002)
TIMEOUT_SEC	int	시간종료 초(ICA2026)
CONN_USERID	char(16)	Socks 연결 사용자명(ICA3001)
응용 프로그램	char(30)	응용 프로그램명 - ″텔넷″, ″ftp″, ... (ICA2167, ICA2168, ICA2170, ICA3012)
주: 관련 메세지: ICA0001 ICA0002 ICA0003 ICA0004 ICA0005 ICA0006 ICA0007 ICA0008 ICA0009 ICA0010 ICA0011 ICA0012 ICA0013 ICA0014 ICA0015 ICA0016 ICA0017 ICA0018 ICA0019 ICA0020 ICA0021 ICA0022 ICA1010 ICA2001 ICA2002 ICA2003 ICA2020 ICA2026 ICA2028 ICA2037 ICA2040 ICA2042 ICA2043 ICA2079 ICA2167 ICA2168 ICA2170 ICA2173 ICA3001 ICA3012 ICA3018 ICA9000 ICA9001		

표 2. FILTER_ACTIVE_RULE. 이 테이블은 f_rule.tbl 파일의 활동 중인 필터 규칙을 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
RULE_NUM	int	규칙 번호(필수)

표 2. FILTER_ACTIVE_RULE (계속). 이 테이블은 f_rule.tbl 파일의 활동 중인 필터 규칙을 포함합니다.

열	데이터 유형	짧은 설명
규칙	char(100)	규칙(필수)
주: 관련 메세지: ICA1037		

표 3. FILTER_INFO. 이 테이블은 f_info.tbl 파일의 필터와 관련된 오류 또는 일반적인 정보 메세지를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
RULE_NUM	int	필터 규칙 번호(ICA1005)
ERROR_NUM	int	시스템 오류 번호 -- AIX errno 또는 Windows NT 마지막 오류(ICA1007, ICA1008, ICA1009, ICA1011 ICA1013, ICA1015, ICA1021, ICA1023, ICA1024) 이 오류 번호에 해당하는 텍스트는 _strerror 함수를 사용하여 나타낼 수 있습니다. Windows NT 최종 오류에 대한 텍스트는 형식 메세지 함수를 통해서나 Win32 프로그래머 참조서 볼륨 2의 부록 A에서 사용할 수 있습니다.
LOAD_PATH	char(100)	커널 확장 로그 경로(ICA1011, ICA1012)
DVC_DRV	char(25)	장치 드라이버(ICA1021)
TERM_SIG	char(25)	종료 신호(ICA1260)
FILE_NAME	char(100)	파일명(ICA1024)
RC	int	내부 Firewall 리턴 코드(ICA1019)
주: 관련 메세지: ICA1001 ICA1002 ICA1003 ICA1005 ICA1007 ICA1008 ICA1009 ICA1011 ICA1012 ICA1013 ICA1014 ICA1015 ICA1016 ICA1017 ICA1019 ICA1021 ICA1022 ICA1023 ICA1024 ICA1200 ICA1260		

표 4. FILTER_MATCH. 이 테이블은 f_match.tbl 파일에 대응하는 필터 규칙을 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
RULE_NUM	int	규칙 번호(필수)
조치	char(6)	규칙 유형: 허용, 거부 등.
방향	char(8)	패킷이 전송되는 방향 인바운드 또는 아웃바운드(필수)
SRC_IP	char(15)	전송자의 IP 주소(필수)

표 4. FILTER_MATCH (계속). 이 테이블은 f_match.tbl 파일에 대응하는 필터 규칙을 포함합니다.

열	데이터 유형	짧은 설명
DST_IP	char(15)	수신자의 IP 주소(필수)
프로토콜	char(7)	상위 프로토콜 - UDP, IPIP, ICMP, TCP 또는 TCP/ACK(필수)
SRC_PORT	int	• ICMP의 IP 패킷 유형 • 그밖의 자원 프로토콜 포트 번호(필수)
DST_PORT	int	• ICMP의 IP 패킷 코드 • 그밖의 목적지 프로토콜 포트 번호(필수)
경로지정	char(5)	패킷 병합 경로지정: 라우트 또는 로컬(필수)
인터페이스	char(10)	인터페이스 유형: 보안 또는 비보안(필수)
분할부분	char(8)	패킷이 분할부분인지 또는 비분할부분인지 식별합니다. (필수)
TUNNEL_ID	int	터널 ID(필수)
암호화	char(7)	암호화 알고리즘: DES_CBC 또는 CDMF 또는 없음
바이트	long int	특정 패킷 길이(필수)
주: 관련 메세지: ICA1036		

표 5. FILTER_STATUS. 이 테이블은 f_stat.tbl 파일의 필터 상태 변경사항에 관한 정보를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
디먼	char(25)	AIX 필터 로깅 디먼(ICA1004) 또는 Windows NT 필터 로깅 서비스입니다.
버전	int	버전 번호(ICA1004, ICA1033)
릴리스	int	릴리스 번호(ICA1004, ICA1033)
PACKET_LOGGING	char(8)	패킷 로깅 사용가능 또는 사용불가 상태(ICA1035)
주: 관련 메세지: ICA1004 ICA1032 ICA1033 ICA1034 ICA1035. 필터 규칙 갱신 세부사항(ICA1032)은 FILTER_ACTIVE_RULE 테이블에서 얻을 수 있습니다.		

표 6. INTERFACES. 이 표에는 interface.tbl 파일에서 가져온 인터페이스(어댑터) 구성 메세지 정보가 들어 있습니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)

표 6. INTERFACES (계속). 이 표에는 interface.tbl 파일에서 가져온 인터페이스(어댑터) 구성 메세지 정보가 들어 있습니다.

열	데이터 유형	짧은 설명
MSG_NUM	int	메세지 번호(필수)
IP	char(15)	어댑터에 대한 IP 주소(ICA9038, ICA9039, ICA9040)
OLD_MASK	char(15)	이전 마스크 값(ICA9040)
NEW_MASK	char(15)	새로운 마스크 값(ICA9040)
주: 관련 메세지: ICA9037, ICA9038, ICA9039, ICA9040, ICA9041		

표 7. NAT_INFO. 이 테이블은 nat_info.tbl 파일의 네트워크 주소 변환 메세지 정보를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
버전	int	NAT 버전 번호(ICA9033)
릴리스	int	NAT 릴리스 번호(ICA9033)
IP	char(15)	IP 주소(ICA9035, ICA9036)
주: 관련 메세지: ICA9032, ICA9033, ICA9034, ICA9035, ICA9036		

표 8. PAGER_INFO. 이 테이블은 pgr_info.tbl 파일로부터 Firewall의 호출 기능과 관련된 정보를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
사용자 ID	char(16)	사용자 ID(ICA4036, ICA4174, ICA4175)
ERROR_NUM	int	시스템 오류 번호 - AIX errno 또는 Windows NT 마지막 오류(ICA4371)
프로그램	char(25)	프로그램명(ICA4000)
신호	int	종료 신호(ICA4000)
ID	int	식별자(ICA4036)
우선순위	int	우선순위(ICA4036)
기간	int	기간(ICA4036)
RETRY_COUNT	int	재시도 회수(ICA4036, ICA4313, ICA4314, ICA4364, ICA4365)
FROM_ENTRY	char(15)	함수명(ICA4036)

표 8. PAGER_INFO (계속). 이 테이블은 pgr_info.tbl 파일로부터 Firewall의 호출 기능과 관련된 정보를 포함합니다.

열	데이터 유형	짧은 설명
HOST_NAME	char(100)	호스트명(ICA4174, ICA4175)
MESSAGE_TEXT	char(250)	페이지 텍스트(ICA4036, ICA4353 - 4360, ICA4368, ICA4372)
서비스	char(25)	서비스명(ICA4017)
Socket	int	Socket 번호(ICA4017)
파일명	char(100)	파일명(ICA4154, ICA4351, ICA4352)
주: 관련 메세지: ICA4000 ICA4001 ICA4007 ICA4017 ICA4036 ICA4154 ICA4168 ICA4174 ICA4175, ICA4300 - 4303, ICA4305 - 4315, ICA4351 - 4360, ICA4362 - 4372)		

표 9. PROXY_FTP. 이 테이블은 p_ftp.tbl 파일의 FTP 세션으로부터의 FTP 조치 정보를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
사용자 ID	char(16)	사용자 ID(필수)
SRC_IP	char(15)	사용자의 IP 주소(필수)
DST_IP	char(15)	원격 시스템의 IP 주소(필수)
조치	char(5)	파일 전송 조치: put 또는 get(필수)
FILE_NAME	char(100)	파일명
바이트	long int	전송된 데이터 양
SID	long int	고유한 세션 ID(필수)
주: 관련 메세지: ICA2075		

표 10. PROXY_HTTP. 이 테이블은 p_http.tbl 파일로부터 프록시 세션의 HTTP 조치 정보를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
상태	int	상태(필수)
SRC_IP	char(15)	사용자의 IP 주소(필수)
요청	char(250)	HTTP 요청의 내용(필수)
바이트	long int	전송된 데이터의 양.
주: 관련 메세지: ICA2099		

표 11. PROXY_INFO. 이 테이블은 p_info.tbl 파일의 프록시 관련 오류 또는 일반적인 메세지를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
사용자 ID	char(16)	사용자 ID(ICA2018, ICA2019, ICA2057, ICA2058, ICA2166, ICA2177, ICA2172)
ERROR_NUM	int	시스템 오류 번호 - AIX errno 또는 Windows NT 마지막 오류(ICA2005, ICA2006, ICA2009, ICA2029, ICA2035, ICA2038, ICA2039, ICA2052, ICA2054, ICA2055, ICA2056, ICA2057, ICA2058, ICA2059, ICA2063, ICA2064, ICA2065, ICA2066, ICA2067, ICA2068, ICA2069, ICA2069, ICA2070, ICA2071, ICA2074, ICA2110, ICA2111, ICA2113, ICA2114, ICA2115, ICA2118, ICA2119, ICA2121, ICA2122, ICA2123, ICA2124, ICA2200, ICA2201, ICA2202, ICA2203) errno의 텍스트(AIX 시스템 오류)는 _strerror 함수에서 얻을 수 있습니다. Windows NT 최종 오류에 대한 텍스트는 형식 메세지 함수를 통해서나 Win32 프로그래머 참조서 볼륨 2의 부록 A에서 사용할 수 있습니다.
OPTION_VAL	char(20)	옵션 플래그 또는 매개변수 값(ICA2014, ICA2015, ICA2049, ICA2050)
시간	char(15)	유효하지 않은 시간 간격(ICA2044, ICA2202)
RC	int	내부 Firewall 리턴 코드(ICA2007, ICA2030, ICA2031, ICA2033, ICA2034, ICA2054, ICA2057, ICA2058, ICA2065, ICA2120 ICA2166, ICA2203)
INVOC_NAME	char(20)	시스템 오류가 발생한 시간의 socket 또는 포트에 대한 호출명(ICA2055, ICA2056)
AUDIT_TYPE	char(7)	알 수 없는 감사 유형(7자리 16진수)(ICA2004)
HOST_NAME	char(100)	호스트명(ICA2106, ICA2107, ICA2126)
FILE_NAME	char(100)	파일명(ICA2029, ICA2030, ICA2072, ICA2183, ICA2204, ICA2205, ICA2206, ICA2207)
LINE_NUM	int	행 번호(ICA2029, ICA2030)
프로토콜	char(25)	잘못된 프로토콜명(ICA2112, ICA2116)
CUSTOMIZED_ATTR	char(25)	라인 번호(ICA2105, ICA2106, ICA2125, ICA2166)
ODM_ERR_NUM	int	오브젝트 데이터 관리자로부터의 오류 번호 (ICA2102, ICA2103, ICA2104, ICA2105, ICA2107, ICA2108, ICA2109,ICA2125)
APPLICATION(NT에만 해당)	char(30)	응용 프로그램 이름(ICA2200, ICA2201, ICA2202, ICA2203, ICA2204, ICA2205, ICA2206, ICA2207)

표 11. PROXY_INFO (계속). 이 테이블은 p_info.tbl 파일의 프록시 관련 오류 또는 일반적인 메세지를 포함합니다.

열	데이터 유형	짧은 설명
CALLER(NT에만 해당)	char(25)	함수 호출(ICA2200, ICA2201, ICA2202, ICA2203, ICA2204, ICA2205, ICA2206, ICA2207)
FAILED_IN(NT에만 해당)	char(25)	함수 실패(ICA2201, ICA2203)
주: 관련 메세지: ICA2004 ICA2005 ICA2006 ICA2007 ICA2009 ICA2014 ICA2015 ICA2018 ICA2019 ICA2023 ICA2029 ICA2030 ICA2031 ICA2032 ICA2033 ICA2034 ICA2035 ICA2038 ICA2039 ICA2044 ICA2045 ICA2046 ICA2047 ICA2048 ICA2049 ICA2050 ICA2051 ICA2052 ICA2053 ICA2054 ICA2055 ICA2056 ICA2057 ICA2058 ICA2059 ICA2060 ICA2061 ICA2062 ICA2063 ICA2064 ICA2065 ICA2066 ICA2067 ICA2068 ICA2069 ICA2070 ICA2071 ICA2072 ICA2073 ICA2074 ICA2100 ICA2102 ICA2103 ICA2104 ICA2105 ICA2109 ICA2110 ICA2111 ICA2112 ICA2113 ICA2114 ICA2115 ICA2116 ICA2117 ICA2118 ICA2119 ICA2120 ICA2121 ICA2122 ICA2123 ICA2124 ICA2125 ICA2126 ICA2127 ICA2166 ICA2171 ICA2172 ICA2183 ICA2200 ICA2201 ICA2202 ICA2203 ICA2204 ICA2205 ICA2206 ICA2207		

표 12. PROXY_LOGIN. 이 테이블은 p_login.tbl 파일로부터의 성공적인 프록시 로그인에 관한 정보(주로 사용자 확인에 관한)를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
사용자 ID	char(16)	사용자 ID(필수)
응용 프로그램	char(30)	응용 프로그램 이름 - 텔넷, ftp, ... (required)
AUTH_METHOD	char(15)	사용자 확인 방법(필수)
네트워크	char(25)	네트워크(보안/비보안 - 또한 추가 정보가 있을 수도 있음)(필수)
HOST_NAME	char(100)	호스트명(필수)
주: 관련 메세지: ICA2024 ICA2025 ICA2169		

표 13. PROXY_STATUS. 이 테이블은 p_stat.tbl 파일로부터 프록시 상태 정보를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
사용자 ID	char(16)	사용자 ID(ICA2008, ICA2016, ICA2021)
SRC_IP	char(15)	출발지 IP 주소(ICA2000, ICA2008, ICA2010, ICA2011, ICA2012, ICA2013, ICA2141, ICA2180)
DST_IP	char(15)	목적지 IP 주소(ICA2000, ICA2010, ICA2011, ICA2012, ICA2013)

표 13. PROXY_STATUS (계속). 이 테이블은 p_stat.tbl 파일로부터 프록시 상태 정보를 포함합니다.

열	데이터 유형	짧은 설명
REMOTE_HOST	char(100)	원격 호스트명(Firewall 시스템에서 인식하는)(ICA2021, ICA2022, ICA2027)
SID(NT에만 해당)	int	세션 식별자(ICA2177, ICA2180, ICA2181 ICA2182)
SOCKET(NT에만 해당)	char(25)	Socket 이름(ICA2177)
RC(NT에만 해당)	int	리턴 또는 이유 코드(ICA2181, ICA2182)
CMD(NT에만 해당)	char(36)	SMTP 카드(ICA2182)
주: 관련 메세지: ICA2000 ICA2010 ICA2011 ICA2012 ICA2013 ICA2016 ICA2021 ICA2022 ICA2027 ICA2097 ICA2098 ICA2141 ICA2163 ICA2164 ICA2165 ICA2177 ICA2180 ICA2181 ICA2182		

표 14. SERVER_INFO. 이 테이블은 srv_info.tbl 파일로부터 구성 서버 상태 및 활동성에 관한 정보를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
사용자 ID	char(16)	사용자 ID(ICA9003, ICA9004)
ERROR_NUM	int	시스템 오류 번호 – AIX errno 또는 Windows NT 마지막 오류(ICA9008, ICA9009) errno의 텍스트(AIX 시스템 오류)는 strerror 함수로부터 얻을 수 있습니다. Windows NT 최종 오류에 대한 텍스트는 형식 메세지 함수를 통해서나 Win32 프로그래머 참조서 볼륨 2의 부록 A에서 사용할 수 있습니다.
주: 관련 메세지: ICA9003 ICA9004 ICA9005 ICA9006 ICA9007 ICA9008 ICA9009 ICA9010 ICA9011 ICA9012 ICA9013 ICA9014 ICA9015		

표 15. 세션. 이 테이블은 session.tbl 파일로부터 SOCKS 및 프록시 세션 시작/중지 정보를 포함합니다.

열	데이터 유형(길이)	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX AIX 프로세스 ID, NT 쓰레드 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
사용자 ID	char(16)	사용자 ID(필수)
SERVICE_TYPE	char(10)	서비스 유형: socks 또는 프록시(필수)
응용 프로그램	char(30)	응용 프로그램명 - 텔넷, ftp, ... (필수)
SRC_IP	char(15)	사용자의 IP 주소(필수)
DST_IP	char(15)	원격 시스템의 IP 주소(필수)

표 15. 세션 (계속). 이 테이블은 session.tbl 파일로부터 SOCKS 및 프록시 세션 시작/중지 정보를 포함합니다.

열	데이터 유형(길이)	짧은 설명
SESSION_EVENT	char(5)	• 세션 설정시 시작. • 세션 종료시 끝남. (필수)
바이트	long int	세션 중 전송된 데이터의 양. 응용 프로그램이 텔넷이면 이 값은 0이 됩니다.
SID	long int	클록 시간에 따라, Firewall에서 생성하는 고유한 세션 식별자.
주: 관련 메세지: • Safemail 세션 시작: ICA2178 • Safemail 세션 중지: ICA2179 • Socks 세션 시작: ICA3011 • Socks 세션 중지: ICA3015 • 프록시 텔넷 세션 시작: ICA2036(AIX 로그) ICA2208, ICA2218(NT 로그) • 프록시 텔넷 세션 중지: ICA2077(AIX 로그) ICA2209, ICA2219(NT 로그) • 프록시 FTP 세션 시작: ICA2041(AIX 로그) ICA2208, ICA2218(NT 로그) • 프록시 FTP 세션 중지: ICA2076(AIX 및 NT 로그) Socks FTP 세션 조치의 세부사항은 SOCKS_FTP 테이블에 있습니다. 프록시 FTP 세션 조치의 세부사항은 PROXY_FTP에 있습니다.		

표 16. SOCKS_FTP. 이 테이블은 p_ftp.tbl 파일의 FTP 세션으로부터의 SOCKS FTP 조치 정보를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
사용자 ID	char(16)	사용자 ID(필수)
SRC_IP	char(15)	사용자의 IP 주소(필수)
DST_IP	char(15)	원격 시스템의 IP 주소(필수)
DATA_BIND	char(5)	• 데이터 바인드 설정시 '시작'.(ICA3010) • 데이터 바인드 종료시 '중지'.(ICA3014) (필수)
바이트	long int	전송된 데이터의 양.
주: 관련 메세지: ICA3010 ICA3014		

표 17. SOCKS_INFO. 이 표에는 s_info.tbl 파일의 SOCKS와 관련된 오류 또는 일반 정보 메세지가 들어 있습니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
사용자 ID	char(16)	사용자 ID(ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
조치	char(7)	연결(ICA3044, ICA3049) 또는 바인드(ICA3046, ICA3047)
ERROR_NUM	int	시스템 오류 번호 - AIX errno(ICA3013, ICA3019, ICA3031, ICA3032, ICA3040, ICA3044, ICA3101, ICA3102, ICA3103, ICA3104, ICA3106, ICA3107, ICA3108, ICA3122, ICA3124, ICA3125, ICA3126, ICA3128)
SRC_HOST	char(25)	출발지 호스트명(ICA3019, ICA3035)
DST_HOST	char(25)	목적지 호스트명(ICA3016, ICA3045)
SRC_IP	char(15)	출발지 주소(ICA3042, ICA3043, ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
DST_IP	char(15)	목적지 주소(ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
LINE_NUM	int	행 번호(ICA3022, ICA3023, ICA3024, ICA3025, ICA3026, ICA3109, ICA3110, ICA3111, ICA3112, ICA3115, ICA3116, ICA3117, ICA3118, ICA3119, ICA3120); 또는 행 수(ICA3113)
EXEC_STATUS	int	실행 상태(ICA3027)
CMD	char(36)	로그인과 같은, 명령(ICA3027, ICA3039, ICA3042, ICA3044, ICA3048) 주: ICA3042의 경우, 명령은 16진수 형식입니다.
FILE_NAME	char(100)	파일명(ICA3030, ICA3032, ICA3105, ICA3109, ICA3110, ICA3111, ICA3112, ICA3113, ICA3114, ICA3115, ICA3116, ICA3117, ICA3118, ICA3119, ICA3120)
응용 프로그램	char(30)	응용 프로그램명 - 텔넷, ftp... (ICA3044, ICA3045, ICA3049)
버전	char(10)	16진수 Socks 버전 번호(ICA3043)

표 17. SOCKS_INFO (계속). 이 표에는 s_info.tbl 파일의 SOCKS와 관련된 오류 또는 일반 정보 메세지가 들어 있습니다.

열	데이터 유형	짧은 설명
주: 관련 메세지: ICA3013 ICA3016 ICA3017 ICA3019 ICA3022 ICA3023 ICA3024 ICA3025 ICA3026 ICA3027 ICA3030 ICA3031 ICA3032 ICA3033 ICA3035 ICA3039 ICA3040 ICA3041 ICA3042 ICA3043 ICA3044 ICA3045 ICA3046 ICA3047 ICA3048 ICA3049 ICA3052 ICA3101 ICA3102 ICA3103 ICA3104 ICA3105 ICA3106 ICA3107 ICA3108 ICA3109 ICA3110 ICA3111 ICA3112 ICA3113 ICA3114 ICA3115 ICA3116 ICA3117 ICA3118 ICA3119 ICA3120 ICA3121 ICA3122 ICA3123 ICA3124 ICA3125 ICA3126 ICA3127 ICA3128		

표 18. SSL_INFO. 이 테이블은 ssl_info.tbl 파일로부터 SSL 상태 및 활동성에 관한 정보를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
Client_IP	char(15)	클라이언트의 IP 주소
주: 관련 메세지: ICA5015 ICA5022 ICA5023 ICA5028 ICA5029 ICA5036 ICA5039 ICA5060 ICA5063 ICA5082 ICA5120		

표 19. SU. 이 테이블에는 AIX su 로그를 로딩할 때 su.tbl 파일의 SU 활동에 대한 세부사항이 들어 있습니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수) AIX에서 su 로그 파일에 연도를 기록하지 않으므로, DATE_TIME 열의 연도부분은 월/일 설정값에 따라(월/일이 현재 월/일보다 늦은 경우, 지난 해를 가정), 현재 연도 또는 이전 연도로 설정됩니다.
FROM_USERID	char(16)	사용자 ID(필수)
TO_USERID	char(16)	사용자 ID(필수)
LOGIN_STATUS	char(7)	로그인 시도 상태: 성공 또는 실패(필수)

표 20. TUNNEL_CONTEXT. 이 테이블은 t_cntxt.tbl 파일로부터 활동 중인 터널 콘텍스트 사양을 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
TUNNEL_ID	long int	터널 ID(필수)
SRC_IP	char(15)	출발지 IP 주소(필수)

표 20. TUNNEL_CONTEXT (계속). 이 테이블은 t_cntxt.tbl 파일로부터 활동 중인 터널 콘텍스트 사양을 포함합니다.

열	데이터 유형	짧은 설명
DST_IP	char(15)	목적지 IP 주소(필수)
암호화	char(7)	암호화 알고리즘 DES_CBC 또는 CDMF
주: 관련 메세지: ICA1043		

표 21. TUNNEL_POLICY. 이 테이블은 t_policy.tbl 파일로부터 터널 규정 명령문을 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
규정	char(60)	fwpolicy 파일로부터 읽혀진 규정 명령문(필수)
주: 관련 메세지: ICA1040		

표 22. TUNNEL_STATUS. 이 테이블은 t_stat.tbl 파일로부터 터널의 상태 변경사항에 관한 정보를 포함합니다.

열	데이터 유형	짧은 설명
DATE_TIME	date_time	조치에 대한 날짜 및 시간(필수)
Firewall	char(100)	Firewall 시스템의 완전히 규정화된 이름(필수)
PID	int	AIX 프로세스 ID, NT 쓰레드 ID(필수)
MSG_NUM	int	메세지 번호(필수)
SESSION_SCKT	long int	세션 socket 포트(ICA1038의 경우)
MASTER_SCKT	long int	마스터 socket 포트(ICA1038의 경우)
TUNNEL_ID	long int	터널 ID가 삭제됨(ICA1041의 경우)

주:

관련 메세지: ICA1038 ICA1039 ICA1041 ICA1042

- 정의된 규정의 세부사항(ICA1039)을 TUNNEL_POLICY 테이블로부터 얻을수 있습니다.
- 정의된 터널 콘텍스트의 세부사항(ICA1042)을 TUNNEL_CONTEXT 테이블로부터 얻을 수 있습니다.

제3장 SafeMail 플러그인 소프트웨어 개발 키트

IBM Firewall SafeMail 게이트웨이의 1차적인 목적은 보안 네트워크 상의 호스트명을 은닉하면서, 보안 및 비보안 네트워크 간에 전자우편을 전달하는 것입니다.

SafeMail 게이트웨이는 그 자신만의 내용 필터링 기능을 제공하지 않습니다. 그러나 SafeMail Content Screener를 작성하여 이를 SafeMail 게이트웨이 플러그인과 같이 Firewall에 설치할 수 있습니다. 여러분의 SafeMail 게이트웨이 플러그인에는 전자 우편 메세지 전체를 열람하고, 사용자가 설정한 기준에 따라 전자 우편을 가려낼 수 있는 기능이 있습니다. SafeMail 게이트웨이 플러그인은 SafeMail 게이트웨이에게 메세지 전송을 중단하거나 메세지를 게이트웨이를 통해 전달하도록 알려줄 수 있습니다.

SafeMail 처리 개요

SMTP 클라이언트가 SafeMail 게이트웨이에 연결될 때, SafeMail 게이트웨이는 목적지 SMTP 서버에 연결하여, 클라이언트로부터 전자우편을 수신하게 되면 클라이언트로부터 목적지 서버로 한 번에 전자우편 메세지 한 행씩을 전달합니다. SafeMail 게이트웨이는 보안 네트워크 호스트의 이름을 은닉하기 위해 필요한 경우, 전자우편의 특정 헤더 행들을 재작성합니다.

내용 보호막 플러그인이 설치되어 있는 경우, SafeMail 게이트웨이는 전자우편 메세지의 각 행이 게이트웨이를 통과할 때마다 내용 보호막을 호출합니다. 또한 SafeMail 게이트웨이는 전자우편 메세지의 출발지와 목적지에 관한 정보 및 기타 정보를 통과시켜, 내용 보호막이 다양한 호출들을 상호 연관시킬 수 있도록 합니다. 이는 내용 보호막이 해당 메세지를 Firewall을 통과하도록 할 것인지 여부를 결정하기 전에 전체 메세지가 분석되어야 하는 경우 유용합니다.

SafeMail 게이트웨이가 보안 네트워크 상의 호스트명을 은닉하기 위해 헤더를 재작성해야 하는 경우, 헤더가 재작성되기 전에 내용 보호막 플러그인이 호출됩니다.

SafeMail 게이트웨이 플러그인 작성

SafeMail 게이트웨이 플러그인을 작성 및 설치하려면 다음과 같이 해야 합니다.

- 플러그인 DLL에 대한 소스 코드를 작성합니다.
- DLL을 빌드합니다.
- Firewall에서 DLL을 설치합니다.

ROOTDIR\samples\safemail에는 내용 보호막 플러그인, 필요한 헤더 파일 및 IBM Visual Age와 Microsoft Visual C++의 Make File 예제가 들어 있습니다. *ROOTDIR*은 설치 프로세스 동안에 IBM Firewall의 목표 위치로 여러분이 선택한 디렉토리입니다.

소스 코드 작성

내용 보호막 플러그인은 다음과 같은 프로토타입을 갖는 UsrCheck라는 기능을 구현해야 합니다.

```
int _Export UsrCheck(pCheckData Data);
```

이는 내용 보호막이 점검해야 할 전자우편 메세지 행이 있을 때 SafeMail 게이트웨이가 호출하는 입력점입니다. 이 기능은 전자우편 메세지 행을 검사하고, 해당 메세지가 SafeMail 게이트웨이를 통과하도록 하려는 경우 0을, SafeMail이 메세지 처리를 중단하도록 하고자 하는 경우는 0이 아닌 값을 리턴합니다.

SafeMail 게이트웨이와 내용 스크리너간의 인터페이스에 대한 완전한 설명은 ROOTDIR\samples\safemail의 usrcheck.c의 샘플 코드를 참조하십시오.

점검 기능의 pCheckData 매개변수는 ROOTDIR\samples\safemail의 usrcheck.h에 문서화 되어 있는 C 구조입니다. 이 구조에는 SMTP 서버의 출발지 및 목적지 주소와 송수신하는 SMTP 서버에 대한 네트워크 유형(보안 또는 비보안)과 같은 처리될 전자우편 메세지에 대한 중요한 정보가 들어 있습니다. 또한 이 구조에는 내용 보호막이 복수의 호출을 하나의 전자우편 메세지에 연관시키도록 해주는 변환 상관자가 들어 있습니다.

DLL 빌드

내용 보호막 플러그인에 대한 소스 코드를 작성할 때, 이를 컴파일하고 DLL로 링크해야 합니다. DLL의 이름은 smusr.dll이 되어야 합니다. 그리고 UsrCheck 입력점이 DLL로부터 반출되어야 합니다. DLL을 올바르게 빌드하는데 필요한 적절한 컴파일 및 링크 스위치의 예는 ROOTDIR\samples\safemail의 Sample make file을 참조하십시오. Sample make file은 IBM VisualAge C++ 및 Microsoft Visual C에 대해서 제공됩니다.

DLL 설치

일단 성공적으로 smusr.dll을 빌드했으면, 이를 Firewall에 설치해야 합니다. smusr.dll을 Firewall의 \bin 디렉토리로 복사하십시오. 그리고나서 Windows NT 제어 패널에서 서비스 제어 관리자를 사용하여, 플러그인이 로드되도록 IBM Firewall SafeMail 서버를 중단한 후 다시 시작하십시오.

IBM Firewall은 Firewall \bin 디렉토리에 샘플 smusr.dll을 제공합니다. 빌드한 smusr.dll을 디렉토리로 복사하기 전에 이 DLL의 이름을 변경하여, 앞으로 플러그인을 제거한 경우 이를 다시 복원할 수 있도록 하십시오.

이 장 및 다음 두 장에서 컴파일러의 이름은 인스턴스마다 다릅니다. 세 장 모두 같은 두 가지 컴파일러를 참조합니다.

제4장 로그 아카이버 플러그인 소프트웨어 개발 키트

IBM Firewall 로그 디먼은 구성 클라이언트의 **로그 기능** 대화 상자를 사용하여 지정한 파일에 로깅 정보를 기록합니다. 그러면 fwlogmgmt 명령을 사용하여 오래된 로그 레코드들을 주기적으로 아카이브합니다. 보통 fwlogmgmt 명령을 Windows NT Scheduler에서 실행시킵니다. 디폴트로 fwlogmgmt 명령은 오래된 로그 레코드를 디렉토리로 아카이브하고, Windows NT 압축(compact) 명령을 사용하여 압축합니다. 그러나 로그 아카이버 플러그인을 작성하여 디폴트 아카이브 조치를 대체할 수 있습니다.

로그 아카이버 플러그인 작성 방법

로그 아카이버 플러그인을 작성하려면 다음과 같이 해야 합니다.

1. 플러그인 DLL에 대한 소스 코드를 작성합니다.
2. DLL을 빌드합니다.
3. Firewall에서 DLL을 설치합니다.

ROOTDIR\sample\logarch 디렉토리에는 Firewall의 디폴트 조치를 복사하는 로그 아카이버 플러그인의 샘플 코드와, C++용 IBM Visual Age for C++에 대한 Make file이 들어 있습니다. *ROOTDIR*은 설치 프로세스 동안에 IBM Firewall의 목표 위치로 여러분이 선택한 디렉토리입니다.

소스 코드 작성

로그 아카이버 플러그인은 아카이브 기능을 수행하기 위하여 Firewall이 사용하는 몇가지 기능들을 구현해야 합니다. 이러한 기능들의 프로토타입은 ROOTDIR\sample\logarch 디렉토리의 fwarch.h에 정의되어 있습니다.

이 기능은 아카이브로 파일을 추가하고, 아카이브에서 파일을 추출하며, 아카이브를 최신으로 갱신하고, 아카이브의 파일을 나열하는 등의 기본적인 아카이브 기능을 구현합니다.

이 기능들에 대한 자세한 내용은 ROOTDIR\sample\logarch 디렉토리의 fwarch.c의 샘플 코드를 참조하십시오.

DLL 빌드

로그 아카이버 플러그인에 대한 소스 코드를 작성할 때, 이를 컴파일하고 DLL로 링크해야 합니다. DLL의 이름은 fwarch.dll이 되어야 합니다. fwarch.h에 나열된 기능들은 모두 DLL로부터 반출되어야 합니다.

샘플 코드를 적절한 DLL로 빌드해주는 C++용 IBM VisualAge의 Sample make file을 ROOTDIR\sample\logarch 디렉토리에서 제공합니다.

DLL 설치

fwarch.dll을 성공적으로 빌드한 후에 이를 Firewall에 설치하십시오. fwarch.dll을 ROOTDIR\bin 디렉토리에 복사하십시오.

Firewall의 디폴트 fwarch.dll도 이 디렉토리에 위치합니다. 대체 DLL을 디렉토리에 복사하기 전에 먼저 이 DLL을 백업해 놓거나 다른 이름으로 재명명하십시오.

현재 fwlogmgmt 명령이 실행되지 않고 있으며, 디폴트 DLL을 대체할 때 IBM Firewall 로그 디먼이 실행되고 있지 않음을 확인하십시오. 서비스 제어 관리자를 사용하여 IBM Firewall 로그 디먼을 중단하고, DLL을 대체한 후에 이를 다시 시작하십시오.

제5장 고유의 사용자 확인 방법 제공

이 장에는 고유의 사용자 확인 방법 제공에 대한 정보가 나와 있습니다.

사용자 제공 사용자 확인

ROOT_DIR\bin\authsdk 디렉토리에는 사용자 확인 샘플이 들어 있습니다. 포함된 파일은 다음과 같습니다.

- authschm.h - 인테페이스 정의 파일
- authus.cpp - 샘플 스킴(scheme)에 대한 소스 파일
- gwauth4.lib - Firewall의 라이브러리
- msvc++.mak - Microsoft Visual C Make 파일
- schmname.h - 인터페이스 정의 파일
- vac++.mak - IBM Visual Age Make 파일

IBM의 Visual Age에 대한 사용자 확인 샘플을 컴파일하려면, 다음 명령을 사용하십시오.

- nmake -f vac++.mak - DLL 구축
- nmake -f vac++.mak install - DLL 구축 및 설치
- nmake -f vac++.mak clean - 로컬 디렉토리 크린업

Mircosoft의 Visual C에 대한 사용자 확인 샘플을 컴파일하려면, 다음 명령을 사용하십시오.

- nmake -f msvc++.mak - DLL 구축
- nmake -f msvc++.mak install - DLL 구축 및 설치
- nmake -f msvc++.mak clean - 로컬 디렉토리 크린업

소프트웨어 개발 키트를 사용하여 사용자 제공 사용자 확인 스킴 작성

IBM Firewall에서는 써드 파티 사용자 확인 보안 제품의 통합이 가능하도록 플러그 인 인터페이스를 제공합니다. Firewall의 사용자 확인 스킴 인터페이스에 플러그인하는 사용자 확인 스킴을 작성하여 이를 실행합니다.

Firewall 사용자 확인 프로세스 개요

다음 Firewall 서비스에서는 사용자가 Firewall 서비스에 액세스할 수 있기 전에 사용자를 확인해야 합니다.

- IBM Firewall 구성 서버
- IBM Firewall 프록시 FTP 디먼
- IBM Firewall 프록시 HTTP 디먼
- IBM Firewall 텔넷 디먼
- IBM Firewall Socks 서버

Firewall에서는 다음의 사용자 확인 스킴(scheme)을 제공합니다.

모두 거부
사용자는 항상 서비스로의 액세스를 거부합니다.

모두 허용
사용자는 챌린지 없이 서비스에 액세스할 수 있습니다.

Firewall 암호
사용자는 Firewall 사용자 데이터베이스에 정의된 암호에 대해 챌린지됩니다.

NT 로그온 암호
사용자는 그 Windows NT 로그온 암호에 대해 챌린지됩니다.

SecureNetKey
사용자가 AssureNet Pathways SecureNet 키로 확인됩니다.

SecurID 카드
사용자가 Security Dynamics SecurID 보안 카드로 확인됩니다.

사용된 사용자 확인 스킴은 사용자당 및 서비스당 기준으로 정의될 수 있습니다. 예를 들어, Firewall은 사용자 *John*이 IBM Firewall 구성 서버로 로그온하려고 할 때, 그 Windows NT 로그온 암호에 대해 챌린지되도록 구성될 수 있습니다. 그러나 *John*이 IBM Firewall 텔넷 프록시를 사용하려고 하면, John은 그 SecurID 카드를 사용하여 확인됩니다. 그 사이에, 사용자 *Mary*가 IBM Firewall 구성 서버에 로그온하려고 하면, Mary는 그 Firewall 암호에 대해 챌린지됩니다. Firewall 제공 사용자 확인 스킴과 각 사용자마다 이들을 정의하는 방법에 대한 자세한 내용은 *IBM eNetwork Firewall 사용자 안내서*를 참조하십시오.

IBM Firewall에서 제공된 사용자 확인 스킴외에도, 최대 3개의 사용자 제공 사용자 확인 스킴까지 설치할 수 있습니다. 이들 스킴(scheme)을 작성하여 기존의 보안 기반과 상호 작용할 수 있으며, 아니면 써드 파티 보안 벤더에서 이들을 확보하여 그 제품을 Firewall과 통합할 수 있습니다.

사용자 제공 사용자 확인 스킴을 포함하여 Firewall의 각 사용자 스킴은 사용자 확인 스킴 API를 구현하는 DLL에 의해 표시됩니다. 이들 API는 사용자 확인 스킴에서 Firewall에 그 자체를 등록하는 방법과 Firewall에서 사용자 확인 요청을 이 스킴에 전달하는 방법을 정의합니다.

사용자 제공 사용자 확인 스킴 작성

사용자 제공 사용자 확인 스킴(scheme) 작성은 다음의 단계로 구성됩니다.

- 사용자 확인 스킴 API를 구현할 소스 코드 작성
- 소스 코드를 DLL로 컴파일 및 링크
- Firewall에 DLL 설치

사용자 제공 사용자 확인 스킴을 작성하는 데 필요한 C 소스 헤더 파일과 라이브러리 파일뿐만 아니라 Microsoft Visual C++ 및 C++용 IBM Visual Age에 대해 동일한 코드 및 동일한 Make file도 ROOTDIR\bin\authsdk에서 찾을 수 있습니다.

소스 코드 작성

모든 사용자 확인 스킴은 다음과 같은 두 가지 단계를 실행해야 합니다.

1. Firewall에 그 자체 등록
2. AuthSchmFn 구현

Firewall에 등록: Firewall 서비스가 시작되기 전에, Firewall은 \bin\authschm 서브디렉토리에서 찾은 모든 DLL 파일을 로드하려고 시도합니다. 각 DLL이 로드되면, 그 초기화 루틴은 Firewall 에 그 자체를 등록하기 위해 registerAuthSchm이라는 Firewall의 함수를 호출해야 합니다.

registerAuthSchm 함수 프로토타입은 authschm.h header 파일에 정의되어 있습니다. 이는 authschm.h에서도 정의되어 있는 AuthSchmInfo 구조의 포인터인 매개변수 하나를 취합니다. AuthSchmInfo 구조는 Firewall이 사용자 확인 요청을 사용자 확인 스킴으로 전달하기 위해 호출해야 하는 해당 AuthSchmFn의 주소와 사용자 확인 스킴 이름을 관련시킵니다.

사용자 제공 사용자 확인 스킴은 다음 3가지 이름 중 하나를 사용해야 합니다.

1. user
2. userauth2
3. userauth3

헤더 파일 schmname.h에 이들 이름에 대해 정의된 기호 이름이 있습니다. 복수 사용자 제공 사용자 확인 스킴(scheme)에서 같은 이름을 필요로 하는 두 개의 서로 다른 스킴(scheme)에 대해 걱정할 필요가 없이 동일한 Firewall에 설치될 수 있도록, 일반 사용자가 사용될 이들 3가지 이름 중 하나를 지정할 수 있게 사용자 제공 사용자 확인 스킴(scheme)을 설계해야 합니다.

DLL 초기화 루틴이 레지스터 AuthSchm을 성공적으로 호출하여 호출자에게 리턴하고 나면, DLL에서는 사용자 확인 요청을 처리할 준비가 되어야 합니다. 이러한 이유로 인해, DLL 초기화 루틴에서도 스킴 고유의 초기화를 실행하는 것이 필수적일 수 있습니다.

AuthSchmFn 구현: 각 사용자 확인 스킴(scheme) DLL은 authschm.h에 정의된 프로토타입을 사용하여 호출된 함수 AuthSchmFn을 구현해야 합니다. AuthSchmFn 함수에는 한 개의 매개변수, AuthReq 구조의 포인터가 있습니다. AuthReq 구조는 현재 사용자 확인 요청에 관련된 모든 정보가 들어 있는 간단한 C 구조입니다. AuthReq는 authschm.h에 정의되어 있습니다. AuthReq 구조에는 확인 중인 사용자의 이름, 사용자 확인을 요청하는 Firewall

구성요소/서비스 및 요청에 관한 기타 정보가 들어 있습니다. AuthReq 구조의 정보의 완전한 리스트 및 설명은 authschmh 안에 있는 이에 관한 주석을 참조하십시오.

사용자 이름과 Firewall 구성요소외에도, 사용자 확인 스킴을 구현하는 데 있어 특히 중요한 3가지 매개변수가 AuthReq 구조 내에 있습니다.

gwaput

이것은 Firewall에서 제공하는 콜백(call back) 루틴의 주소로서, 사용자에게 메세지를 전송해야 할 때마다 사용자 확인 스킴에서 사용할 수 있습니다. 예를 들어, 사용자 확인 스킴이 사용자에게 프롬프트 메세지를 발행해야 할 경우, 이 스킴은 이를 실행하도록 gwaput 매개변수에서 제공된 입력점을 호출하게 됩니다. gwaput 콜백 함수는 authschm.h에 있는 AuthSchmPut typedef에 의해 프로토타입됩니다. AuthSchmFn이 이 호출에서 전달해야 하는 매개변수의 완전한 리스트는 AuthSchmPut typedef에 대한 주석을 참조하십시오.

gwaget

이것은 Firewall에서 제공되는 콜백(call back) 루틴의 주소로서, 확인되고 있는 일반 사용자의 응답을 검색해야 할 때마다 사용자 확인 스킴을 사용할 수 있습니다. 예를 들어, 사용자 확인 스킴이 사용자로부터 암호를 얻어야 할 경우, 이 스킴은 이를 실행하도록 gwaget 매개변수에서 제공된 입력점을 호출하게 됩니다. gwaget 콜백 함수는 authschm.h에 있는 AuthSchmGet typedef에 의해 프로토타입됩니다. AuthSchmFn이 이 호출에서 전달해야 하는 매개변수의 완전한 리스트는 AuthSchmGet typedef에 대한 주석을 참조하십시오. 특히 중요한 하나의 매개변수는 반향(echo) echo 매개변수입니다. AuthSchmFn에서는 이 매개변수를 사용하여 사용자의 응답이 사용자에게로 다시 반향되어야 하는지 여부를 나타낼 수 있습니다.

opaque_data

opaque_data 필드는 AuthSchmFn에 대한 호출을 그 콜백(call back) 루틴에 대한 호출과 관련시키기 위해 Firewall에서 사용됩니다. gwaget 또는 gwaput 루틴을 호출할 때, AthSchmFn에서는 AuthReq 구조상에 있는 루틴으로 전달되었을 때와 동일한 opaque_data값을 전달해야 합니다.

사용자 확인 스킴이 모든 Firewall 구성요소와 상호작용할 수 있어야 한다는 점에 유의하십시오. 일부 Firewall 구성요소는 일반 사용자와의 복수의 챌린지/응답 대화를 지원할 수 있습니다. 이들 구성요소는 대화식 Firewall 구성요소라고 합니다. 일부 Firewall 구성요소는 그 프로토콜의 특성으로 인해 하나의 챌린지/응답만 지원할 수 있습니다. 이들을 비-대화식 Firewall 구성요소라 합니다.

사용자 제공 사용자 확인 스킴(scheme)은 AuthReq 구조의 구성요소 필드에 의해 표시된 대로, 이를 호출하는 Firewall 구성요소에 따라 그 활동을 수정할 수 있어야 합니다. 구성요소 필드의 유효한 값은 authschm.h에 정의되어 있습니다. 구성요소 필드의 현재 유효한 값은 다음과 같습니다.

표 23. 구성요소 필드에 유효한 값

AuthSchm.h의 구성요소 기호	**Firewall 구성요소**	**대화식/비대화식**
AUTHSCHM_UNKNOWN	신규 또는 인식하지 못한 Firewall 구성요소	대화식으로 가정
AUTHSCHM_REMADMIN	구성 서버	대화식
AUTHSCHM_FTP	FTP 프록시	비대화식
AUTHSCHM_TELNET	텔넷 프록시	대화식
AUTHSCHM_HTTP	HTTP 프록시	대화식
AUTHSCHM_SOCKS_PWD	암호 확인을 사용한 Socks 서버	비대화식
AUTHSCHM_SOCKS_CRAM	CRAM 확인을 사용한 Socks 서버	대화식
AUTHSCHM_REMIPSEC	원격 클라이언트 IPSEC 서버(현재 Windows NT에서 사용할 수 없음)	대화식

AuthSchmFn에서 그 처리를 완료했으면, authschm.h에 정의되어 있는 GWA 리턴 코드 중 하나와 함께 호출자로 리턴해야 합니다. 이 리턴 코드는 사용자가 성공적으로 확인되었는지 여부와 처리시 오류의 존재 여부를 나타내는 데 사용됩니다.

표 24. GWA 리턴 코드

리턴 코드	**의미**
GWA_OK	처리 중에 오류가 발생하지 않았으며, 사용자가 성공적으로 확인되었습니다.
GWA_DENY	처리 중에 오류가 발생하지 않았으나, 사용자가 그 자신을 확인하는 데 실패했습니다.
GWA_IOFAILURE	사용자에게 프롬프트를 전송하려고 하거나 사용자로부터 응답을 얻으려고 하는 중에 오류가 발생했습니다. 일반적으로 콜백(call back) 루틴에 오류가 있는 경우, 이것이 리턴됩니다.
GWA_BUFFERTOOSMALL	AuthSchmFn 함수가 응답을 수신하는 데 충분히 큰 버퍼를 할당할 수 없었으므로, 사용자로부터 응답을 검색할 수 없었습니다.
GWA_NOAUTHFN	오류 - 사용자 확인 스킴에 적절하지 않음
GWA_FNNOTREG	오류 - 사용자 확인 스킴에 적절하지 않음
GWA_RSVNAME	오류- 사용자 확인 요청에 예약된 이름이 들어 있어, 이 사용자 확인 스킴(scheme)에 사용될 수 없습니다.
GWA_BADNETTYPE	오류 - 사용자 확인 스킴에 적절하지 않음

표 24. GWA 리턴 코드 (계속)

리턴 코드	의미
GWA_BADAPP	오류 - 사용자 확인 스킴에 적절하지 않음
GWA_BADADDR	오류 - 사용자 확인 요청에 제공된 주소가 유효하지 않습니다.
GWA_MEMSHORTAGE	오류 - 메모리를 할당할 수 없었으므로, 사용자 확인 요청이 처리될 수 없었습니다.
GWA_USERDBFAIL	오류 - Could not query a required dababase
GWA_REGFAILED	오류 - 사용자 확인 스킴에 적절하지 않음
GWA_AUTHERROR	오류 - 사용자 확인 스킴 고유 오류 상태
GWA_INTERNAL	오류 - 사용자 확인 스킴의 기타 오류 상태

AuthSchmFn이 Firewall으로 리턴되면, 리턴 코드가 GWA_OK인 경우, 사용자는 확인되도록 고려되며 요청된 서비스에 대한 액세스가 제공됩니다. GWA_DENY는 오류가 아닌 상태로 처리되지만, 사용자는 요청된 서비스에 대한 액세스를 거부합니다. 다른 모든 리턴 코드가 오류 상태이며, 사용자는 요청된 서비스에 대한 액세스를 거부합니다.

소스 코드로 컴파일 및 링크: 소스 코드를 DLL로 컴파일 및 링크시, authschm.h에 정의된 입력점 이름을 분석하기 위해 \bin\authsdk 디렉토리에 제공된 gwauth4.lib를 사용하여 gwauth4.dll에 DLL을 링크해야 합니다. 또한, AuthSchmFn이 DLL로부터 반출되지 않는다는 점도 중요합니다. C++용 IBM VisualAge 및 Microsoft Visual C++에 대한 일부 make 파일은 \bin\authsdk 디렉토리에서 제공됩니다.

DLL 설치: 일단, DLL이 성공적으로 구축되었으면, 이를 ROOTDIR\bin\authschm 디렉토리에 복사한 후, Firewall 시스템을 다시 부트하십시오. Firewall에서 DLL을 로드하려고 시도하고 DLL의 사용자 확인 스킴을 등록하기 위해서는 재부팅이 필요합니다.

모두 함께 넣기: 57페이지의 그림 1은 사용자 확인 스킴(scheme)이 로드되는 방법과 사용자 확인 요청 처리시 키 함수 호출을 보여줍니다.

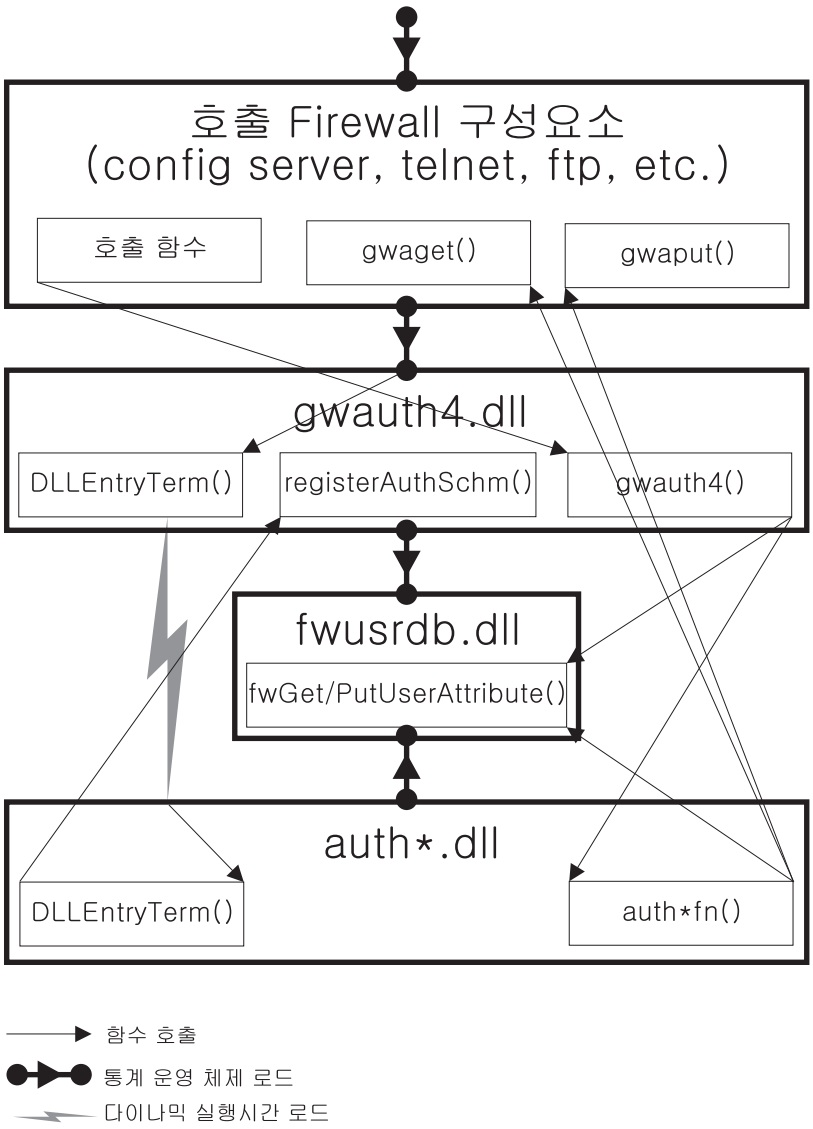

그림 1. DLL 초기화 및 등록

사용자 확인 서비스를 사용해야 하는 Firewall 구성요소는 gwauth4라는 Firewall DLL과 링크합니다. gwauth4 dll이 로드되면, 그 DLLEntryTerm 루틴이 호출되어 ROOTDIR\bin\authschm에서 모든 DLL의 수행시 로드를 시도하게 됩니다. 사용자 확인 스킴이 로드하는 데 실패할 경우, 이것은 gwauth4 dll 로딩에 대한 오류로 간주되지 않습니다. gwauth4 dll은 이러한 로드 시도를 차례로 나열합니다.

사용자 확인 스킴의 DLLEntryTerm 루틴이 수행되면, 이들은 gwauth4.dll에 사용자 확인 스킴을 등록해야 합니다. 이것은 registerAuthSchm을 호출하여 실행됩니다. authschm dll은 DLL에서 지원하는 각 사용자 확인 스킴마다 한번 registerAuthSchm을 호출해야 합니다. registerAuthSchm 함수상에서 전달된 AuthSchmInfo 구조는 사용자 데이터베이스에 저장된 대로의 사용자 확인 스킴의 이름을 AuthSchmFn 함수의 입력점과 연관시킵니다. 등록 함수는

authschm dll에서 필요한 만큼 이 구조를 재사용/수정할 수 있도록 이 함수에 전달된 구조의 사본을 작성하게 됩니다. 사용자 확인 스킴 DLL은 AuthSchmInfor 구조도 해제해야 합니다.

registerAuthSchm 함수는 등록된 모든 사용자 함수 스킴을 나타내는 링크된 리스트를 구축해야 합니다. gwauth4의 DLLEntryTerm 루틴은 리스트 앵커를 NULL로 초기화하게 됩니다. 그런 후 authschm DLL에서 registerAuthSchm 함수를 호출하면, 이 함수는 다음을 수행합니다.

1. 전달된 이름과 동일한 이름의 항목을 찾아 사용자 확인 스킴 리스트를 스캔합니다. 동일한 이름의 항목이 존재하는 경우, 리스트에서 이를 삭제한 후 그 관련된 모든 기억영역을 삭제하십시오.
2. AuthSchmInfo 구조에 따라 AuthSchmEntry 구조를 구축한 후, 이를 사용자 확인 스킴 리스트에 추가하십시오.
3. 등록이 성공했는지(GWA_OK) 또는 실패했는지(GWA_REGFAILED)의 표시를 호출자에게 리턴합니다.

gwauth4의 DLLEntryTerm이 각 authschm dll에서 수행시 로드를 실행하고 authschm DLL이 그 사용자 확인 스킴(scheme)을 등록하면, gwauth4의 DLLEntryTerm 루틴이 호출자로 리턴됩니다. 이 때, 다른 구성요소는 gwauth4 함수를 호출하여 사용자 확인 서비스 요청을 시작할 수 있습니다.

gwauth4.dll이 언로드되면, DLLEntryTerm 루틴은 종료 처리를 위해 다시 호출됩니다. 종료를 위해 호출되면, 이 루틴은 AuthSchmList 및 그 관련 기억영역에서 모든 AuthSchmEntry 항목을 삭제하게 됩니다. 이것은 사용자 확인 스킴이 Firewall으로부터 그 자체의 등록을 취소하지 못하도록 실행됩니다.

사용자 확인 요청 처리: Firewall 서비스에서 사용자를 확인해야 할 경우, 이 서비스에서는 gwauth4.dll에서 함수를 호출합니다. gwauth4에서는 해당 호출 구성요소에서 정보를 취하고 Firewall 사용자 데이터베이스를 조회하여 요청을 처리하는 데 사용할 사용자 확인 스킴의 이름을 판별합니다.

일단 gwauth4에서 사용자 확인 스킴의 이름을 판별했으면, 여기에서는 스킴에 대해 등록된 사용자 확인 스킴의 해당 리스트를 동일한 이름에 의해 스캔합니다. 동일한 이름에 의해 등록된 스킴을 찾으면, 현재 요청을 나타내는 AuthReq 구조를 구축하고 이름과 관련된 사용자 확인 스킴 DLL의 입력점을 호출합니다.

gwauth4 프로세스에서 호출된 AuthSchmFn 함수는 요청을 처리한 후, 일반 사용자와의 대화에 필요한 만큼 gwaget 및 gwaput 콜백(callback)을 호출합니다. 그 처리가 완료되면, 해당 리턴 코드와 함께 gwauth4로 제어를 리턴합니다.

gwauth4는 적절한 로그 레코드를 작성하여 사용자 확인 요청을 문서화한 후, 사용자 확인 스킴(scheme) DLL에서 수신한 리턴 코드를 전달하는 요청이 시작되는 Firewall 구성요소로 다시 리턴합니다.

제6장 Make Key File 유틸리티 사용(MKKF)

보안 SSL 네트워크 연결을 구성하려면, 먼저 다음을 실행해야 합니다.

- SSL에 대한 사용자 구성 서버 구성
- 보안 통신을 위한 키 작성
- 서버에서 신뢰할만한 root로 지정됨
- 키 파일 암호 폐기

초기 서버 키, 키 링 파일 및 인증 요청을 작성하려면 MKKF를 사용하십시오. 또한 MKKF는 키 링으로 초기 인증을 수신하고 키 파일 암호를 폐기하는 데 사용됩니다.

키파일 작성

이 유틸리티를 실행할 때 Windows NT 관리자 계정을 사용하여 로그온해야 합니다.

1. ROOTDIR\config 디렉토리로 가서 다음을 입력하여 키 유틸리티를 시작하십시오.

   ```
   c:\program files\IBM\Firewall\config > mkkf

   MKKF 키 관리자
   Copyright IBM Corp. 1996
   All Rights Reserved
   ```

2. 새로운 키 링 파일을 작성하십시오.

   ```
   키 링 메뉴
   현재 선택된 키 링: (없음)

   N - 새로운 키 링 파일 작성
   O - 키 링 파일 열기
   X - 종료

   명령을 입력하십시오. n
   ```

   새로운 키 파일을 작성하려면 위에 표시된 것처럼 'n'을 입력하십시오.

   키 파일에 사용할 파일명을 입력하도록 프롬트가 표시됩니다. 임의의 파일명을 사용할 수 있으며, .kyr로 끝나야 합니다. 기본적으로, Firewall은 fwkey.kyr이라는 파일명을 찾습니다.

   키 링 파일의 이름을 입력하거나, ENTER 키를 눌러서 디폴트 **fwkey.kyr**을 승인하십시오.

   MKKF에서 새로운 키 파일을 작성하고 키 링 메뉴를 표시합니다. 키 파일이 현재 선택된 키 링으로 나열됨을 유의하십시오.

3. 새로운 키와 인증 요청을 작성하십시오.

```
키 링 메뉴
현재 선택된 키 링: fwkey.kyr

N - 새로운 키 링 파일 작성
O - 키 링 파일 열기
S - 키 링 파일 저장
A - 다른 파일로 키 링 저장
P - 키 링 파일 암호 설정
C - 키 링 파일에 대한 해독 파일 작성
R - 키 링 파일로 인증 수신
W - 키 및 인증에 대한 작업
X - 종료

명령을 입력하십시오. w
```

키 메뉴로 이동하려면 위에 표시된 것처럼, 'w'를 입력하십시오.

```
키 메뉴
현재 선택된 키 링: fwkey.kyr
선택된 키 항목: (없음)

L - 작업할 키 나열/선택
C - 새로운 키 및 인증 요청 작업
I - 보호된 키 파일에서 키 반입
X - 메뉴 종료

명령을 입력하십시오. c
```

새로운 키를 작성하려면 위에 표시된 것처럼 'c'를 입력하십시오.

키를 키 파일에 저장하려면, 키 파일이 암호로 보호되어야 합니다. MKKF에서 키 파일을 보호하는 데 사용할 암호를 입력하도록 프롬트를 표시합니다. 암호는 입력할 때 표시되지 않습니다. MKKF는 또한 암호가 만료되는지 여부를 묻습니다. 위에 표시된 것처럼 'n'을 입력하십시오.

```
키 파일에 사용할 암호를 입력하십시오.
password
검증을 위하여 암호를 다시 입력하십시오.
password
암호가 만료됩니까?
예의 경우 Y 또는 아니오의 경우 N을 입력하십시오.
n
암호가 성공적으로 설정됩니다.
계속하려면 ENTER 키를 누르십시오.
```

MKKF에서 작성할 키 유형을 입력하라는 메세지를 표시합니다.

```
인증 유형 메뉴 선택
S - PEM(Private Enhanced Message) 인증 요청 형식
P - PKCS10 인증 요청 형식
C - 취소

명령을 입력하십시오. s
```

위에 표시된 것처럼 's'를 입력하여 PEM 인증 요청 형식을 작성하십시오. MKKF에서는 다음과 같이 비어 있는 인증을 생성합니다.

```
보안 서버 인증 작성 메뉴

현재 인증 정보
키 이름: (없음)
키 크기: 0
서버 이름: (없음)
조직: (없음)
조직 단위: (없음)
시/군: (없음)
주/도: (없음)
우편번호: (없음)
국가: (없음)

M - 인증 필드 수정
R - 키 및 인증 요청 작성 준비
C - 취소

명령을 입력하십시오. m
```

비어 있는 인증을 수정하려면 'm'을 입력하십시오. 새로운 인증에 관한 정보를 입력하도록 프롬트가 표시됩니다.

- 사용할 이름을 입력하십시오. 이 이름은 임의의 문자열일 수 있으며 MKKF 유틸리티에서만 사용합니다.

  ```
  키 항목에 사용할 이름을 입력하십시오.

  Firewall 키
  ```

- 키 크기를 입력하십시오. IBM Firewall은 MKKF의 반출 가능 버전만을 적재합니다. 최대 키 크기는 1024입니다.

  ```
  1:   508
  2:   512
  3:   768
  4:   896
  5:   1024
  원하는 키 크기에 해당하는 숫자를 입력하십시오.

  2
  ```

- Firewall에 대한 완전한 규정화 TCP/IP 호스트 이름을 입력하십시오(예: jupiter.raleigh.ibm.com).

  ```
  서버의 완전 규정 TCP/IP 도메인 이름을 입력하거나 또는
  필드를 공백으로 두려면 Enter 키를 누르십시오.

  jupiter.raleigh.ibm.com
  ```

- 인증과 연관시킬 조직 이름을 입력하십시오(예를 들어, 회사 이름).

  ```
  인증할 조직 이름을 입력하거나 또는 필드를 공백으로
  두려면 ENTER 키를 누르십시오.
  AAA Inc.
  ```

- 조직 단위 이름을 입력하십시오(예를 들어, 부서 이름).

인증할 조직 단위 이름을 입력하거나 또는 필드를 공백으로
두려면 ENTER 키를 누르십시오.
네트워크 보안 제품

- 인증을 사용할 시를 입력하십시오.

  인증할 군/시 이름을 입력하거나 또는 필드를 공백으로 두려면
  ENTER 키를 누르십시오.
  RTP

- 주 또는 도를 입력하십시오.

  주: 인증 사양에 따라 이 필드는 최소 세 개의 문자로 이루어져야 하며, 따라서 두 글자의 일반적인 약자는 유효하지 않습니다.

  인증할 주/도 이름을 입력하거나 또는 필드를 공백으로
  두려면 ENTER 키를 누르십시오. 주/도는 적어도 세 개의
  문자여야 합니다.

  N.C.

- 인증과 연관시킬 우편번호를 입력하십시오(이것은 zip 코드와 같습니다).

  인증할 우편번호를 입력하거나 또는 필드를 공백으로 두려면
  ENTER 키를 누르십시오.
  27709

- 두 글자 국가 코드를 입력하십시오.

  인증할 국가 코드를 입력하거나 또는 필드를 공백으로 두려면
  ENTER 키를 누르십시오. 국가 코드는 정확히 두 글자여야 합니다.

  US

MKKF에서 사용자로부터 모든 정보를 수집하고 나면, 다음과 같이 인증이 표시됩니다.

보안 서버 인증 작성 메뉴

현재 인증 정보
키 이름: Firewall 키
키 크기: 512
서버 이름: jupiter.raleigh.ibm.com
조직: AAA Inc.
조직 단위: 네트워크 보안 제품
시/군: RTP
주/도 N.C.
우편번호: 27709

```
국가: US

M - 인증 필드 수정
R - 키 및 인증 요청 작성 준비
C - 취소

명령을 입력하십시오. r
```

인증 정보에 오류가 있는 경우, 수정하려면 'm'을 입력하십시오. 정보가 올바른 경우, 새로운 키와 연관된 키 파일을 작성하려면 'r'을 입력하십시오.

MKKF는 인증을 저장하기 위한 파일을 프롬트합니다. 임의의 파일명을 사용할 수 있지만, 따라야 할 좋은 규칙은 키 파일과 같은 기본 이름을 사용하고 확장자로 .cert를 추가하는 것입니다.

```
인증 요청을 저장할 파일을 입력하십시오.
fwkey.cert
개인용 키 작성 중...
개인용 키가 성공적으로 작성되었습니다.
인증 요청 작성 중...
인증 요청이 성공적으로 작성되었습니다.
새로운 키를 키 파일에 추가 중임.
새로운 키와 인증 요청이 성공적으로 작성되었습니다.
계속하려면 ENTER 키를 누르십시오.
```

4. 새로 작성된 키를 디폴트 키로 설정하십시오.

   키와 인증이 작성되고 나면, 키 메뉴가 표시됩니다. 새로 작성된 키가 선택된 키 항목으로 나열됩니다.

```
키 메뉴
현재 선택된 키 링: fwkey.kyr
선택된 키 항목: Firewall 키

L - 작업할 키 나열/선택
S - 선택된 키에 관한 정보 표시
D - 선택된 키 삭제
C - 새로운 키 및 인증 요청 작성
I - 보호된 키 파일에서 키 반입
E - 보호된 키 파일로 선택된 키 반출
F - 선택된 키를 해당 키 링에 대한 디폴트 키로 설정
U - 선택된 키의 신뢰할만한 Root 상태 표시 해제
R - 선택된 키에 대한 인증 요청 작성
X - 메뉴 종료

명령을 입력하십시오. f
```

키 파일에서 새로 작성된 키를 디폴트 키를 설정해야 합니다. 이전 예에서 표시된 것처럼 'f'를 입력하십시오. 조치를 확인하도록 프롬트가 표시됩니다.

```
키 메뉴
현재 선택된 키: Firewall 키
이 키를 디폴트 키로 설정하겠습니까?
예의 경우 Y 또는 아니오의 경우 N을 입력하십시오.
y
키가 디폴트 키로 설정되었습니다.
계속하려면 ENTER 키를 누르십시오.
```

키가 디폴트 키로 표시되고 나면, 키 메뉴가 표시됩니다.

```
키 메뉴
현재 선택된 키 링: fwkey.kyr
선택된 키 항목: Firewall 키

L - 작업할 키 나열/선택
S - 선택된 키에 관한 정보 표시
D - 선택된 키 삭제
C - 새로운 키 및 인증 요청 작성
I - 보호된 키 파일에서 키 반입
E - 보호된 키 파일로 선택된 키 반출
F - 선택된 키를 해당 키 링에 대한 디폴트 키로 설정
U - 선택된 키의 신뢰할만한 Root 상태 표시 해제
R - 선택된 키에 대한 인증 요청 작성
X - 메뉴 종료

명령을 입력하십시오. x
```

'x'를 입력하여 키 메뉴를 종료하십시오.

5. 키 링 파일로 인증을 수신하십시오.

   다음과 같이 키 링 메뉴가 표시됩니다.

```
키 링 메뉴
현재 선택된 키 링: fwkey.kyr

N - 새로운 키 링 파일 작성
O - 키 링 파일 열기
S - 키 링 파일 저장
A - 다른 파일로 키 링 저장
P - 키 링 파일 암호 설정
C - 키 링 파일에 대한 해독 파일 작성
R - 키 링 파일로 인증 수신
W - 키 및 인증에 대한 작업
X - 종료

명령을 입력하십시오. r
```

   주: Firewall이 인증 목적으로 SSL을 사용하지 않으므로, 사용자 인증을 인증 확인에서 서명받을 필요가 없습니다.

```
파일명을 입력하거나 Cert.txt를 사용하려면 ENTER 키를 누르십시오.
fwkey.cert
이것은 자체 서명 인증입니다. 키 파일에 추가하겠습니까?
예의 경우 Y 또는 아니오의 경우 N을 입력하십시오.
y
인증이 키 링에 추가되었습니다.
계속하려면 ENTER 키를 누르십시오.
```

6. 키 파일에 대한 해독 파일을 작성하십시오.

   인증이 키 링에 추가되고 나면, 다음과 같이 키 링 메뉴가 표시됩니다.

```
키 링 메뉴
현재 선택된 키 링: fwkey.kyr

N - 새로운 키 링 파일 작성
O - 키 링 파일 열기
```

```
S - 키 링 파일 저장
A - 다른 파일로 키 링 저장
P - 키 링 파일 암호 설정
C - 키 링 파일에 대한 해독 파일 작성
R - 키 링 파일로 인증 수신
W - 키 및 인증에 대한 작업
X - 종료

명령을 입력하십시오. c
```

키 파일에 대한 해독 파일을 작성해야 합니다. 이전 예에 표시된 것처럼 'c'를 입력하십시오. MKKF에서는 키 파일명과 같은 기본 이름을 사용하고 확장자로 .sth를 사용합니다.

```
해독된 암호 파일이 fwkey.sth에 저장됩니다.
계속하려면 ENTER 키를 누르십시오.
```

해독 파일이 작성되고 나면, 키 링 메뉴가 표시됩니다.

```
키 링 메뉴
현재 선택된 키 링: fwkey.kyr

N - 새로운 키 링 파일 작성
O - 키 링 파일 열기
S - 키 링 파일 저장
A - 다른 파일로 키 링 저장
P - 키 링 파일 암호 설정
C - 키 링 파일에 대한 해독 파일 작성
R - 키 링 파일로 인증 수신
W - 키 및 인증에 대한 작업
X - 종료

명령을 입력하십시오. x
```

이제 키 파일을 사용할 준비가 되었습니다. MKKF를 종료하려면 위에 표시된 것처럼 'x'를 입력하고 키 파일 변경사항을 저장하려면 다음에 표시된 것처럼 'y'를 입력하십시오.

```
키 링 파일이 변경되었습니다. 저장하겠습니까?
예의 경우 Y 또는 아니오의 경우 N을 입력하십시오.
y
키 링이 fwkey.kyr에 저장되었습니다.
계속하려면 ENTER 키를 누르십시오.
#
```

7. 구성 파일 갱신.

   키 파일을 작성한 후에는 fwcfgsrv 명령을 사용하여 구성 서버 매개변수 파일에 키 파일명을 지정해야 합니다.

   구성 서버에 대해 SSL 암호화를 사용 중인 경우에는 fwcfgsrv 명령을 사용하여 encryption=ssl 옵션도 설정해야 합니다.

   fwcfgsrv 명령을 사용한 후에는 서버 서비스를 중지한 후 다시 시작하십시오.

제7장 문제해결 및 검사

이 장에서는 IBM Firewall 설정 및 구성시 발생하는 몇 가지 공통적인 문제점의 해결 방법을 설명합니다.

문제가 발생하면, 먼저 디버그 우선순위를 포함한 Firewall 로그를 작성하여 로그에 전송된 정보를 늘리십시오. 자세한 정보는 6페이지의 『로그파일 관리』를 참조하십시오.

설치 및 설정

필터 지원 실패

문제 설명

다음의 오류 메세지를 수신합니다.

```
필터 지원 검증이 실패했습니다. Socket 작성 호출이 실패했습니다.
경로명에 있는 파일 또는 디렉토리가 존재하지 않습니다.
```

이 문제는 설치 후 Firewall을 재부팅하지 않음으로써 야기됩니다.

권장되는 조치

Firewall을 재부팅하고 절차를 재시도하십시오.

경로지정 문제

IBM Firewall은 **IP 경로지정 검사**라는 제목의 *보안 규정* 대화 상자에 기능을 제공하며, 경로지정 문제를 디버깅하는 데 유용합니다. 이 확인란을 활성화하고, 연결 구성을 활성화한 다음, 연결 규칙 로깅을 활성화하십시오. 그런 후, Firewall 로그를 검사하여 Firewall을 통해 이동하는 모든 패킷에 관한 자세한 정보를 열람하십시오.

먼저 IP 주소를 사용한 다음, 호스트 이름을 사용하여 이들 테스트를 수행하십시오. 트래픽이 주소를 사용하여 제대로 경로지정하지만 이름을 사용하여 그렇지 않은 경우, 자세한 정보는 69페이지의 『DNS 문제』를 참조하십시오.

Firewall에서 호스트를 ping할 수 없음

문제 설명

네트워크 인터페이스가 제대로 구성되어 있지 않습니다.

권장되는 조치

운영 체제 관련 문서를 참조하십시오.

문제 설명

비보안 네트워크에 대한 연결이 제대로 구성되어 있지 않습니다.

권장되는 조치

도움을 요청하려면 인터넷 서비스 제공자에게 문의하십시오.

문제 설명

보안 네트워크가 라우터와 격리된 경우, Firewall에는 해당 라우터에 대한 정적인 경로가 존재해야 합니다. netstat -rn을 사용하여 정적 경로지정을 검증하십시오.

```
netstat -rn
```

프로토콜 계열 2의 출력은 다음과 같습니다.

```
목적지        게이트웨이        플래그    ....
디폴트        nrr.nrr.nrr.nrr  UG
nnn.nnn.nnn   nnn.nnn.nnn.nnn  U
sss.sss.sss   sss.sss.sss.sss  U
ss1.ss1.ss1   srr.srr.srr.srr  UG
127           127.0.0.1        U
```

그림 2. netstat -rn의 샘플 출력.

nrr.nrr.nrr.nrr

인터넷에 대한 라우터를 나타내며 디폴트 경로입니다. 디폴트 경로는 정적 경로(Flag=UG)입니다.

nnn.nnn.nnn

비보안 도메인을 나타냅니다. 이것은 인터페이스 경로(Flag=U)입니다.

nnn.nnn.nnn.nnn

비보안 인터페이스를 나타냅니다.

sss.sss.sss

보안 도메인을 나타냅니다. 이것은 인터페이스 경로(Flag=U)입니다.

sss.sss.sss.sss

보안 인터페이스를 나타냅니다.

ss1.ss1.ss1

네트워크의 보안측 서브도메인을 나타내며 srr.srr.srr.srr은 해당 서브도메인에 대한 라우터를 나타냅니다. 이것은 정적 경로(Flag=UG)입니다.

127.0.0.1

루프백 또는 로컬 호스트입니다. 이것은 인터페이스 경로(Flag=U)입니다.

각 인터페이스에 대한 인터페이스 루트가 있어야 하며 디폴트 루트는 Firewall의 비보안 부분에 있는 라우터를 가리켜야 합니다.

권장되는 조치

여러분의 라우터에 정적 라우트를 추가하십시오. 라우터 관리자에게 문의하십시오. 라우트 추가 명령을 사용하십시오.

문제 설명

보안 인터페이스의 서브네트 마스크 또는 연결 시도 중인 호스트가 잘못되었습니다.

권장되는 조치

클라이언트의 구성 유틸리티를 사용하여 마스크 설정을 정정하십시오.

보안 호스트로부터 비보안 호스트를 ping할 수 없음(또는 역도 성립)

문제 설명

Firewall에 인접한 각 라우터에는 Firewall을 지나 위치하는 목적지 네트워크에 대한 게이트웨이로 Firewall을 지정하는 정적 루트가 들어 있어야 합니다.

권장되는 조치

라우터 관리자에게 문의하십시오.

문제 설명

보안 네트워크가 비보안 네트워크에서 RFC 1597에 지정된 개인용 주소를 포함하여 등록되지 않은 경로지정 가능한 주소를 사용할 경우, 패킷은 전송자에게 다시 경로지정되지 않습니다.

권장되는 조치

등록된 주소를 가진 클라이언트를 사용하십시오.

DNS 문제

Firewall DNS는 보안 이름 서버를 조회하여 이름을 해결합니다. 보안 이름 서버는 보안 네트워크에 있는 모든 이름을 해결합니다. 보안 이름 서버는 비보안 이름에 대한 요청을 Firewall 이름 서버로 전송합니다. Firewall 이름 서버는 요청을 해결하기 위해 비보안 이름 서버를 조회합니다.

DNS 문제는 Firewall 조작의 다른 영역에 영향을 줄 수 있습니다. 문제가 명백하게 DNS에 관련되지 않더라도, DNS를 점검하는 것이 좋습니다.

다음은 문제를 해결하기 위하여 `nslookup` 유틸리티를 사용하여 이 방법의 각각의 단계를 안내하는 몇 가지 예입니다. 이들 예에서, 다음과 같은 값을 사용합니다.

www.ibm.com

비보안 네트워크에 있는 임의의 호스트명을 나타냅니다.

nns.nns.nns.nns

비보안 이름 서버의 주소를 나타냅니다.

sns.sns.sns.sns
보안 이름 서버의 주소를 나타냅니다.

host.secure.company.com
보안 네트워크 내에 있는 임의의 호스트명을 나타냅니다.

127.0.0.1
Firewall 상의 루프백 주소를 나타냅니다.

이들 값은 구성 클라이언트의 **도메인 이름 서비스** 대화 상자에서 얻을 수 있습니다. 해당 연습(exercise)에서 작업할 때 이들 값이 필요합니다.

주: nslookup 명령은 nslookup이 보안 도메인 이름을 확장하지 못하도록 호스트명 다음에 추가의 점을 요구합니다.

DNS가 아직 환경설정되지 않았음

문제 설명
Firewall의 DNS 기능이 구성되어 있지 않습니다.

권장되는 조치
도메인 이름 서비스 대화 상자를 완료하십시오.

DNS 조회 실패 또는 시간 종료

문제 설명
Firewall 통신량 조절이 DNS 패킷 통과를 허용하지 않습니다.

권장되는 조치
보안 규정 패널로 이동하여 *DNS 조회의 승인* 확인란을 설정하고 통신량 조절을 다시 활성화하십시오.

nslookup www.ibm.com. nns.nns.nns.nns 실패

문제 설명
비보안 이름 서버가 표시된 주소를 사용 중이 아니거나 제대로 구성되지 않았습니다.

권장되는 조치
유효한 이름 서버 주소를 DNS 서비스 제공자에게 문의하십시오.

nslookup www.ibm.com. 127.0.0.1 실패

문제 설명
Microsoft DNS 서비스가 실행 중일 수 있습니다. 서비스 제어 관리자로 가서 이 서비스가 수행 중인지 판별하십시오.

권장되는 조치
서비스 제어 관리자를 사용하여 DNS를 시작하십시오.

nslookup host.secure.company.com. sns.sns.sns.sns 실패

문제 설명

보안 이름 서버가 중단됩니다.

권장되는 조치

이름 서버를 재시작하십시오.

nslookup www.ibm.com. sns.sns.sns.sns 실패

문제 설명

보안 이름 서버가 IBM Firewall과 상호 작용하도록 제대로 구성되지 않았습니다.

권장되는 조치

구성 요구사항에 대해서는 *IBM eNetwork Firewall 사용자 안내서*를 참고하십시오.

구성 클라이언트

서버가 응답하지 않음

문제 설명

구성 클라이언트와 구성 서버가 서로 다른 언어를 사용 중입니다.

권장되는 조치

패널상의 구성 클라이언트 로그에서, Firewall이 설치된 언어를 선택하십시오.

문제 설명

SSL 암호화가 제대로 구성되지 않았습니다.

권장되는 조치

SSL이 클라이언트 로그온 패널에서 선택되었는지 확인하십시오. 서비스 제어 관리자를 사용하여 Firewall 구성 서버를 중단한 후 다시 시작하십시오.

문제 설명

Firewall의 구성 서버의 사용이 중단되었을 수 있습니다.

권장되는 조치

Firewall 구성 서버가 수행 중인지 확인하십시오.

문제 설명

Firewall의 구성 서버가 비표준 포트를 모니터하고 있을 수 있습니다.

권장되는 조치

`c:\winnt\system32\drivers\etc\services`를 검사한 후, 행 `ibmfwrcs 1014/tcp`를 포함하는지 확인하십시오. 다른 포트에서 서버를 사용하려는 경우, `ibmfwrcs 1014/tcp`를 알맞게 편집하고 클라이언트의 로그온 패널에 새로운 포트를 지정했는지 확인하십시오. 서비스 제어 관리자를 사용하여 구성 서버를 중단한 후 다시 시작하십시오.

문제 설명

Firewall의 통신량 조절이 구성 서버와의 통신을 허용하지 않을 수 있습니다. 이것은 원격 호스트에서 실행 중인 구성 클라이언트에만 영향을 미칩니다.

권장되는 조치

구성 클라이언트가 실행되는 시스템과 Firewall이 실행되는 시스템 간 연결을 코드화하십시오. 구성 클라이언트는 연결의 출발지여야 하고 Firewall은 목적지여야 합니다. 변경사항을 재생성하여 활성화하십시오. 자세한 내용은*IBM eNetwork Firewall 사용자 안내서*를 참고하십시오.

문제 설명

원격 호스트로부터 로그인을 허용하지 않도록 구성 서버를 구성했습니다.

권장되는 조치

`fwcfgsrv` 명령을 사용하여 `localonly` 매개변수가 아니오로 설정되어 있는지 확인하십시오.

구성 서버에 로그온할 수 없음

문제 설명

Firewall에서 확인된 각 사용자 이름은 몇몇 사용자 확인 방법 중 하나를 사용하여 구성됩니다. 모든 거부는 해당 사용자에 대한 특정 서비스의 사용을 금지하는 데 사용됩니다.

권장되는 조치

사용 중인 사용자명의 보안 관리 및 비보안 관리 필드를 조사하십시오. 이들 필드는 Firewall 사용자가 아닌 관리자에 대해서만 유효합니다.

통신량 조절 필터

연결에 수행된 변경사항이 영향이 미치지 않음

문제 설명

통신량 조절 구성요소 중 하나를 변경해도 이들이 활성화될 때까지는 적용되지 않습니다. 이것은 시스템 관리 아래에 **보안 규정**을 포함합니다.

권장되는 조치

연결 활성화 대화 상자를 사용하여 구성을 재생성한 후 활성화하십시오.

프록시 서버

전송된 데이터가 없음

문제 설명

Firewall의 프록시 서비스가 설치 후 시스템이 재부트될 때까지 시작되지 않습니다.

권장되는 조치

시스템을 다시 부트하십시오.

문제 설명

Firewall의 통신량 조절은 Firewall을 통한 직접 소통이 아니라 프록시 프로세스로의 패킷 흐름을 허용하도록 구성되어야 합니다.

권장되는 조치

*IBM eNetwork Firewall 사용자 안내서*에 설명된 대로, 각 일부분의 프록시 연결을 구성하십시오.

가능한 경우 사전 정의된 서비스(특히 FTP 트래픽을 사용하여)를 사용하십시오.

원하는 호스트에 연결할 수 없음

문제 설명

데이터가 프록시를 통하여 전송되지만 호스트가 연결되지 않은 경우, 클라이언트가 제대로 호스트 이름을 해결할 수 없습니다.

권장되는 조치

*DNS 질의 승인*이 **보안 규정** 대화 상자에서 사용 가능한지 그리고 연결 구성이 활성화되었는지 확인하십시오. 자세한 정보는 69페이지의 『DNS 문제』를 참조하십시오.

문제 설명

Firewall 서비스 중 하나에 의해 Firewall에서 사용자 확인되고 있는 각 사용자 이름이 여러 개의 사용자 확인 방법 중 하나를 사용하여 구성될 수 있습니다. 모두 거부는 해당 사용자에 대한 특정 프록시의 사용을 금지하는 데 사용됩니다.

권장되는 조치

구성 클라이언트의 **사용자** 대화 상자에서 사용자 계정의 사용자 확인 설정을 조사하십시오.

사용자 확인 서비스

Windows NT 관리자 계정이 확인될 수 없음

문제 설명

Windows NT 관리자 계정에 대한 Firewall 속성은 `fwdfadm` 아래에서 Firewall 사용자 데이터베이스에 저장됩니다.

권장되는 조치

fwdfadm이 사용하려는 서비스에 대해 올바른 사용자 확인 방법 세트인지 확인하십시오.

Firewall 프록시 사용자가 확인될 수 없음

문제 설명

Firewall 프록시 사용자가 Firewall 사용자 데이터베이스에 정의되어 있지 않으면, fwdfuser 이름이 사용자의 속성을 정의하는 데 사용됩니다.

권장되는 조치

fwdfuser의 사용자 확인 방법이 사용자가 액세스하려는 서비스에 대해 올바르게 정의되어 있는지 확인하십시오.

네트워크 주소 변환

NAT 연결이 작동되지 않음

문제 설명

NAT를 설정하여 활성화했으나, 연결이 작동되지 않습니다.

권장되는 조치

경로지정 테이블의 문제점이나 NAT 구성 문제점이 있습니다.

NAT 패킷에 대해 라우트를 구성하는 방법

문제 설명

NAT 패킷에 대해 구성된 라우트가 없습니다.

권장되는 조치

목적지가 있는 Firewall 앞에서 라우터의 정적 라우트를 추가하십시오.

NAT를 돕는 데 사용할 수 있는 디버깅 툴

문제 설명

NAT를 돕는 데 사용할 수 있는 디버깅 툴은 무엇입니까?

권장되는 조치

동적으로 등록된 주소의 관리를 추적할 수 있게 해 주는 NAT 로깅.

로그 기능

로그 기능 변경사항이 서버에 적용되지 않음

문제 설명

로그 기능 삭제 또는 변경시, 이는 GUI에서 작동되는 것처럼 보이지만, 서버상에서 적용되지는 않습니다.

권장되는 조치

시스템을 다시 부트하십시오.

보고서 유틸리티

파일 액세스 중 오류 발생:

문제 설명

다음의 명령을 사용하면, 위의 오류를 볼 수 있습니다.

```
db2 -vf fwschema.dll > schema.out
db2 -vf fwimport.dat > import.out
db2 -vf fwqrysmp.dml > sample.out
```

권장되는 조치

.ddl, .dat 또는 .dml 파일에 대해 올바른 완전한 규정화 파일명을 제공하십시오.

데이터를 데이터베이스에 반입하는 중 오류 발생

문제 설명

`db2 -vf fwimport.dat>import.out` 명령에서 얻어진 import.out 파일에는 반입 중 하나가 실패했거나 부분적으로만 성공했음을 지시하는 메세지가 들어 있습니다.

권장되는 조치

문제가 발생한 반입 명령문에 해당하는 .msg 파일을 검토하십시오. 이 파일에서 그 문제에 대해 더 자세한 내용을 알 수 있습니다. 해당 .tbl 파일에서 관련 레코드(들)를 찾아 입력 데이터를 살펴보고 무엇이 잘못되었는지 판별하십시오. 예를 들면, 다음과 같습니다. 데이터베이스에서 목표 열에 비해 지나치게 깁니까? 목표 열 유형에 대해 데이터 유형이 적절합니까? 입력 데이터가 올바르게 나타나지 않을 경우, 원래 로그 파일 레코드를 찾아 `fwlogtbl`이 .tbl 파일 레코드를 올바르게 생성했는지 확인하십시오.

문제를 해결할 수 없는 경우, IBM 서비스 센터에 문의하기 전에 import.out 파일, .msg 파일, 관련된 .tbl 파일 및 원래 로그 파일을 저장하십시오.

부록A. 메세지

이 부록에는 AIX용 IBM Firewall의 메세지와 NT용 IBM Firewall의 메세지 및 두 Firewall에 공통적인 메세지가 있습니다. 또한 이 부록에서는 IBM Firewall 메세지에 관한 다음의 정보도 제공합니다.

- 메세지 형식화 방법
- 메세지 심각도 레벨
- 메세지 및 설명

메세지와 그 설명을 검토했으나 정보가 더 필요하면, 67페이지의 『제7장 문제해결 및 검사』를 참조하십시오.

메세지 태그

ICA 첫번째 3 고정 바이트

xxxx 범위 0000 – 9999 사이의 숫자.

a 심각도 지시자. 메세지는 심각도 레벨에 의해 분류됩니다.

- i – 정보
- w– 경고
- e – 오류
- s – 심각도

숫자 0000 – 9999는 계속 다음과 같은 범주로 분류됩니다.

- 0000 – 0999 침입 경보
- 1000 – 1999 필터
- 2000 – 2999 프록시
- 3000 – 3999 Socks
- 4000 – 4999 호출기
- 5000 – 8999 사용가능
- 9000 – 9999 일반/기타

메세지

ICA0001 경보 - *count* 확인에 실패했음.

설명: 사용자 확인 실패에 대한 임계값 조건이 만족되었습니다.

ICA0002 경보 - 사용자 *user_name*에 대한 *count* 확인에 실패했음.

설명: 특정 로그 메세지를 감지하기 위한 임계값 조건이 만족되었습니다.

ICA0003 경보 - *host IP address*호스트에 대한 *count*확인에 실패했음.

설명: 특정 호스트의 사용자 확인 실패 임계값 조건이 만족되었습니다.

ICA0004 **경보 - *count* 로그와 함께 *message_id* 항목을 태그하십시오.**

설명: 특정 로그 메세지를 감지하기 위한 임계값 조건이 만족되었습니다.

ICA0005 **로그 모니터 - 메모리 부족.**

설명: 프로세스를 실행할 메모리가 부족합니다.

ICA0006 **로그 모니터 - 서비스 파일 액세스 실패:** *errno*

설명: etc/services에서 fwlogmond 항목을 찾을 수 없습니다.

ICA0007 **로그 모니터 - socket 작성 실패:** *errno*

설명: Socket을 열 수 없음 - 오류 메세지를 참조하십시오.

ICA0008 **로그 모니터 - bind() 실패:** *errno*

설명: Socket을 바인드할 수 없음 - 오류 메세지를 참조하십시오.

ICA0009 **임계값 정의 파일을 열 수 없음:** *errno*

설명: 임계값 정의 파일 액세스 문제점 - 오류 메세지를 참조하십시오.

ICA0010 **로그 모니터 - 치명적인 읽기 오류:** *errno*

설명: Socket에서 읽기 문제점 - 오류 메세지를 참조하십시오.

ICA0011 **임계값 정의 파일의 상태를 얻을 수 없음:** *errno*

설명: 임계값 정의 파일 액세스 문제점 - 오류 메세지를 참조하십시오.

ICA0012 **로그 모니터 디먼 종료.**

설명: 디먼을 중지 중이거나 종료 신호를 수신했습니다. 이전 로그 메세지에서 자세한 정보를 제공합니다.

ICA0013 **로그 모니터에서 종료 신호를 수신했음**

설명: 디먼이 종료 신호를 수신했으므로 종료됩니다.

ICA0014 **로그 모니터 디먼 시작.**

설명: 디먼이 시작되었습니다.

ICA0015 **로그 모니터에 대한 디먼을 작성할 수 없음:** *errno*

설명: 디먼 작성 실패 - 오류 메세지를 참조하십시오.

ICA0016 ***process id file*을 열 수 없음 - 디먼이 이미 활동 중일 수도 있음.**

설명: 디먼이 프로세스 id 파일을 열 수 없습니다.

ICA0017 **프로세스 id(*process id*)를 *file*에 기록할 수 없음.**

설명: 디먼이 프로세스 id를 파일에 기록할 수 없음.

ICA0018 **로그 모니터 - 데이터가 없음.**

설명: 데이터 없는 패킷이 수신되었습니다. 패킷은 삭제되었습니다.

ICA0019 **로그 모니터 - 짧은 내용이 읽힘. 태그가 삭제됨.**

설명: 데이터가 부족한 패킷이 수신되었습니다. 패킷은 삭제되었습니다.

ICA0020 **로그 모니터 - ICA 태그 서식이 잘못됨.**

설명: 서식이 잘못된 데이터를 가진 패킷이 수신되었습니다. 패킷은 삭제되었습니다.

ICA0021 **로그 모니터 - 사용자 확인 데이터의 서식이 잘못됨.**

설명: 서식이 잘못된 데이터를 가진 패킷이 수신되었습니다. 패킷은 삭제되었습니다.

ICA0022 **임계값 정의 파일의 구문이 유효하지 않음(*invalid entry*).**

설명: 임계값 파일의 지정된 항목이 구문적으로 잘못되었습니다.

ICA0023 **fwmail.conf 파일을 열 수 없음.**

설명: fwmail.conf 파일 열기에 실패했거나 파일이 비어 있습니다.

ICA0024 **SMTP 서버로 연결할 수 없음.**

설명: SMTP 서버가 사용 중이거나 연결을 거부하고 있습니다.

ICA0025 **경보 메세지 전자우편 전송에 실패.**

설명: 지정한 주소로 로그 모니터 경보 메세지 전자우편을 전송할 수 없습니다.

ICA0051 **로그 파일 *log file name*의 보존 일수는 unsigned short 정수값이어야 함.**

설명: 로그 파일의 보존 일수는 유효한 정수값이어야 합니다.

ICA0052 **아카이브, *log file name*의 보존 일수는 unsigned short 정수값이어야 함.**

설명: 아카이브의 보존 일수는 정수값이어야 합니다.

ICA0053 **logmgmt.cfg에서 로그 파일, *log file name* 에 대한 복수의 항목은 허용되지 않음.**

설명: logmgmt.cfg에서 로그 파일에 대한 복수의 항목은 허용되지 않습니다.

ICA0054 ***$ Variables :*파일을 열 수 없습니다.**

설명: logmgmt.cfg 파일을 열 수 없습니다.

ICA0055 **logmgmt.cfg 파일에 유효한 항목이 없습니다.**

설명: logmgmt.cfg 파일에 유효한 항목이 없습니다.

ICA0056 **로그 메세지 *"$ Variables:"*이(가) 유효하지 않음.**

설명: 로그 메세지가 유효하지 않습니다.

ICA1001 **프로세스 ID로 파일을 작성할 수 없음.**

설명: 파일 fwlogd.pid 작성시 필터 로깅 디먼에서 오류를 발견했습니다.

사용자 응답: 디렉토리 /etc/security가 위치하는 파일 시스템을 점검하십시오. 공간 부족 조건이 존재할 수 있습니다.

ICA1002 **cfgfilt 프로그램과의 통신이 가능하지 않음.**

설명: fwlogd.pid 파일이 작성되지 않았으므로, fwlogd 디먼과 cfgfilt 응용 프로그램(필터 제어에 필요한)과의 통신이 가능하지 않습니다.

사용자 응답: 디렉토리 /etc/security가 위치하는 파일 시스템을 점검하십시오. 공간 부족 조건이 존재할 수 있습니다.

ICA1003 **로깅 디먼 초기화 계속.**

설명: fwlogd 디먼이 시작 프로세스를 계속합니다.

ICA1004 ***fwlogd*필터 로깅 디먼 (*version.release*레벨) 이 *date time*에 초기화되었습니다**

설명: IP 패킷 로깅 디먼이 시작되었습니다. 패킷 로깅이 사용 가능하면 디먼 fwlogd는 syslog, 로컬4, 파일로 필요한 레코드를 기록합니다.

ICA1005 **버퍼 오버플로우로 인하여 *filter_rule_no* 패킷 메세지 (들)를 로그할 수 없음**

설명: fwlogd 디먼 필터 로그 버퍼가 오버플로우되었습니다. 지정된 필터 규칙에 대한 패킷을 로그할 수 없습니다.

사용자 응답: 로그를 확인하십시오. Firewall이 서비스 거부 시스템 공격을 당하고 있거나 요구되지 않은 메세지를 기록하고 있는 것입니다. 예를 들어, 로그 작성을 방지하려면 브로드캐스트 메세지에 로그 제어 세트가 no(l=n)로 설정된 거부 규칙이 있어야 합니다.

ICA1006 **치명적 fwlogd 오류 - *failing function*: 오류 메세지**

설명: 표시된 함수 실행시 fwlogd 서버 실패, 디먼이 종료됩니다.

사용자 응답: 표시된 시스템 문제를 해결하고 fwlogd를 재시작하십시오.

ICA1007 **하위 프로세스를 분기할 수 없음: *errno***

설명: 필터 로깅 디몬 시동 중에 표시된 시스템 오류가 발생했습니다.

사용자 응답: 표시된 오류에 따라, 수정 조치를 취하십시오.

ICA1008 **setpgrp 루틴에서 오류 전송: *errno***

설명: 필터 로깅 디몬 시동 중에 표시된 시스템 오류가 발생했습니다.

ICA1009 **2번째 하위 프로세스를 분기할 수 없음: *errno***

설명: 필터 로깅 디몬 시동 중에 표시된 시스템 오류가 발생했습니다.

ICA1010 **이 디먼은 루트 권한으로 실행해야 함.**

설명: 필터 로깅 디몬은 루트 권한 레벨 하에서 시작되어야 합니다.

사용자 응답: 루트 권한 레벨을 사용하여 재시작하십시오.

ICA1011 **커널 확장자 *load_path*를 조회하기 위한 sysconfig 호출이 실패했음: *errno***

설명: 필터 로깅 디몬 시동 중에 표시된 시스템 오류가 발생했습니다.

ICA1012 **AIX 커널 확장 기능 *netinet*를 로드할 수 없음, 계속할 수 없음.**

설명: **netinet** 장치 드라이버가 필터 지원을 포함하지 않습니다.

사용자 응답: Firewall 코드를 설치하십시오. 잠재적으로, 코드가 설치되어 있을 수도 있지만 *재부팅*이 수행되지 않았습니다.

ICA1013 **Socket 작성 호출 실패: *errno***

설명: 필터 로깅 디몬 시동 중에 표시된 시스템 오류가 발생했습니다.

ICA1014 **AIX netinet 장치 드라이버가 필요한 레벨이 아님.**

설명: netinet 장치 드라이버 및 fwlogd 디먼이 같은 레벨이 아닙니다.

사용자 응답: 충돌을 해결하고 새로운 Firewall 레벨을 설치한 후에 재부팅하십시오.

ICA1015 **ioctl() 호출(SIOCGFWLOG) 오류: *errno***

설명: 필터 로깅 디몬 시동 중에 표시된 시스템 오류가 발생했습니다.

ICA1016 **현재 지연된 로그 대기행렬을 가져올 수 없음.**

설명: 추가 정보는 바로 이전 로그 메세지와 연관됩니다.

ICA1017 **SIOCGFWLOG ioctl() 호출에서 오류 전송.**

설명: 필터 로깅 디몬 시동 중에 표시된 시스템 오류가 발생했습니다.

ICA1018 **치명적 fwlogd 오류 - *failing function*: 시스템 오류 메세지**

설명: 표시된 함수 실행시 fwlogd 서버 실패, 디먼이 종료됩니다.

사용자 응답: 표시된 시스템 문제를 해결하고 fwlogd를 재시작하십시오.

ICA1019 **rc *internal_fw_return_code*로 인한 예기치 못한 오류 종료.**

설명: 필터 로깅 디몬 시동 중에 표시된 시스템 오류가 발생했습니다.

ICA1020 치명적 **fwlogd** 오류 - *failing function*: 리턴 코드 = **0x***function return code*

설명: 표시된 함수 실행시 fwlogd 서버 실패, 디먼이 종료됩니다.

사용자 응답: 표시된 시스템 문제를 해결하고 fwlogd를 재시작하십시오.

ICA1021 열기 오류 */dev/ipsp_poif*: *errno*

설명: 표시된 장치 드라이버가 설치되어 있지 않습니다.

사용자 응답: Firewall 코드가 설치되어 있는 경우, /tmp/rc/net.out 파일에서 가능한 오류 메세지를 확인하십시오.

ICA1022 필터 지원 검증이 실패했음.

설명: 이 메세지 이전에 기록된 오류로 인해 필터 지원을 확인할 수 없습니다.

ICA1023 **ioctl() 호출(SIOCGFWLVL) 오류:** *errno*

설명: 필터 로깅 디몬 시동 중에 표시된 시스템 오류가 발생했습니다.

사용자 응답: 다음 중 하나를 수행하십시오.

- AIX의 경우: 올바른 레벨의 Firewall netinet 디바이스 드라이버가 설치되어 있는지와 시스템이 설치 이후에 재부팅되었는지 확인하십시오.
- OS/390의 경우: 올바른 레벨의 TCP/IP가 설치되어 있는지와 **IPCONFIG FIREWALL** 구성 명령문과 함께 시작되었는지 확인하십시오.

ICA1024 파일 쓰기 오류 */etc/security/fwlogd.pid*: *errno*

설명: 표시된 시스템 errno으로 인하여, fwlogd가 지정된 파일에 쓸 수 없습니다.

사용자 응답: 표시된 문제점을 수정하고 필터 로깅 디몬을 재시작하십시오.

ICA1032 필터 규칙이 일(*date*) 시(*time*)에 갱신되었음.

설명: IP 패킷 필터링 규칙이 갱신되었습니다.

ICA1033 필터 지원 (*version.release*레벨)이 *date time*에 초기화되었습니다

설명: Firewall 필터 지원이 초기화되었습니다.

ICA1034 필터 지원이 일(*date*) 시(*time*)에 비활성화되었음.

설명: IP 패킷 필터링이 현재 /etc/security/fwfilters.cfg 파일에 정의된 필터 규칙이 아닌 디폴트 필터 규칙을 사용하고 있습니다.

ICA1035 패킷 로깅 상태가 일(*date*) 시(*time*)에 *enabled/disabled*로 설정되었음.

설명: 패킷 로깅 상태가 변경되었습니다. 메세지는 현재 상태를 시간 소인과 함께 표시합니다.

ICA1036 *#:rule_noR: rule_type direction: interface s:src_addr d: dst_addr p: protocol tag: scr_port/icmp_type tag: dst_port/icmp_code r:routed/local a: secure/non_secure f:yes/no T:tunnel_id e:C/D/n l:packet_length*

설명: 처리된 IP 패킷과 이와 일치하는 해당 필터 규칙을 알리는 레코드를 기록하십시오. 이 레코드가 기록되면, 일치되는 필터 규칙에서는 로그 제어가 *yes*로 설정되어야 합니다. 이러한 규칙에 맞는 IP 패킷이 한 부분이면, ports/icmp type/code 정보는 헤더 패킷에 대해 표시되지만, 헤더 패킷외의 패킷의 경우에는 0으로 표시됩니다.

ICA1037 *#:rule_no action src_addr src_mask dst_addr dst_mask protocol logical_op value logical_op value interface_type routing directionl= log_control f=fragment_controlt= tunnel_ID enc_alg auth_alg*

설명: 필터 규칙이 갱신되면, 활성화된 규칙이 로그에 기록됩니다. 이 로그 메세지는 활성화된 규칙 중 하나를 설명합니다.

ICA1038 세션 키 엔진이 시작되었으며, 세션 **socket** 포트: *port_no* 및 마스터 **socket** 포트:*port_no*를 사용함.

설명: /etc/services에 정의된 대로, 지정된 UDP 포트 번호를 사용하는 암호화 터널이 시작되었습니다.

ICA1039 **규정이 다음과 같이 (재)정의됨.**

설명: 파일 /etc/security/fwpolicy를 사용하여 규정 캐쉬가 (재)정의됩니다. 다음의 행은 새로운 규정 캐쉬를 보여줍니다.

ICA1040 **>Policy문:** *tunnel_origin tunnel_end tunnel_ID encrypt_flag/authenticate_flag*

설명: 로그된 행이 /etc/security/fwpolicy 파일에서 읽혀졌습니다.

ICA1041 **콘텍스트 사양이 터널:** *tunnel_ID***에 대하여 삭제되었음.**

설명: 나열된 ID에 대한 터널 콘텍스트가 더이상 작동가능하지 않습니다.

ICA1042 **다음과 같은 터널 콘텍스트 사양(들)이 정의됨.**

설명: 다음 로그 레코드에 나열된 것처럼, 터널 콘텍스트 사양이 정의됩니다.

ICA1043 **>tunnel_ID:***number***, src_addr:***IP_address***, dst_addr:***IP_address***, 암호화:***algorithm*

설명: 메세지는 활성화된 터널 콘텍스트의 특정 속성을 나열합니다.

ICA1044 **호스트 카운터 경고: IP(***IP Address***) 한계 초과.**

설명: Firewall 시스템과 연결하기 위한 보안 호스트 시도가 너무 많습니다.

시스템 조치: 연결 통과

ICA1045 **TCP 한계 초과:** *IP Address*(*Port*)**->***IP Address*(*Port*)**이(가) 거부되었습니다**

설명: Firewall 시스템에 TCP 세션이 너무 많습니다.

시스템 조치: 연결 거부

ICA1046 **UDP 한계 초과:** *IP Address*(*Port*)**->***IP Address*(*Port*)**가 거부되었습니다.**

설명: Firewall 시스템에 UDP 세션이 너무 많습니다.

시스템 조치: 연결 거부

ICA1047 **그레이스 기간 경고 : TCP 세션이 너무 많습니다.** *IP Address*(*Port*)**->***IP Address*(*Port*)**이(가) 통과되었습니다**

설명: Firewall 시스템에 TCP 세션이 너무 많습니다.

시스템 조치: 연결 통과

ICA1048 **Grace Period 경고 : UDP 세션이 너무 많습니다.** *IP Address*(*Port*)**->***IP Address*(*Port*)**이(가) 통과되었습니다**

설명: Firewall 시스템에 UDP 세션이 너무 많습니다.

ICA1049 **유효하지 않은 ipsec 패키지: s:***IP Address* **d:***IP Address* **프로토콜:***Protocol* **spi:***Security Parameters Index*

설명: Firewall을 수신함으로써 IPSec 패키지의 캡슐화를 해제할 수 없습니다.

사용자 응답: 터널 정의가 제대로 반출되었는지와 각 Firewall에서 활성화되었는지 확인하십시오.

ICA1050 *tunnel_ID***터널에 대한 사양이 삭제되었습니다.**

설명: 나열된 ID에 대한 터널 사양이 더 이상 작동가능하지 않습니다.

ICA1051 **다음 터널 사양(들)이 정의됩니다.**

설명: 터널 사양은 다음 로그 레코드에 나열된 것처럼 정의됩니다.

ICA1052 **>tunnel_ID:***number***, src_addr:***IP_address***, dst_addr:***IP_address***, src_enc:***algorithm* **rem_enc:***algorithm* **src_mac:***algorithm* **rem_mac:***algorithm* **src_enc_mac:***algorithm* **rem_enc_mac:***algorithm* **src_pol:***policy* **rem_pol:***policy* **mode:***transport_mode*

설명: 메세지는 활성화된 터널의 고유 속성을 나열합니다.

ICA1200 **위의 오류로 인한 로깅 디먼 종료.**

설명: 이 메세지 이전에 기록된 오류로 인하여, fwlogd 디먼을 종료합니다.

시스템 조치: IP 필터 로깅이 활성화되지 않습니다.

사용자 응답: 표시된 오류를 수정하고 fwlogd를 재시작하십시오.

ICA1260 *termination* **신호를 수신했으므로 일(***date***) 시 (***time***)에 필터 로깅 디먼을 종료함.**

설명: fwlogd 디먼이 표시된 종료 신호를 수신했으며 중단됩니다.

ICA1305 **\″알 수 없음[″]**

설명: syslog에 대한 IP 패킷 포맷시, 알 수 없는 프로토콜 사양을 가진 레코드를 발견했습니다. 프로토콜 IP, ICMP, TCP, UDP 및 IPSP는 인식되는 프로토콜입니다. IPSP는 터널을 통하여 전달되는 암호화된 패킷에 대한 IBM 설계입니다.

ICA1400 **치명적 fwtimernat 오류 -** *failing function***:** *system error message*

설명: fwtimernat 서버는 표시된 기능에서 실패했습니다. fwtimernat 서버는 중단됩니다.

사용자 응답: 표시된 시스템 문제를 해결하고 fwtimernat를 재시작하십시오.

ICA1401 **치명적 fwtimernat 오류 -** *failing function***: 리턴 코드 = 0x***function return code*

설명: fwtimernat 서버는 표시된 기능에서 실패했습니다. fwtimernat 서버는 중단됩니다.

사용자 응답: 표시된 시스템 문제를 해결하고 fwtimernat를 재시작하십시오.

ICA1402 **치명적 fwtimernat 오류 -** *failing function***:** *error message*

설명: fwtimernat 서버는 표시된 기능에서 실패했습니다. fwtimernat 서버는 중단됩니다.

사용자 응답: 표시된 시스템 문제를 해결하고 fwtimernat를 재시작하십시오.

ICA2000 *IP_address***로부터** *IP_address***로의 새로운 FTP 세션(비보안 사이트).**

설명: 비보안 사이트로부터 새로운 ftp 세션을 시작합니다.

ICA2001 *net ftp***:***IP_address***로부터 사용자** *name***(알 수 없음)에 대한 사용자 확인에 실패했음.**

설명: 계정이 없는 사용자가 네트워크에서 FTP 프록시를 사용하려 했습니다.

사용자 응답: 프록시 계정을 설정하려면 Firewall 관리자를 참조하십시오.

ICA2002 *network***:***host name***에서** *authentication***을(를) 사용하여 사용자** *name***을(를) 확인하는데 실패했습니다.**

설명: Firewall에서 지정된 사용자 확인 방법을 사용하여 표시된 사용자 이름을 확인할 수 없습니다.

사용자 응답: Firewall 관리자를 참조하십시오.

ICA2003 *user name***에 대해 구성된 쉘이 없습니다.**

설명: 식별된 사용자가 프록시 로그인을 시도했지만 정의된 로그인 쉘이 없습니다.

사용자 응답: 해당 사용자 로그인 프로파일을 수정하려면 Firewall 관리자를 참조하십시오.

ICA2004 **0x***hex_value***에서 알 수 없는 감사 이벤트를 수신했습니다.**

설명: 모듈 tcpip_audit.c에서 알 수 없는 감사 요청을 수신했습니다.

ICA2005 **클라이언트에 쓰기 오류:** *errno*.

설명: 클라이언트와 통신할 수 없습니다. 기록된 시스템 메세지를 참고하십시오.

ICA2006 **ptelnetd: auditproc:** *errno*.

설명: 텔넷 감사 프로세스에서 표시된 오류를 전송했음. 시스템 파일이 손상되었을 수 있습니다.

ICA2007 **ptelnetd: 패닉 단계=***value*.

설명: 알 수 없는 오류가 감지되었습니다. 시스템 파일이 손상되었을 수 있습니다.

ICA2008 *IP_address*에서 비-**Firewall** 사용자 *name* 이(가) 텔넷에 들어왔습니다.

설명: Firewall 계정이 없는 사용자가 텔넷 프록시를 사용하려고 시도했습니다.

시스템 조치: 총칭 확인을 사용한다고 가정하십시오.

ICA2009 **/bin/login:** *errno*.

설명: 시스템 로그인 중에 치명적인 오류가 발생했습니다. 표시된 시스템 오류 메세지를 참조하십시오.

ICA2010 *IP_address*(비보안)에서 *IP_address*로 연결합니다.

설명: 비보안 인터페이스를 통한 표시된 IP 주소간 연결 성공.

ICA2011 *IP_address*(보안)에서 *IP_address*로 연결합니다.

설명: 보안 인터페이스를 통한 표시된 IP 주소간 연결 성공.

ICA2012 *IP_address*로부터 *IP_address*로의 새로운 **FTP** 세션(보안 사이트).

설명: 새로운 FTP 세션을 시작함.

ICA2013 *IP_address*에서 *IP_address*로 새로운 텔넷 세션.

설명: 새로운 텔넷 세션이 설정되었습니다.

ICA2014 옵션 *value*이(가) 지원되지 않습니다.

설명: 표시된 플래그가 지원되지 않음, 이전 메세지를 참조하십시오.

ICA2015 옵션 -*value*이(가) 지원되지 않습니다.

설명: 표시된 플래그가 지원되지 않음, 이전 메세지를 참조하십시오.

ICA2016 리모트 사용자 **ID** \"*name*\".

설명: 표시된 사용자에 대한 ftp 연결 요청.

ICA2017 - *in line*을 디버그합니다.

ICA2018 사용자 *name*에 대한 **SNK** 키를 찾을 수 없음.

설명: 표시된 user_ID에 대한 SecureNetKey 값을 찾을 수 없습니다.

사용자 응답: 가능한 로그인 구성 문제에 대하여 Firewall 관리자를 참조하십시오.

ICA2019 사용자 *name*에 대해 **SNK** 키를 제대로 읽을 수 없음.

설명: 표시된 user_ID에 대하여 8진수로 SecureNetKey 값을 읽을 수 없습니다.

사용자 응답: 가능한 로그인 구성 문제에 대하여 Firewall 관리자를 참조하십시오.

ICA2020 **/usr/bin/fwuserau** 또는 **/usr/bin/fwuserpt**가 없음.

설명: 사용자 제공 사용자 확인 방법을 사용한 사용자 확인이 취소되었습니다.

시스템 조치: 사용자 확인이 취소되었습니다.

사용자 응답: /usr/bin/fwuserau 및 /usr/bin/fwuserpt가 존재하는지와 소유자가 루트인지 확인하십시오. 이 실행 파일이 없으면 사용자는 Firewall의 운영 체계와 호환될 수 있는 컴파일러를 사용하여 실행 파일을 만들고 /usr/bin/fwuserau나 /usr/bin/fwuserpt로 명명하십시오.

ICA2021 사용자 **id** *name*을 사용하여 원격 호스트 *name*에 연결 시도 중.

설명: 새로운 FTP 연결 설정이 시도 중입니다.

ICA2022 원격 호스트 *name*에 연결 시도 중.

설명: 새로운 FTP 연결 설정이 시도 중입니다.

ICA2023 사용법: **ptelnetd ns**

설명: ptelnet 디먼 시작시 알 수 없는 플래그가 지정되었습니다.

사용자 응답: 플래그 -n 및/또는 -s만을 사용하십시오.

ICA2024 *network*:*host name*에서 *method*확인 방법을 사용하여 사용자 *name*을(를) 성공적으로 확인하였습니다.

설명: FW에서 지정된 사용자 확인 방법을 사용하여 표시된 사용자 이름을 확인했습니다.

ICA2025 *network*:*host name*에서 *method*확인 방법을 사용하여 사용자 *name*이(가) 로그인되었습니다.

설명: FTP 사용자가 로그인되었습니다.

ICA2026 *current time*의 *n* 초 후에 사용자 *name*이 시간종료되었습니다.

설명: 지정된 사용자에 대한 연결 시도가 시간종료되었습니다. 네트워크 경로지정 문제가 발생했거나 원격 호스트가 사용 가능하지 않은 것입니다.

ICA2027 *time*에 *원격* 호스트 연결.

설명: Firewall으로의 Net ftp 연결이 설정되었습니다.

ICA2028 *IP_address*로부터 *IP_address*로의 FTP 연결 시도가 거부되었습니다. 이 시스템은 비보안 사이트로부터 FTP를 지원하지 않음.

설명: 일반적으로 비보안 인터페이스를 통하여 Firewall에 연결을 설정하려는 시도를 나타냅니다.

시스템 조치: 연결 거부.

ICA2029 행 *line에서* errno = -로 시스템 오류.

설명: 시스템 호출을 실행하는 중 문제가 발생했습니다.

시스템 조치: 시스템 실행이 정지됨

사용자 응답: 로그를 표시하고 errno의 의미를 이해한 다음 문제를 해결해 보십시오. 해결할 수 없는 경우, IBM 서비스에 문의하십시오.

ICA2030 행 *line에서* 리턴 코드 = -로 함수 호출.

설명: 함수 호출에 문제가 발생했습니다.

시스템 조치: 오류 전송

사용자 응답: 로그를 열람하여, 리턴 코드의 의미를 이해한 다음 문제 해결을 다시 시도하십시오. 해결할 수 없는 경우, IBM 서비스에 문의하십시오.

ICA2031 sdi 함수 호출 creadcfg() rc = -.

설명: 함수 호출에 문제가 발생했습니다.

시스템 조치: 오류 전송

사용자 응답: sdi 참조서에서 설명을 찾아 보십시오.

ICA2032 연결 손실.

설명: ftp 연결이 손실되었습니다.

사용자 응답: 세션을 재설정하십시오.

ICA2033 sdi 함수 호출 sd_init rc = -.

설명: 함수 호출에 문제가 발생했습니다.

시스템 조치: 오류 전송

사용자 응답: sdi 참조서에서 설명을 찾아 보십시오.

ICA2034 sdi 함수 호출 sd_check rc = -.

설명: 함수 호출에 문제가 발생했습니다.

시스템 조치: 오류 전송

사용자 응답: sdi 참조서에서 설명을 찾아 보십시오.

ICA2035 setsockopt(): *errno*.

설명: setsocketopt 호출시 시스템 오류 발생했습니다.

ICA2036 *session id* 텔넷 세션이 사용자 *user id*용으로 시작되었습니다. (*source IP addr*:*dest IP addr*).

설명: 메세지는 각각의 텔넷 세션을 시작할 때 생성됩니다. 사용자 ID, 출발지 ip 및 목적지 ip가 모두 Firewall에 잘 알려진 경우 세션이 시작됩니다. 세션 id는 Firewall에서 생성하는 고유한 식별자입니다.

ICA2037 사용자 fwdfuser 또는 fwdpuser가 로그인을 시도하지만, 허용되지 않음.

설명: fwdfuser 및 fwdpuser는 예약된 사용자이며 사용할 수 없습니다.

시스템 조치: 로그인이 거부되었습니다.

사용자 응답: 관리자는 해당 계정을 사용 중인 사용자를 조사해야 합니다.

ICA2038 **ttloop: 피어가 중단됨: *errno*.**

설명: 네트워크 출력 버퍼를 채우는 동안 오류가 발생했습니다. 피어 프로세스가 중단된 것을 나타냅니다.

ICA2039 **ttloop: 읽기: *errno*.**

설명: 네트워크 출력 버퍼를 채우는 동안 오류가 발생했습니다.

ICA2040 **암호에 대한 사용자 확인이 설정됨, 사용자 ID fwdfuser에 대해 none 또는 snk는 허용되지 않음.**

설명: fwdfuser는 예약된 사용자 ID이므로 사용자 확인 방법으로 암호나 none을 사용할 수 없습니다.

시스템 조치: 로그인이 거부되었습니다.

사용자 응답: 관리자가 사용자 ID fwdfuser에 대한 사용자 확인 방법을 변경해야 합니다.

ICA2041 ***session id* FTP 세션이 *user id*용으로 시작되었습니다(*source IP addr*:*dest IP addr*).**

설명: 메세지는 각각의 FTP 세션을 시작할 때 생성됩니다. 사용자 ID, 출발지 ip 및 목적지 ip가 모두 Firewall에 잘 알려진 경우 세션이 시작됩니다. 세션 id는 Firewall에서 생성하는 고유한 식별자입니다.

ICA2042 **req_rsp_code가 FW_AUTH_REQ로 잘못 설정되었음.**

설명: fw_tn_authenticate가 req_rsp_code를 FW_AUTH_REQ로 설정할 수 없습니다.

시스템 조치: 사용자 확인을 취소합니다.

사용자 응답: fw_tn_authenticate를 변경하고, 라이브러리 fwuser.o를 다시 만든 다음, Firewall에 저장하십시오.

ICA2043 ***user_name*에 대한 암호를 얻을 수 없음.**

설명: 해당 사용자에 대한 사용자 확인 유형이 '암호'이며 암호를 찾을 수 없습니다.

사용자 응답: Firewall 관리자를 참조하십시오.

ICA2044 **-t에 대하여 지정된 시간(*value*)이 잘못되었음.**

설명: 나타나는 시간값에 숫자 범위 0..9를 벗어나는 문자가 들어 있거나 허용되는 최대값을 초과합니다.

ICA2045 **옵션 -T가 Firewall에서 지원되지 않음.**

설명: 표시된 옵션이 지원되지 않습니다.

ICA2046 **옵션 -k가 Firewall에서 지원되지 않음.**

설명: 표시된 옵션이 지원되지 않습니다.

ICA2047 **옵션 -s가 Firewall에서 지원되지 않음.**

설명: 표시된 옵션이 지원되지 않습니다.

ICA2048 **옵션 -u가 Firewall에서 지원되지 않음.**

설명: 표시된 옵션이 지원되지 않습니다.

ICA2049 **알 수 없는 플래그 -*value*가 무시됩니다.**

설명: 표시된 플래그가 지정되었으나 인식되지 않습니다.

ICA2050 **알 수 없는 매개변수 *value*.**

설명: 옵션으로 지정된, 표시된 값이 인식되지 않습니다.

ICA2051 **주소의 adapt_addr 변환 오류.**

설명: 표시된 IP 주소가 유효하지 않습니다.

사용자 응답: 파일 /etc/security/fwsecadpt.cfg가 손상되었을 수 있습니다. 파일을 삭제하고 보안 인터페이스를 재구성하고 필터를 재초기화하십시오.

ICA2052 **afopen이 /etc/security/login.cfg를 열 수 없음: *errno*.**

설명: 사용자를 확인할 수 없음, 표시된 파일에 대한 열기 오류임.

ICA2053 보안 인터페이스 파일을 열 수 없음.

설명: 보안 인터페이스가 구성되지 않았습니다.

사용자 응답: 보안 인터페이스가 정의되어야 하는 경우 Firewall 명령/smit 패널을 사용하여 보안 인터페이스를 정의하십시오.

ICA2054 enduserdb rc=*value, errno*.

설명: 사용자 로그인 프로파일 정보를 검색하려는 중 표시된 시스템 오류 코드가 수신되었습니다.

사용자 응답: 로그인 계정을 검증하려면 Firewall 관리자를 참조하십시오.

ICA2055 getpeername() (*invocation name*): *errno*.

설명: FTP 디먼이 socket 이름을 찾으려는 중 시스템 오류 발생.

ICA2056 getsockname() (*invocation name*): *errno*.

설명: FTP 디먼이 포트 이름을 찾으려는 중 시스템 오류 발생.

ICA2057 getuser 비보안 쉘 *user_ID*용 rc=*user_ID, errno*.

설명: Firewall의 비보안 부분으로부터 연결에 대한 쉘 이름을 검색하려는 중 표시된 시스템 오류 코드가 수신되었습니다.

사용자 응답: 사용자 로그인 프로파일에 대하여 쉘을 설정하려면 Firewall 관리자를 참조하십시오.

ICA2058 getuser 보안 쉘 *user_ID*용 rc=*user_ID, errno*.

설명: Firewall의 보안 부분으로부터 연결에 대한 쉘 이름을 검색하려는 중 표시된 시스템 오류 코드가 수신되었습니다.

사용자 응답: Firewall 관리자에게 문의하여 사용자 로그인 프로파일에 대한 쉘을 알아보십시오.

ICA2059 ioctl(): *errno*

설명: SIOCSPGRP에 대한 ioctl() 호출에서 시스템 오류.

ICA2060 ptelnetd: 공유 메모리에 대한 ftok 실패.

설명: 공유 메모리 세그먼트를 할당할 수 없습니다.

사용자 응답: Firewall 관리자에게 문의하십시오. 명백한 메모리 문제점입니다.

ICA2061 ptelnetd: 공유 메모리에 대한 shmat 실패.

설명: 공유 메모리 세그먼트를 할당할 수 없습니다.

사용자 응답: Firewall 관리자에게 문의하십시오. 명백한 메모리 문제점입니다.

ICA2062 ptelnetd: 공유 메모리에 대한 shmget 실패.

설명: 공유 메모리 세그먼트를 할당할 수 없습니다.

사용자 응답: Firewall 관리자에게 문의하십시오. 명백한 메모리 문제점입니다.

ICA2063 setsockopt()(SO_DEBUG): *errno*.

설명: 시스템 호출 'setsockopt'에 표시된 오류 메세지가 전송되었습니다.

ICA2064 setsockopt()(SO_KEEPALIVE): *errno*.

설명: 시스템 호출 'setsockopt'에 표시된 오류 메세지가 전송되었습니다.

ICA2065 setuser rc=*value, errno*.

설명: 표시된 이유로 시스템 호출에 잘못된 리턴 코드가 수신되었습니다.

ICA2066 신호(): *errno*.

설명: FTP 디먼이 신호 처리기를 설정하려는 중 시스템 오류 발생.

ICA2067 치명적 pftpd 초기화 오류 - bind(): *errno*

설명: pftpd 서버 초기화가 실패함, 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 해결하고 pftpd를 재시작하십시오. 이 오류의 가장 일반적인 원인은 표준 FTP 포트(21)와의 연결을 대기하고 있는 또 다른 FTP 디먼이 있다는 것입니다.

ICA2068 **치명적 pftpd 초기화 오류 - listen(): *errno***

설명: pftpd 서버 초기화가 실패함, 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 해결하고 pftpd를 재시작하십시오.

ICA2069 **치명적 pftpd 오류 - main accept(): *errno***

설명: pftpd 서버 기본 루틴이 실패함, 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 해결하고 pftpd를 재시작하십시오.

ICA2070 **치명적 pftpd 초기화 오류 - socket(): *errno***

설명: pftpd 서버 초기화가 실패함, 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 해결하고 pftpd를 재시작하십시오.

ICA2071 **연결이 거절되었습니다. 연결의 최대 수에 도달했습니다.**

설명: 세션의 최대 수가 이미 존재하기 때문에 pftpd 서버가 다른 FTP 세션을 작성할 수 없습니다.

시스템 조치: 연결이 거절되었습니다.

사용자 응답: 기존 연결이 종료될 때까지 기다린 후 요청을 다시 시도하십시오.

ICA2072 **ftp 구성 파일(*filename*)이 사용 가능하지 않음.**

설명: ftp 디먼이 지정한 FTP 구성 파일을 열려했으나 존재하지 않거나 열 수 없습니다.

시스템 조치: ftp 디먼 프로세싱에서 디폴트 구성이 사용됩니다.

사용자 응답: 파일이 존재해야 하는 경우, 파일을 작성하거나 메세지에 지정된 위치로 이동해야 합니다.

ICA2073 **FTP 언어표에 대한 기억영역을 확보할 수 없음.**

설명: FTP 구성 파일의 REPLYLANGUAGE 명령문을 표시하는데 필요한 기억영역을 확보할 수 없습니다.

시스템 조치: 처리가 계속됩니다.

사용자 응답: 영역 크기를 증가시키거나 구성 파일의 항목을 감소시키십시오.

ICA2074 **FTP config 명령문에 대한 프로세싱이 완료됨: *configuration statement***

설명: ftp에서 표시된 구성 명령문을 처리했습니다.

시스템 조치: 처리가 계속됩니다.

사용자 응답: 없음

ICA2075 ***user id*용 FTP (*source IP addr*:*dest IP addr*), *operation file name*, *numbytes* 바이트. sid: *session id.***

설명: FTP 세션을 열 때 각각의 파일 전송에 대하여 메세지가 생성됩니다. sid는 세션 시작시 Firewall에서 생성하는 고유한 식별자입니다.

ICA2076 ***session id* FTP 세션이 *user id*용으로 종료되었습니다 (*source IP address*:*dest IP addr*). *duration* 초, *numbytes* 바이트.**

설명: 각 FTP 디먼의 끝에서 메세지가 생성되었습니다. sid는 세션 시작시 Firewall에서 생성하는 고유한 식별자입니다.

ICA2077 ***session id* 텔넷 세션이 *user id*용으로 종료되었습니다 (*source IP address*:*dest IP addr*). *numbytes* 바이트.**

설명: 메세지가 각각의 텔넷 세션이 끝날 때 생성됩니다. sid는 세션 시작시 Firewall에서 생성하는 고유한 식별자입니다.

ICA2078 **프록시 사용자 *user*가 단절되었음 - 시 (*time*)분동안 유휴 상태.**

설명: 사용자 세션이 최대 허용 유휴 시간을 초과했습니다.

ICA2079 **주의 - *IP_address*로부터 *IP_address*로의 확인되지 않은 연결 시도.**

설명: 일반적으로 비보안 인터페이스를 통하여 Firewall에 연결을 설정하려는 시도를 나타냅니다.

시스템 조치: 연결 거부.

ICA2080 **FTP 구성 파일 행 *line*의 컬럼 *column* 부분에서 구문 오류(*reason*) 발생: *configuration statement***

설명: 제공된 행의 ftp 구성 명령문에 오류가 있습니다. 오류의 원인과 오류가 감지된 위치가 제공됩니다.

시스템 조치: 명령문이 무시됩니다.

사용자 응답: FTP 구성 파일에서 명령문을 수정하십시오.

ICA2081 **FTP 구성 명령문이 제공하는 메세지 카탈로그는 모두 사용할 수 없음.**

설명: REPLYLANGUAGE ftp 구성 명령문이 제공하는 메세지 카탈로그를 열지 못했습니다. 클라이언트 메세지 카탈로그를 사용할 수 없습니다.

시스템 조치: 클라이언트 메세지 카탈로그가 C 디렉토리에서 영어로 시행됩니다.

사용자 응답: FTP 구성 REPLYLANGUAGE 명령문의 언어 디렉토리와 관련된 각 디렉토리에 카탈로그 파일이 있는지 확인하십시오. 또한 NLSPATH 환경 변수가 LANG 환경 변수(%L) 및 카탈로그명(%N)의 서브디렉토리를 모두 대체할 수 있도록 올바로 설정되었는지 확인하십시오.

ICA2082 **ftp LANG 환경 변수를 *sub-directory*로 설정할 수 없음. 이유: *reason***

설명: FTP 디먼이 LANG 환경 변수를 지정된 서브디렉토리로 변경하려는 중 시스템 오류가 발생했습니다.

시스템 조치: 처리가 계속됩니다. 복구시 다른 메세지를 생성할 수도 있습니다.

사용자 응답: 제공된 원인을 사용하여 이것이 시스템 오류인지 또는 프로그래밍 오류인지 여부를 결정하십시오.

ICA2083 **디렉토리의 FTP 클라이언트 메세지 카탈로그를 열 수 없음: *sub-directory*, 이유: *reason***

설명: ftp 디먼이 제공된 서브디렉토리에 있는 메세지 카탈로그를 열 수 없습니다. 제공된 원인은 catopen()에서 전송된 errno입니다.

시스템 조치: 처리가 계속됩니다. 복구시 다른 메세지를 생성할 수도 있습니다.

사용자 응답: 제공된 언어 디렉토리와 관련된 디렉토리에 카탈로그가 있는지 확인하십시오. NLSPATH 환경 변수가 LANG 환경 변수 (%L) 및 카탈로그명(%N)의 서브디렉토리를 모두 대체할 수 있도록 올바로 설정되었는지 확인하십시오.

ICA2084 **C 서브디렉토리를 통하여 ftp 클라이언트 메세지 카탈로그가 영어로 실행됨.**

설명: 앞서 나열된 오류로 인해 ftp 디먼이 C 서브디렉토리를 사용하여 클라이언트 메세지 카탈로그를 영어로 실행했습니다.

시스템 조치: 언어를 C 메세지 카탈로그로 시행할 수 있는 경우 처리를 계속합니다. 시행할 수 없는 경우, 프로그램이 종료됩니다.

사용자 응답: 이전 메세지에서 오류를 수정하십시오. 프로그램이 또한 존재하는 경우, C 서브디렉토리에 메세지 카탈로그를 작성하고 NLSPATH 환경 변수를 올바로 설정하십시오.

ICA2085 ***Process id* pid용으로 텔넷 세션이 종료되었습니다. (*source IP address*).**

설명: 메세지가 각각의 텔넷 세션이 끝날 때 생성됩니다.

ICA2086 **사용자 파일이 잘못 구성되었음; 키 *key*가 없는 사용자 *user*).**

설명: ftpd가 사용자 파일에서 요청된 사용자를 찾았으나 키를 찾을 수 없습니다. 사용자 파일이 잘못 구성되어 있습니다.

사용자 응답: 이러한 문제를 해결하려면 Firewall 명령/smit 패널을 사용하십시오.

ICA2087 **ftpd가 사용자 구성 파일에서 사용자 *user*를 찾을 수 없음.**

설명: 지정된 사용자명이 구성되지 않았거나 user.cfg 파일이 손상되었습니다.

사용자 응답: 이러한 문제를 해결하려면 Firewall 명령/smit 패널을 사용하십시오.

ICA2088 **ftpd가 사용자 구성 파일을 열 수 없음.**

설명: ftpd가 사용자 구성 파일을 열 수 없으므로 fopen에 대하여 수행한 호출이 실패했습니다.

사용자 응답: 사용자 구성 파일(기본적으로 user.cfg)이 사용가능한지 확인하십시오; Firewall 명령/smit 패널을 사용하십시오.

ICA2089 **사용자 파일의 사용자 권한 유형(*Authorization type*)이 테이블 (struct tab2 authtab)의 어떠한 항목과도 일치하지 않습니다.**

설명: 지정된 사용자의 사용자 확인 유형(user.cfg에서 전송된)이 지원되는 유형(거부,없음,snk,sdi,암호 등과 같은)과 일치하지 않습니다.

사용자 응답: user.cfg 파일 무결성 또는 구성을 확인하십시오; 이러한 문제를 해결하려면 Firewall 명령/smit 패널을 사용하십시오.

ICA2090 **user.cfg 파일의 KEY=DENY로 인하여 사용자 *user name*'에 대한 *client ip*로부터의 확인에 실패했음.**

설명: Firewall 관리자가 설정한 user.cfg 파일 사양으로 인하여 사용자 확인에 실패했습니다.

사용자 응답: Firewall 관리자를 참조하십시오.

ICA2091 **사용자의 '*user name*'이 비보안 포트(*Firewall ip*)로의 ftp를 허용하지 않음.**

설명: 사용자가 비보안 포트(nsp)를 통해 Firewall 서버로 ftp를 시도했음 - 모든 nsp 사용자에게 유효한 권한 유형으로 적절히 구성된 'fwnsftp' 키가 있어야 합니다(user.cfg 파일에).

사용자 응답: user.cfg 파일 무결성 또는 구성을 확인하십시오; 이러한 문제를 해결하려면 Firewall 명령/smit 패널을 사용하십시오.

ICA2092 **내부 오류: nt_gwauth() 실패.**

설명: nt_gwauth()는 보통 세 값(AUTHENTICATED, NOT_AUTHENTICATED 또는 DENY) 중 하나를 리턴하는데 이 경우에 nt_gwauth가 유효하지 않은 일부 정수를 리턴했음.

ICA2093 **'*user name*'사용자는 보안 포트(*port number*)에 ftp하도록 허락되지 않았습니다.**

설명: 사용자가 보안 포트(sp)를 통해 Firewall 서버로 ftp를 시도했음 - 모든 sp 사용자에게 유효한 권한 유형으로 적절히 구성된 'fwsftp' 키가 있어야 합니다(user.cfg 파일에).

사용자 응답: user.cfg 파일 무결성 또는 구성을 확인하십시오; 이러한 문제를 해결하려면 Firewall 명령/smit 패널을 사용하십시오.

ICA2094 **로그인 실패: 예상한 형식: "USER <*user name*> 다음 "PASS <암호>"; *invalid cmd*를 수신했음.**

설명: FTP 클라이언트가 예상된 형식(PASS 'password' per RFC959)을 전송하지 못했으므로 사용자 확인에 실패했습니다.

사용자 응답: "user <username>"을 입력하십시오; 정확한 암호를 입력하십시오. Firewall 관리자를 참조하십시오.

ICA2095 **로그인 실패: (사용자 *auth method* 방법을 통한) 사용자 '*user name*'의 *client ip*(클라이언트 사이트)로부터의 확인에 실패했음.**

설명: 잘못된 입력(지정된 사용자 확인 유형에 대하여 클라이언트에 의한)으로 인하여 사용자 확인이 실패했음 - 사용자가 입력한 잘못된 암호, snk 키 등.

사용자 응답: Firewall 관리자를 참조하십시오.

ICA2096 **사용자 확인: (사용자 *auth method* 방법을 통한) 사용자 '*user name*'의 *client ip*(클라이언트 사이트)로부터의 사용자 확인이 성공했음.**

설명: 사용자 확인을 성공했습니다.

ICA2097 **httpd --> HTTP 프록시 서버 버전 *HTTP Proxy Version* 시작 중.**

설명: WWW 액세스를 위한 HTTP 프록시 시작 중입니다.

ICA2098 **httpd --> HTTP 프록시 서버 종료 중.**

설명: WWW 액세스를 위한 HTTP 프록시 종료 중입니다.

ICA2099 **httpd --> 상태: <*HTTP Status code*> 고객 발신 <*IP address*>, 요청자 <\"*HTTP GET request*\"> <*number of bytes*> 바이트용.**

설명: 프록시를 통한 일부 파일에 대한 클라이언트 HTTP 요청 상태. "상태" 코드값에 대한 자세한 내용은 ds.internic.net을 포함하여 인터넷의 다양한 사이트에서 사용할 수 있는 HTTP 1.0(RFC 1945) 또는 HTTP 1.1(RFC 2068) 문서(또는 RFC)를 참고하십시오.

ICA2100 **Socket 주소가 0과 같음.**

설명: 로컬 요청에서 잘못된 목적지 주소가 발견되었습니다.

ICA2101 **Socket 주소 계열 오류: *sin_family_type*.**

설명: 로컬 요청에서 잘못된 주소 계열 유형이 발견되었습니다.

ICA2102 **odm 초기화 오류: *odmerrno*.**

설명: ODM(오브젝트 데이터 관리자)에 대하여 odm_initialize() 오류가 발생했습니다.

ICA2103 **odm 디폴트 경로 설정 오류: *odmerrno*.**

설명: ODM(오브젝트 데이터 관리자)에 대하여 odm_set_path() 오류가 발생했음. 오브젝트 클래스, OCSvhost.

ICA2104 **odm 데이터베이스 잠금 오류: *odmerrno*.**

설명: ODM(오브젝트 데이터 관리자)에 대한 odm_lock() 오류가 발생했습니다.

ICA2105 **odm 오브젝트 열기 오류 *Customized_Attribute*: *odmerrno*.**

설명: ODM(오브젝트 데이터 관리자)에 대하여 odm_open_class() 오류가 발생하였습니다.

ICA2106 **odm object 찾기 오류 *OCS_virtual_host*: *odmerrno*.**

설명: ODM(오브젝트 데이터 관리자)에 대하여 odm_get_first() 오류가 발생했습니다. 오브젝트 클래스, OCSvhost.

ICA2107 **odm object 닫기 오류 *OCS_virtual_host*: *odmerrno*.**

설명: ODM(오브젝트 데이터 관리자)에 대하여 odm_close_class() 오류가 발생하였습니다. 오브젝트 클래스, OCSvhost.

ICA2108 **odm 데이터베이스 잠금 해제 오류: *odmerrno*.**

설명: ODM(오브젝트 데이터 관리자)에 대하여 odm_unlock() 오류가 발생했습니다.

ICA2109 **odm 종료 오류: *odmerrno*.**

설명: ODM(오브젝트 데이터 관리자)에 대하여 odm_terminate() 오류가 발생했습니다.

ICA2110 **이름별 서버 확보 오류: *errno*.**

설명: getservbyname() 오류가 발생했습니다. 호스트 로그인 모니터 서비스, lm이 /etc/services 파일에 제대로 지정되어 있지 않습니다.

ICA2111 **byname() 오류: *errno*.**

설명: gethostbyname() 오류가 발생했습니다. 호스트 시스템 이름이 /etc/hosts에 제대로 지정되어 있지 않습니다.

ICA2112 **잘못된 프로토콜 이름: *protocol_name*.**

설명: ODM 오브젝트 클래스, OCSvhost에 지정된 프로토콜 이름이 지원되지 않습니다.

ICA2113 LM에 대한 socket 열기 오류: *errno*.

설명: 로그인 모니터가 거주하는 호스트 시스템에 대하여 socket() 오류가 발생했습니다.

ICA2114 로컬 주소 바인딩 오류: *errno*.

설명: 해당 OCS 노드에 대하여 로컬 주소 사용시 bind() 오류.

ICA2115 LM에 socket 연결 오류: *errno*.

설명: 로그인 모니터가 거주하는 호스트 시스템에 connect() 오류가 발생했습니다.

ICA2116 프로토콜 유형 오류: *protocol_type*.

설명: 호스트 로그인 모니터와 통신하는데 사용되는 가상 터미널 프로토콜 유형이 유효하지 않습니다.

ICA2117 LM 메세지에서 Malloc 오류.

설명: 가변 길이 로그인 모니터 메세지에 대하여 동적으로 공간을 할당할 때 malloc() 오류가 발생했습니다.

ICA2118 LM에 메세지 전송 오류: *errno*.

설명: 올바른 호스트 장치를 열기 위하여 로그인 모니터에 요청을 전송할 때 send() 오류가 발생했습니다.

ICA2119 LM에서 메세지 수신 중 오류: *errno*.

설명: 로그인 모니터가 확인응답을 전송할 때 recv() 오류가 발생했습니다.

ICA2120 LM에서 상태 오류: *status*.

설명: 로그인 모니터의 확인응답이 호스트 장치가 성공적으로 열리지 않았음을 나타냅니다.

ICA2121 OCS 관리 장치 열기 오류: *errno*.

설명: OCS 관리 장치가 성공적으로 열리지 않았습니다.

ICA2122 TBM ID로 IP 주소 변환이 실패했음: *errno*.

설명: ioctl() OCS_GET_TBMID 오류가 발생했습니다. ioctl 명령 OCS_GET_TBMID가 OCS 관리 장치에서 실패했습니다.

ICA2123 rlogin에서 결정한 TBM 연결 오류: *errno*.

설명: ioctl() OCS_IS_TBM_CONNECTED 오류가 발생했습니다. ioctl 명령 OCS_IS_TBM_CONNECTED가 OCS 관리 장치에서 실패했습니다.

ICA2124 호스트 노드가 연결되지 않음: *errno*.

설명: 가능한 호스트 노드 리스트에서 해당 OCS 노드에 연결된 호스트 노드가 없습니다.

ICA2125 ODM(오브젝트 데이터 관리자): *Customized_Attribute*: *odmerrno*.

설명: ODM 오브젝트 클래스, CuAt(사용자 정의 속성)에 대하여 odm_get_list() 오류가 발생했습니다.

ICA2126 OCS 호스트 노드 이름이 연관되지 않음: *hostnode_to_connect*.

설명: CuAt(사용자 정의 속성) 항목이 발견되었지만 hostnode/ocsnode가 일치하지 않습니다.

ICA2127 호스트 배열에서 Malloc 오류.

설명: 가능한 호스트 이름의 배열에 대하여 동적으로 공간을 할당할 때 malloc() 오류가 발생했습니다.

ICA2128 사용자 확인 전에 *client ip*(클라이언트 사이트)의 사용자가 명령 '*invalid command*'을 시도했음.

설명: 사용자 확인을 위하여 사용자명과 암호를 입력하기 전에 사용자가 조치를 시도하였습니다 - 처리를 계속하려면 사용자가 먼저 확인되어야 합니다.

사용자 응답: USER 및 PASS로 로그인 하십시오.

ICA2129 gethostbyname (*invocation name*): *errno*

설명: ftpd에서 호스트명에 해당하는 호스트 정보를 얻으려는 중 시스템 오류가 발생했습니다.

ICA2130 *client ip*(클라이언트 사이트)로부터 사용자 (*username*)가 '*invalid command*'명령을 시도했습니다.

설명: 지정된 사용자가 잘못된 명령을 시도했음.

사용자 응답: "quote site 목적지"를 지정할 때까지 USER, QUOTE SITE 및 QUIT 명령만이 허용됩니다.

ICA2131 **user. cfg 파일의 오류로 인하여 사용자 *user name*'에 대한 *client ip*로부터의 사용자 확인이 실패했습니다.**

설명: Firewall 관리자가 설정한 user.cfg 파일 사양으로 인하여 사용자 확인이 실패했습니다(이전 로그 확인).

사용자 응답: Firewall 관리자를 참조하십시오.

ICA2132 ***client ip*(클라이언트 사이트)로부터 사용자 '*user*'가 '*invalid command*'명령을 시도했습니다.**

설명: 사용자가 잘못된 명령을 시도했습니다. 이 시점에서 유효한 명령은 SITE, USER 및 QUIT 뿐입니다.

ICA2133 **오류: *function* 호출이 *instance*:*line*에서 실패했습니다. *WSAGetLastError***

설명: 일반적인 오류 메세지; 로그를 확인하십시오.

ICA2134 **알림: ftpd: connect() (*instance*에서)가 *IP*, *WSAGetLastError*에 도달할 수 없습니다.**

설명: Connect()에서 요청된 주소를 찾을 수 없음; WSAGetLastError 결과를 확인하십시오.

사용자 응답: 주소를 다시 확인하십시오 - DNS 또는 네트워크 오류일 수도 있습니다.

ICA2135 **데이터 전송이 완료되었습니다: *bytes* 바이트 (발신처 *source IP*에서)수신; *bytes* 바이트 송신 (송신처 *destination IP*).**

설명: 이 정보는 특정 FTP 세션 중에 단일 데이터 전송을 반영합니다. 그러나 데이터 전송이 성공적으로 완료되지 못했을 수 있습니다(실패한 호출 수신 또는 전송이 있었는지 로그를 점검하십시오).

ICA2136 **오류: CreateThread()가 *instance*에서 실패했습니다: *errno*.**

설명: ftpd가 쓰레드를 작성할 수 없습니다.

ICA2137 **데이터 연결 설정; 서버: *source ip* 클라이언트: *destination ip*.**

설명: 데이터 연결을 성공했습니다.

ICA2138 **메모리 부족: pftpd: malloc(*bytes*)은 함수 *instance*에서 NULL 값을 리턴합니다.**

설명: 충분한 메모리를 할당할 수 없음 - malloc이 NULL을 전송했습니다.

ICA2139 **LogonUser() 실패: *reason*.**

설명: Windows NT(SAM) API LogonUser(암호 확인을 위한)가 지정된 원인(들)으로 실패했습니다.

사용자 응답: Firewall 관리자에게 문의하십시오.

ICA2140 **httpd --> HTTP 프록시 사용자 확인 *result* 다음 사용자용 < *user*>, 장소 < *user ip*>, 통로 *network* ... RC:< *reason*>.**

설명: HTTP 프록시가 사용자 확인을 시도했습니다. 지정된 이유로 인해 그 성공이나 실패가 여기에 보고되었습니다.

사용자 응답: Firewall 관리자에게 문의하십시오.

ICA2141 ***IP_address*에서 *IP_address*로 FTP 세션이 중단됩니다.**

설명: Firewall으로의 ftp 세션이 중단됩니다.

ICA2142 **fw_tn_authenticate가 *userid*를 성공적으로 확인했습니다.**

ICA2143 **fw_tn_authenticate이 *userid*용으로 사용자 ID를 확인하는데 실패 했습니다.**

설명: fw_tn_authenticate가 지정된 사용자 ID를 확인할 수 없습니다.

시스템 조치: 로그인이 거부되었습니다.

사용자 응답: fw_tn_authenticate에 로깅 기능이 있는 경우, 원인을 결정하려면 관리자 n은 로그 파일을 조사해야 합니다.

ICA2144 **fw_tn_authenticate가 성공적으로 리턴되지 않았음.**

설명: fw_tn_authenticate에서 전송한 값이 0이 아닙니다. 함수 fw_tn_authenticate가 누락되었을 수도 있습니다.

시스템 조치: 로그인이 거부되었습니다.

사용자 응답: 0이 아닌 값을 전송한 적이 있는지 알려면 fw_tn_authenticate를 자세히 조사하고 발생한 경우 수정하십시오. 해당하는 경우, 라이브러리 fwuser.o를 다시 만든 다음 Firewall에 저장하십시오.

ICA2145 **시스템이 파일 *filename*의 행 *linenumber*에 리턴 코드 *rc*를 전송했음.**

설명: 시스템 호출이 실패했습니다. 라이브러리 fwuser.o가 없을 수도 있습니다.

시스템 조치: 사용자 확인이 취소되었습니다.

사용자 응답: /usr/lib/fwuser.o가 존재하는지 확인하십시오. 존재하는 경우, IBM 대표부에 문의하십시오.

ICA2146 **IBM-제공 fwuser.o가 교체되지 않았음.**

설명: 사용자 자신의 fwuser.o로 대체하지 않았으므로 IBM-제공 fwuser.o를 사용 중입니다.

시스템 조치: 사용자 확인이 취소되었습니다.

사용자 응답: 사용자 제공 사용자 확인을 사용하기 위하여 사용자를 정의한 경우 자신의 사용자 확인을 작성하여 컴파일해야 합니다. IBM-제공 fwuser.o는 모든 비-AIX 및 비 -Firewall 사용자에 대한 액세스를 거부합니다.

ICA2147 **fwtelnet: 사용자 *user id*가 *dest IP addr* (보안측)로부터 *source IP addr*로 가시적인 텔넷 세션을 시작했음.**

설명: 각각의 가시적인 프록시 세션(fwtelnet) 시작시 메세지가 생성됩니다. 세션은 사용자 id, 출발지 ip 및 목적지 ip가 모두 Firewall에 알려지면 시작됩니다. 보안측에서 시작된 세션만이 허용됩니다.

시스템 조치: 가시적인 텔넷을 허용합니다.

ICA2148 **주의 -- 사용자 *user id*에 대한 *source IP addr*(비보안 측)으로부터 *dest IP addr*에 대해 사용자 확인되지 않은 연결 시도가 허용되지 않음.**

설명: 일반적으로 비보안 인터페이스를 통하여 Firewall에 연결을 설정하려는 시도를 나타냅니다.

시스템 조치: 연결 거부.

사용자 응답: 가시적인 프록시를 사용하여 보안측에서 텔넷 연결을 수행해야 합니다.

ICA2149 **fwtelnet: *source IP addr*로부터 *dest IP addr*로 가시적인 텔넷 세션을 시작하는 동안 LOGIN_ADAPTER_ERROR가 발생했습니다.**

설명: q_check_secure(0)을 호출할 때 LOGIN_ADAPTER_ERROR가 발생했습니다.

시스템 조치: 연결 거부.

사용자 응답: 보안 어댑터를 확인하십시오.

ICA2150 **Pftpd 오류 - *failing function*: 리턴 코드 = 0x*function return code***

설명: pftpd 서버가 표시된 함수에서 오류를 발견했습니다. 디먼이 종료됩니다.

사용자 응답: 표시된 시스템 문제를 해결하고 pftpd를 재시작하십시오.

ICA2151 **로그인이 거부됨.**

설명: 이 메세지는 로그인하려고 시도하지만 허용되지 않은 사용자에게 표시됩니다.

ICA2152 **fwlogin: *device*에 쓰지 못했음.**

설명: 장치에 쓸 수 없습니다.

ICA2153 **fwlogin: *deivce*로부터 읽지 못했음.**

설명: 장치를 읽을 수 없습니다.

ICA2154 ***reason* 문제로 *portname*상의 오류.**

설명: 이 Firewall에 문제점이 발생했습니다.

ICA2155 **Pftpd 오류 - *failing function*: *system error message***

설명: pftpd 서버가 표시된 함수에서 오류를 발견했습니다. 디먼이 종료됩니다.

사용자 응답: 표시된 시스템 문제를 해결하고 pftpd를 재시작하십시오.

ICA2156 주의 -- 사용자 *user id*가 비보안 부분 *source IP addr*에서 *dest IP addr*로의 가시적 **FTP**를 사용하려 했으나 허용되지 않았음.

설명: 일반적으로 비보안 인터페이스를 통하여 Firewall에 연결을 설정하려는 시도를 나타냅니다.

시스템 조치: 연결 거부.

사용자 응답: 가시적 프록시를 사용하여 보안 부분으로부터 ftp를 수행해야 합니다.

ICA2157 *source IP addr*의 *user id*사용자는 *dest IP addr*에 가시적 프록시를 사용하도록 허가되지 않았습니다.

설명: 일반적으로 가시적인 프록시가 구성되지 않은 경우 Firewall에 대한 연결을 설정하려는 시도를 나타냅니다.

시스템 조치: 연결 거부.

사용자 응답: fwtpproxy ftp = on으로 설정

ICA2158 옵션 *value*이 틀리게 지정되었음.

설명: 표시된 플래그가 틀리게 지정되었습니다.

ICA2159 **-t** 옵션에 대하여 시간종료 값이 지정되지 않음.

설명: -t 옵션에 대한 시간종료 값을 제공해야 합니다.

ICA2160 *network*:*hosst name*에 :*user ID*사용자용 암호가 변경되었습니다.

설명: FTP 사용자가 암호 데이터베이스에서 자신의 암호를 성공적으로 변경했습니다.

시스템 조치: 없음

사용자 응답: 없음

ICA2161 사용자 *user ID*가 *network*:*host name*으로부터 만료된 암호를 사용하여 로그인을 시도했음.

설명: FTP 사용자가 만료된 암호를 사용하여 Firewall에 대한 연결을 설정하려고 시도했습니다.

시스템 조치: FTP 로그인 유효성 검증이 실패했으며 사용자가 FTP 명령어 쉘로 복귀합니다.

사용자 응답: 사용자는 FTP USER 명령을 통하여 또는 FTP 연결을 다시 설정하고 ″old_password/new_password/new_password″ 형태의 암호 문자열을 전달하여 유효성 검증을 다시 시도해야 합니다.

ICA2162 *network*:*hosst name*에 :*user ID*사용자용 암호 변경이 실패했습니다.

설명: FTP 사용자가 암호를 변경하려고 시도했으며 암호 유효성 검증 루틴이 실패했습니다. 가능한 실패 원인에는 다음이 포함됩니다. : - 잘못된 ″이전″ 암호가 지정되었음, - ″새로운″ 암호가 한 번만 지정됨, - ″새로운″ 암호가 사용된 두 경우에 암호가 서로 일치하지 않음, 또는 - 암호를 분리하는데 사용되는 분리자가 ″/″가 아님.

시스템 조치: FTP 암호 유효성 검증이 실패했으며 사용자가 FTP 명령 쉘로 복귀합니다.

사용자 응답: 암호를 검증하는 FTP 서버의 유효성 재확인 시도가 제대로 입력되었습니다. 문제가 지속되면 서비스 대표부에 문의하십시오.

ICA2163 **safemaild**가 시작됨.

설명: safemaild가 시작됩니다.

ICA2164 **safemaild**가 중지됨.

설명: safemaild가 중지됩니다.

ICA2165 텔넷 세션이 인터럽트되었음.

설명: 텔넷 세션이 종료 중이지만, 파이프에서 세션 정보를 검색할 수 없습니다. 아마도 세션은 클라이언트에 의해 시작 중에 인터럽트되었으며, 따라서 세션이 완전히 초기화되지 않았습니다.

ICA2166 *user id*사용자용으로 *attribute*속성을 검색할 수 없습니다. 리턴 코드 = *return code*.

설명: 사용자 확인 서비스가 지정된 사용자에 대한 사용자 데이터베이스로부터 지정된 속성을 검색할 수 없습니다. 시스템 조치: 사용자 확인에 실패합니다.

사용자 응답: 시스템 관리자에게 문의하여 사용자의 데이터베이스 레코드를 수정하십시오.

ICA2167 *network type*의 *client address*에서 *service*에 대한 *authentication scheme*을 이용한 *user id*사용자 확인이 실패했습니다.

설명: 지정된 사용자가 지정된 사용자 확인 방법을 사용하여 지정된 서비스에 대해 확인되지 못했습니다. 사용자는 표시된 주소와 네트워크 유형으로부터 서비스를 요청했습니다. 시스템 조치: 사용자 확인에 실패합니다.

사용자 응답: 시스템 관리자에게 문의하십시오.

ICA2168 기억영역 부족으로 *service*에 대한 *user id* 확인에 실패했음.

설명: 사용자 ID가 사용자 확인 프로세싱 중에 메모리 할당 실패로 인해 서비스에 대해 확인되지 못했습니다. 시스템 조치: 사용자 확인에 실패합니다.

사용자 응답: 시스템 관리자에게 문의하십시오.

ICA2169 *network*:*host name*에서 *method*확인 방법을 사용하여 *service*용 사용자 *name*을(를) 성공적으로 확인하였습니다.

설명: FW에서 지정된 확인 방법을 사용하여 요청된 서비스에 대해 표시된 사용자 이름을 확인했습니다.

ICA2170 *service*에 대한 *user id*사용자 확인이 실패했습니다. *auth method*가 **Firewall**에 등록되어 있지 않습니다.

설명: 사용자 ID가 서비스에 대해 확인되지 못했습니다. 요청된 사용자 확인 방법은 Firewall에 등록되어 있지 않습니다. 시스템 조치: 사용자 확인에 실패합니다.

사용자 응답: 시스템 관리자에게 문의하십시오.

ICA2171 계정 *user_name*이 만기된 암호로 인해 잠겨 있음.

설명: 암호가 만기되었으며 변경되지 않았습니다. 이 계정은 잠겨 있습니다.

시스템 조치: 해당 계정은 잠겨 있으며 Firewall 암호 사용자 확인은 실패합니다. UserRes

ICA2172 계정 *user_name*은 잠겨 있습니다.

설명: 이 계정은 잠겨 있습니다.

시스템 조치: 해당 계정은 잠겨 있습니다. Firewall 암호 사용자 확인은 실패합니다.

사용자 응답: 계정 잠금해제에 대해 Firewall 관리자에게 문의하십시오.

ICA2173 사용자가 예약된 사용자 이름 *user id*를 사용하여 로그인하려 했음.

설명: 사용자가 제공한 ID가 Firewall에 의해 사용이 예약되었습니다.

시스템 조치: 로그인이 거부되었습니다.

사용자 응답: 관리자는 이 사용자 이름을 사용 중인 사용자를 조사해야 합니다.

ICA2174 내부 프로세싱 오류로 인해 *network type*의 *client address*에서 *service*에 대한 *authentication scheme*을 이용한 *user id*사용자 확인이 실패했습니다.

설명: 지정된 사용자가 지정된 사용자 확인 방법을 사용하여 지정된 서비스에 대해 확인되지 못했습니다. 사용자는 표시된 주소와 네트워크 유형으로부터 서비스를 요청했습니다. 사용자 확인 요청은 내부 프로세싱 오류로 인해 실패했습니다. 시스템 조치: 사용자 확인에 실패합니다.

사용자 응답: 시스템 관리자에게 문의하십시오.

ICA2175 사용자 *user name*에 대한 **Windows NT LogonUser** 호출이 실패했습니다. 최종 오류는 *last error*입니다.

설명: 지정된 사용자 이름이 Windows NT LogonUser API 호출에 의해 확인되지 못했습니다. Windows NT는 LogonUser 실패 후에 마지막 오류를 보고했습니다. 시스템 조치: 사용자 확인에 실패합니다.

사용자 응답: 시스템 관리자에게 문의하십시오.

ICA2176 알 수 없는 사용자 확인 스킴(**scheme**) *authentication scheme*은 *network*에서 *component*를 사용하여 *user name*용으로 정의되었습니다.

설명: 지정된 사용자 확인 스킴(scheme)이 지정된 네트워크로부터 지정된 Firewall 구성요소를 사용하여 지정된 사용자에 대해 정의되었으나 이 사용자 확인 스킴(scheme)은 현재 Firewall에 등록되어 있지 않습니다. 시스템 조치: 사용자 확인 요청이 실패합니다.

사용자 응답: 시스템 관리자에게 문의하십시오.

ICA2177 **SafeMail** 연결 **0x***session ID*은(는) *socket peer name*에서 수신되었습니다.

설명: SafeMail이 나열된 피어 이름으로부터 인바운드 연결을 수신했습니다. 추적을 위해 표시된 연결 ID 번호가 할당되었습니다. (디버그 레벨)

시스템 조치: 이 연결을 처리하기 위해 쓰레드가 디스패치되었습니다.

ICA2178 **SafeMail 세션 0x*session ID*은 *sender's IP address*에서 *recipient's IP address*으(로) 구축되었습니다.**

설명: SafeMail이 수신자 전자우편 서버와의 접촉을 설정했으며 전자우편 전송 준비가 완료되었습니다. (정보 레벨)

시스템 조치: 데이터 전송이 곧 시작됩니다.

ICA2179 **SafeMail이 *sending server's address*에서 *receiving server's address*로 0x*session ID* 연결을 위해 *message size*bytes 전송되었습니다.**

설명: SafeMail이 나열된 두 전자우편 서버 사이에서 메세지를 성공적으로 전달했습니다. 이 세션은 앞서 ICA2166 메세지에서 제시되었습니다. 이 메세지에는 표시된 바이트 수가 포함되어 있습니다. (정보 레벨)

ICA2180 **SafeMail이 세션 0x*Session ID*를 *sender's address*에서 중단하였습니다.**

설명: SafeMail이 표시된 세션에 송신되고 있는 전자우편의 전송을 거부했습니다. (정보 레벨)

시스템 조치: 세션이 중단되었습니다.

사용자 응답: 로깅 우선순위 레벨을 증가시켜 좀더 자세한 진단 정보를 얻으십시오.

ICA2181 **SafeMail이 세션 0x*Session ID*를 *reason code*로 인해 중단하였습니다.**

설명: SafeMail의 기본 프로세서는 1차 오류 상태가 발견되었으므로 표시된 세션을 종료했습니다. 이유 코드에는 다음이 포함됩니다. \01 - 수신자 전자우편 서버를 찾을 수 없습니다. \02 - 송신자가 두 비보안 서버간 전자우편 경로를 지정하려 합니다. \03 - 수신자 전자우편 서버가 연결을 거부합니다. 다운되었을 수 있습니다. \04 - 수신자 전자우편 서버가 전자우편 수신을 거부합니다. \05 - 하나 이상의 연결이 시간 종료되었습니다. 송신중인 또는 \수신중인 전자우편 서버가 다운되었을 수 있습니다. \06 - recv()가 0 바이트를 반환했습니다. 송신중인 또는 수신중인 전자우편 서버가 \다운되었을 수 있습니다. \07 - recv()가 음수를 반환했습니다. 송신중이거나 수신중에 \전자우편 서버가 다운되었을 수 있습니다. \08 - 오류 명령이 지나치게 많이 수신되었습니다. \09 - select()가 음수를 반환했습니다. 송신중인 또는 수신중인 전자우편 서버가 \다운되었을 수 있습니다. @404C 메세지가 디버그 레벨에 기록됩니다.

시스템 조치: 연결이 중단되었습니다.

ICA2182 **SafeMail이 세션 0x*Session ID*를 유효하지 않은 *SMTP command* 명령때문에 거부했습니다. 이유 코드 *reason code*.**

설명: SafeMail의 명령 유효성 검증 서브루틴이 유효하지 않거나 위험한 명령을 발견했습니다. 이러한 이유 코드는 각 SMTP 명령에서 달라집니다. IBM Firewall 지원 웹 페이지를 참고하여 현재 값을 찾아 보십시오. (디버그 레벨)

시스템 조치: 연결이 중단되었습니다.

사용자 응답: 안전하고 유효한 정보가 송신되도록 송신중인 전자우편 클라이언트 또는 송신 중인 전자우편 서버를 수정하십시오.

ICA2183 **httpd --> HTTP 프록시 구성 파일 (*filename*)이 사용 가능하지 않음.**

설명: HTTP 프록시 디먼이 지정된 구성 파일을 열려했으나 존재하지 않거나 열 수 없습니다.

시스템 조치: HTTP 프록시가 시작되지 않습니다.

사용자 응답: GUI 또는 fwhttp 명령을 통해 프록시를 구성하고 프록시를 재시작하십시오.

ICA2184 **신호 *signal No.*에서 signal() 오류 발생. safemaild 종료.**

설명: safemaild 디먼이 신호 처리기를 설정하려 할 때 시스템 오류가 발생했습니다.

ICA2185 **Socket을 열 수 없음. safemaild가 종료됨.**

설명: Socket 열기를 실패했습니다.

ICA2186 **Socket을 포트로 바인드할 수 없음. safemaild가 종료됨.**

설명: 포트로 socket 바인드를 실패했습니다.

ICA2187 **새로운 연결을 수용할 수 없음. safemaild가 다시 시도함.**

설명: 새로운 연결 수용을 실패했습니다.

ICA2188 **-l에 대하여 지정된 시간(*value*)이 잘못되었습니다.**

설명: 나타나는 시간값에 숫자 범위 0..9를 벗어나는 문자가 들어 있거나 허용되는 최대값을 초과합니다.

ICA2189 **-l 옵션에 대하여 시간종료 값이 지정되지 않았습니다.**

설명: -l 옵션에 대한 시간종료 값을 제공해야 합니다.

ICA2200 **(*service*:*function*) WinSocket 초기화 오류:** *WSAGetLastError*

설명: WinSocket을 초기화할 때 오류가 발생했습니다.

사용자 응답: WSAGetLastError가 나타내는 시스템 문제를 수정하고 표시된 서비스(첫 번째 매개변수)를 재시작하십시오.

ICA2201 **(*service*:*calling function*) *failed function*이(가) *line number*라인 : *WSAGetLastError*에서 실패했습니다.**

설명: 지정된 네트워킹 구성요소가 실패합니다.

사용자 응답: WSAGetLastError가 나타내는 시스템 문제를 수정하고 표시된 서비스(첫 번째 매개변수)를 재시작하십시오.

ICA2202 **(*service*:*calling function*) *timeout*이(가) *WSAGetLastError* seconds : 후에 시간종료되었습니다.**

설명: 지정된 시간 동안 유휴 상태에 있은 후 표시된 함수의 시간이 초과됩니다.

사용자 응답: 표시된 서비스로 재연결하고 표시된 시간 초과 이전에 응답하십시오.

ICA2203 **(*service*:*calling function*) 메모리 오류; *failed function*이 *return value*를 *line number*라인 : *WSAGetLastError*에서 리턴했습니다.**

설명: 메모리 오류가 발생했습니다. 대개 메모리 부족 상태입니다. WSAGetLastError를 점검하십시오.

사용자 응답: 디스크 공간을 확보하십시오. 시스템 관리자에게 문의하십시오.

ICA2204 **(*service*:*calling function*) *filename* 오류: 액세스가 거부되었거나 작성이 실패했습니다.**

설명: 표시된 서비스가 지정된 파일이나 파일 매개변수와 관련된 파일에 액세스하거나 이러한 파일을 작성하려 할 때 오류가 발생했습니다.

사용자 응답: 표시된 파일명이 존재하는지와 올바른 허용권한을 가지는지 확인하십시오.

ICA2205 **(*service*:*calling function*) 파일 *filename*이 요구되었으나 찾을 수 없음.**

설명: 지정된 파일이 없습니다. 실패의 가장 일반적인 원인은 Firewall 디폴트 구성이 지워진 것입니다. 현재 백업으로부터 파일을 복원하십시오.

사용자 응답: 구성 파일이 없는지 확인하십시오. 구성 프로그램은 이 파일이 존재하는 것으로 예상합니다. 백업 버전이 사용 가능하지 않습니다. 서비스 대표부에 문의하십시오.

ICA2206 **(*service*:*calling function*) 구성 파일 *filename*이(가) 손상되었습니다.**

설명: 표시된 구성 파일 형식이 사용 가능한 형식이 아닙니다. 내용이 손상되었습니다. 손상의 가장 일반적 원인은 파일이 수동으로 편집되었거나 유효하지 않은 데이터가 추가된 것입니다.

사용자 응답: 구성 파일을 제대로 재작성해야 합니다. 먼저 파일을 작성하고(또는 열람 가능한 사본을 작성) 원래 파일을 지우십시오. 필요한 경우 참조용으로 원래 파일을 사용하여 적절한 Firewall 구성 명령으로 파일을 재구성하십시오.

ICA2207 **(*service*:*calling function*) 구성 파일 *filename*이(가) 비어 있습니다.**

설명: 표시된 구성 파일을 찾을 수 없거나 파일이 있어도 비어 있습니다. 파일을 찾을 수 없는 가장 일반적인 원인은 표시된 서비스에 대한 구성이 수행되지 않은 것입니다.

사용자 응답: 구성 파일의 상태를 확인하십시오. 파일이 있으면 구성 명령은 이 파일에 데이터가 있는 것으로 간주합니다. 추가 정보에 대해서는 설명서를 참고하십시오.

ICA2208 *service session id* 세션이 비보안 어댑터에서 *user id*용으로 시작되었습니다 (*source IP address*:*dest IP addr*).

설명: 표시된 각 세션의 처음에 메세지가 생성되었음.

ICA2209 *service session id* 세션이 비보안 어댑터에서 *user id*용으로 종료되었습니다. (*source IP address*:*dest IP addr*); *total bytes*바이트.

설명: 표시된 각 세션의 끝에서 메세지가 생성되었습니다. 전체 바이트 수는 세션 중에 전송된 바이트 수를 나타냅니다. 전체 바이트 수를 지원하지 않는 서비스(예: ptelnetd)는 0을 나타냅니다.

ICA2210 (*service*) *user id* 사용자가 *source IP address* (비보안)으로부터 만기된 암호를 사용하여 로그인을 시도했습니다.

설명: 표시된 사용자가 비보안 어댑터 상에서 표시된 출발지 IP로부터 표시된 만기된 암호를 사용하여 Firewall으로의 연결을 설정하려 했습니다.

사용자 응답: 제공된 암호가 암호 ruleset마다 만기되었습니다. 시스템 관리자에게 문의하십시오.

ICA2211 (*service*) *user id* 사용자가 *source IP address* (보안)으로부터 만기된 암호를 사용하여 로그인을 시도했습니다.

설명: 표시된 사용자가 보안 어댑터 상에서 표시된 출발지 IP로부터 표시된 만기된 암호를 사용하여 Firewall으로의 연결을 설정하려 했습니다.

사용자 응답: 제공된 암호가 암호 ruleset마다 만기되었습니다. 시스템 관리자에게 문의하십시오.

ICA2212 (*service*) *name* 사용자가 *source IP address* (보안)에서 성공적으로 확인되었습니다.

설명: FW에서 보안 어댑터 상의 표시된 출발지 IP로부터 표시된 사용자 이름을 확인했습니다.

ICA2213 (*service*) *name* 사용자가 *source IP address* (비보안)에서 성공적으로 확인되었습니다.

설명: FW에서 비보안 어댑터 상의 표시된 출발지 IP로부터 표시된 사용자 이름을 확인했습니다.

ICA2214 (*service*) *name* 사용자가 *source IP address* (비보안)에서 사용자 확인에 실패했습니다.

설명: FW에서 비보안 어댑터 상의 표시된 출발지 IP로부터 표시된 사용자 이름에 대한 확인에 실패했습니다.

사용자 응답: 가장 가능성 있는 원인은 사용자 이름이나 암호를 잘못 입력한 것입니다. 사용자 이름과 암호는 대소문자를 구분합니다(Caps Lock키를 점검하십시오).

ICA2215 (*service*) *name* 사용자가 *source IP address* (보안)에서 사용자 확인에 실패했습니다.

설명: FW에서 보안 어댑터 상의 표시된 출발지 IP로부터 표시된 사용자 이름에 대한 확인에 실패했습니다.

사용자 응답: 가장 가능성 있는 원인은 사용자 이름이나 암호를 잘못 입력한 것입니다. 사용자 이름과 암호는 대소문자를 구분합니다(Caps Lock키를 점검하십시오).

ICA2216 (*service*) *source IP address*(비보안)으로부터 사용자 *name*이 일치하는(검증) 암호를 입력하지 못했음.

설명: 암호 변경이 요청되었거나 필요한 상황에서 비보안 어댑터 상의 표시된 출발지 IP로부터 표시된 사용자가 일치하지 않는 암호를 입력했습니다. 사용자 확인 데이터는 변경되지 않았습니다.

사용자 응답: 암호 변경시 검증을 위해 암호를 두 번 입력해야 합니다. 가장 가능성 있는 원인은 검증 암호를 잘못 입력한 것입니다.

ICA2217 (*service*) *source IP address*(보안)으로부터 사용자 *name*이 일치하는(검증) 암호를 입력하지 못했음.

설명: 암호 변경이 요청되었거나 필요한 상황에서 보안 어댑터 상의 표시된 출발지 IP로부터 표시된 사용자가 일치하지 않는 암호를 입력했습니다. 사용자 확인 데이터는 변경되지 않았습니다.

사용자 응답: 암호 변경시 검증을 위해 암호를 두 번 입력해야 합니다. 가장 가능성 있는 원인은 검증 암호를 잘못 입력한 것입니다.

ICA2218 *service session id* 세션이 보안 어댑터에서 *user id*용으로 시작되었습니다 (*source IP address*:*dest IP addr*).

설명: 표시된 각 세션의 처음에 메세지가 생성되었음.

ICA2219 *service session id* 세션이 보안 어댑터에서 *user id*용으로 종료되었습니다. (*source IP address*:*dest IP addr*); *Total Bytes*바이트.

설명: 표시된 각 세션의 끝에서 메세지가 생성되었습니다. 전체 바이트 수는 세션 중에 전송된 바이트 수를 나타냅니다. 전체 바이트 수를 지원하지 않는 서비스(예: ptelnetd)는 0을 나타냅니다.

ICA2220 (*service*) *user id*사용자가 *source IP addr*에서 (보안면) to *dest IP addr*로 가시적 프록시 세션을 시작했습니다.

설명: 각 가시적 프록시 세션의 시작에서 메세지가 생성되었습니다. 세션은 사용자 ID, 출발지 IP와 목적지 IP가 Firewall에 모두 알려지면 시작됩니다. 보안측에서 시작된 세션만이 허용됩니다.

시스템 조치: 가시적 프록시를 허용합니다.

ICA2221 (*service*) 경고: 제어 행의 피어 끝에 있는 IP(*Control IP addr*)가 데이터 행의 피어 끝에 있는 IP(*Data IP addr*)와 일치하지 않음.

설명: 보안을 위해(예: 반 하이제킹) 제어 연결 socket이 연결되어 있는 피어의 IP 주소가 데이터 연결 socket이 연결되어 있는 피어의 IP 주소와 같은지 확인하십시오. 이들 주소는 Net Dispatcher를 사용하고 있거나 목적지에서 다중 어댑터를 사용하는 경우에는 달라질 수 있습니다.

시스템 조치: 목적지 FTP 서버가 다중 어댑터를 사용하는지 혹은 Net Dispatcher가 사용되고 있은지 점검하십시오. 필터가 포트 20과 포트 21을 통해 유효한 IP 주소만 허용하는지 확인하십시오.

ICA2222 (*service*) 경고 프로토콜 위반. RFC를 준수하지 않는 명령 *invalid string*; 예상치 못한 *protocol string*.

설명: 표시된 서비스가 관련 RFC를 준수하지 않는 예상치 못한 문자열을 수신했습니다. 헤커가 관련될 수 있습니다.

시스템 조치: 표시된 서비스에 대해 RFC를 준수하는 클라이언트를 사용하십시오.

ICA3001 *경고*: 실제 사용자는 *socks connect user name*이 아니라 *ident user name*입니다.

설명: 보안 분기 시도가 있었습니다. 사용자 이름이 확인되지 않았습니다.

ICA3006 *client*에서 *count* 바이트, *server*에서 *count* 바이트

설명: 메세지는 sockd 디먼과 개별 클라이언트 및 서버 호스트간에 전송되는 바이트 수를 나타냅니다.

ICA3007 최대 연결 수 초과로 인해 연결이 거절되었습니다.

설명: SOCKS 서버는 특정 클라이언트 세션의 최대 수만을 수용하도록 구성됩니다. 임계값이 이미 충족되고 추가 연결 요청이 도달할 때 이 메세지가 작성됩니다.

시스템 조치: 새로 시도된 연결이 종료되었습니다.

사용자 응답: 병렬 연결의 최대 수는 socks5.conf 안의 SOCKS5_MAXCHILD 매개변수에 의해 판별됩니다. 이 설정을 증가시키고 서버를 최신으로 고치십시오. 세부사항은 IBM Firewall 참조를 참고하십시오. start unused

ICA3010 연결이 설정됩니다 -- *user*(*real_user*)@*src_addr* for *dst_addr* (*destination port*에서 연결)

설명: 연결이 설정됩니다.

ICA3011 연결이 설정됩니다 -- *user*(*real_user*)@*src_addr* to *dst_addr* (*application*에서 연결)

설명: 외부로의 socket 연결에 성공했습니다.

ICA3012 연결이 거부되었습니다 -- *user*(*real_user*)@*src_addr* to *dst_addr* (*application*에서 연결 거부)

설명: 원격 호스트에서 연결을 거부했습니다.

ICA3013 select() *errno*

설명: 시스템 오류.

ICA3014 연결이 종료되었습니다 -- *user*(*real_user*)@*src_addr* **for** *dst_addr* (*destination port*).(*count* **bytes from** *client*, *count* **bytes from** *server*에서 연결 종료)

설명: 연결이 종료되었습니다.

ICA3015 연결이 종료되었습니다 -- *user*(*real_user*)@*src_addr* **to** *dst_addr* (*destination host*).(*count* **bytes from** *client*, *count* **bytes from** *server*에서 연결 종료)

설명: 서버로의 연결이 종료되었습니다.

ICA3016 ***destination host*와 통신하기 위한 적절한 인터페이스를 찾을 수 없음.

설명: 파일 /etc/sockd.route가 지정된 목적지 호스트에 대한 라우팅 정보를 포함하지 않습니다.

ICA3017 **pid** *sockd process*에 대하여 쉘 명령을 실행할 수 없음.

설명: Sockd 디먼이 /bin/sh 명령을 실행할 수 없습니다.

사용자 응답: /bin/sh 쉘이 시스템에서 사용 가능한지 확인하십시오.

ICA3018 거부 -- *user*(*real_user*)@*src_addr*로부터 *dst_addr*(*destination port*)로 바인드

설명: 원격 호스트에서 연결을 거부했습니다.

ICA3019 호스트 *socks_src_name*으로부터 **GetDst()** 오류: *errno*

설명: 요청된 연결에 대한 목적지 주소 해결시 오류.

ICA3022 행 *line number*로부터 잘못된 **?=** 필드

설명: /etc/sockd.conf 파일에 잘못된 항목이 발견되었습니다.

ICA3023 행 *line number*에 잘못된 비교.

설명: /etc/sockd.conf 파일에 잘못된 항목이 발견되었습니다.

ICA3024 행 *line number*에 잘못된 항목.

설명: /etc/sockd.route 파일에 잘못된 항목이 발견되었습니다.

ICA3025 행 *line number*에 잘못된 허용/거부 필드.

설명: /etc/sockd.conf 파일에 잘못된 항목이 발견되었습니다.

ICA3026 행 *line number*에 잘못된 포트 번호.

설명: /etc/sockd.conf 파일에 잘못된 항목이 발견되었습니다.

ICA3027 쉘 명령이 (*exec status*) \"*cmd*\"용으로 실패했습니다

설명: 표시된 쉘 명령이 실패했습니다.

사용자 응답: 쉘 프로세서가 시스템에서 사용가능한지 확인하십시오.

ICA3030 구성 파일(*/etc/sockd.conf*)을 열 수 없음.

설명: 표시된 파일에 대한 열기 요청이 실패했습니다.

ICA3031 라우팅 파일(*/etc/sockd.route*)을 열 수 없음: *errno*

설명: 표시된 파일에 대한 열기 요청이 실패했습니다.

사용자 응답: Firewall 관리자를 참조하십시오. Firewall 설치시 디폴트 파일이 제공되었습니다.

ICA3032 사용자 파일(*user name file*)을 열 수 없음: *errno*

설명: 허용 규칙의 *=userlist에 지정된 파일명을 찾을 수 없습니다.

ICA3033 **Validate()**의 예기치못한 결과.

설명: 사용자 이름의 Identd 검증이 지정되었습니다. Identd는 예상치 못한 결과를 나타내며 응답했습니다.

ICA3035 *client host*의 **identd**로 연결할 수 없음.

설명: 사용자 이름의 Identd 검증이 지정되었습니다. Identd는 응답하지 않습니다.

ICA3039 오류 -- 쉘 명령 \″*cmd*\″가 영숫자 문자를 포함하지 않음.

설명: 잘못된 쉘 명령입니다. 로그 메세지를 참고하십시오.

ICA3040 오류 -- **shell_cmd fork()** *errno*

설명: Sockd 디먼이 'fork()'를 통해 하위 프로세스로 전환할 수 없습니다.

ICA3041 오류 -- 클라이언트 주소를 얻을 수 없음.

설명: 'getpeername()' 호출로부터 오류가 전송되었습니다.

사용자 응답: 라우팅 및 DNS 구성을 확인하십시오.

ICA3042 오류 -- 호스트 *클라이언트 주소*의 정의되지 않은 명령(**0x***hex-command-received*)

설명: 클라이언트 응용 프로그램으로부터 잘못된 명령을 수신했습니다.

사용자 응답: 클라이언트 구성 문제이거나 클라이언트와 Firewall 지원 레벨이 일치하지 않는 것입니다.

ICA3043 오류 -- 호스트 *client address*의 잘못된 버전 (**0x***hex-version-number*).

설명: Firewall에서 socks 버전 4.2를 지원합니다.

사용자 응답: 클라이언트 구성 문제이거나 클라이언트와 Firewall 지원 레벨이 일치하지 않는 것입니다.

ICA3044 연결이 실패했습니다 -- *user*(*real_user*)@*src_addr* **to** *dst_addr* (*application*)에서 연결 요청. 오류 코드 : *command causing failure errno*.

설명: 연결 요청이 실패했습니다.

ICA3045 실패했습니다 -- *user*(*real_user*)@*src_addr* **for** *dst_addr*에서 연결 요청. 오류: 잘못된 호스트 *dst_name*에 연결되었습니다 (*dst_port (application)*).

설명: 바인드 요청이 실패했습니다.

ICA3046 실패했습니다 -- *user*(*real_user*)@*src_addr* **for** *dst_addr*에서 연결 요청. 오류 코드: *command causing failure errno*.

설명: 바인드 요청이 실패했습니다.

ICA3047 시간종료 -- *user*(*real_user*)@*src_addr*로부터 *dst_addr*로 바인드.

설명: 연결 시간이 종료되었습니다.

ICA3048 쉘 명령이 너무 김: *command...*

설명: /etc/sockd.conf 파일에서 실행할 명령이 너무 깁니다.

ICA3049 시간 종료 -- *user*(*real_user*)@*src_addr* **to** *dst_addr* (*application*에서 연결 시간 종료)

설명: 연결 시간이 종료되었습니다.

ICA3050 *matched sockd.conf filter rule*

설명: socks 연결에 대응하는 /etc/sockd.conf 파일의 필터 규칙입니다.

ICA3051 **AIX sockd_route()**에서 *remote address*에 대한 인터페이스를 찾을 수 없음.

설명: 인터페이스 라우트 정보를 찾을 수 없습니다.

ICA3052 **userid**를 ″**nobody**″로 설정 오류.

설명: 하위 sockd 프로세스의 userid를 ″nobody″로 설정할 수 없습니다.

ICA3053 **popen(AIX** 라우트 스크립트**)** 오류: *system error message*.

설명: 라우팅 정보를 찾기 위한 스크립트 실행이 실패했습니다.

ICA3054 **AIX sockd_route()에서 치명적인 메모리 할당 실패.**

설명: 라우팅 정보 수집 시도 중 메모리 할당이 실패했습니다.

ICA3055 ***input line*의 첫번째 공간에 대한 치명적인 AIX sockd_route() 구문분석 오류.**

설명: 시스템 라우트 정보 구문분석 오류입니다.

ICA3056 ***input line*의 두번째 공간에 대한 치명적인 AIX sockd_route() 구문분석 오류.**

설명: 시스템 라우트 정보 구문분석 오류입니다.

ICA3057 **라우트 스크립트 출력: *system error message*를 읽는 중 AIX sockd_route()에 치명적인 오류**

설명: 스크립트 출력 읽기 오류입니다.

ICA3058 **popen(AIX 어댑터 스크립트) 오류: *system error*.**

설명: 인터페이스 정보를 찾기 위한 스크립트 실행이 실패했습니다.

ICA3101 **Sockd 데이터 전송 오류 - select(): *system error message*.**

설명: (SOCKS422) 데이터 전송시 오류입니다.

ICA3102 **Sockd 데이터 전송 오류 - write(): *system error message*.**

설명: (SOCKS422) 데이터 전송시 오류입니다.

ICA3103 **Sockd 데이터 수신 오류 - select(): *system error message*.**

설명: (SOCKS422) 데이터 수신 오류입니다.

ICA3104 **Sockd 데이터 수신 오류 - read(): *system error message*.**

설명: (SOCKS422) 데이터 수신 오류입니다.

ICA3105 **프로세스 id 파일 *filename*을 작성할 수 없음.**

설명: (SOCKS422) 프로세스 id 파일 작성/쓰기가 실패했습니다.

ICA3106 **Sockd에서 하위 분기 실패: *system error message*.**

설명: (SOCKS422) SOCKS 요청을 처리하기 위한 하위 분기 시도가 실패했습니다.

ICA3107 **인바운드 socket SO_LINGER 옵션 설정 실패: *system error message*.**

설명: (SOCKS422) 심각하지 않습니다.

ICA3108 **아웃바운드 socket SO_LINGER 옵션 설정 실패: *system error message*.**

설명: (SOCKS422) 심각하지 않습니다.

ICA3109 **파일 *filename*의 행 *line number*에 잘못된 항목.**

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3110 **파일 *filename*의 라인 *line number*에 잘못된 인터페이스 필드.**

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3111 **파일 *filename*의 라인 *line number*에 잘못된 목적지 IP.**

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3112 **파일 *filename*의 라인 *line number*에 잘못된 목적지 마스크.**

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3113 ***filename* 파일의 *number of lines*라인이 분석되었습니다.**

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3114 파일 *filenema*에서 유효한 행을 찾을 수 없음.

설명: (SOCKS422) 구성 파일이 비어 있거나, 구문이 잘못되었습니다.

사용자 응답: 표시된 구성 파일을 수정하십시오.

ICA3115 파일 *filename*의 라인 *line number*에 잘못된 '허용/거부' 필드.

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3116 파일 *filename*의 라인 *line number*에 잘못된 '?=' 필드.

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3117 파일 *filename*의 라인 *line number*에 잘못된 출발지 IP.

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3118 파일 *filename*의 라인 *line number*에 잘못된 출발지 마스크.

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3119 파일 *filename*의 라인 *line number*에 잘못된 비교.

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3120 파일 *filename*의 라인 *line number*에 잘못된 포트 번호.

설명: (SOCKS422) 잘못된 구성 항목 구문입니다.

ICA3121 **SIGUSR1 수신 - socks 구성 덤핑.**

설명: (SOCKS422) 다음 메세지 뒤에 나오는, 활동 중인 구성을 로그 파일에 덤프하기 위한 신호입니다.

ICA3122 **Sockd에서 디먼을 분기할 수 없음:** *system error message*.

설명: (SOCKS422) sockd 디먼을 초기화하기 위한 분기 실패합니다.

사용자 응답: 표시된 시스템 문제를 해결하고 sockd를 재시작하십시오.

ICA3123 **Sockd 서버 시작 중.**

설명: (SOCKS422) Sockd가 성공적으로 초기화되었으며 연결을 대기 중입니다.

ICA3124 **치명적인 sockd 초기화 오류 - bind():** *system error message*.

설명: (SOCKS422) Sockd 서버 초기화 실패, 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 해결하고 sockd를 재시작하십시오.

ICA3125 **치명적인 sockd 초기화 오류 - listen():** *system error message*.

설명: (SOCKS422) Sockd 서버 초기화 실패, 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 해결하고 sockd를 재시작하십시오.

ICA3126 **치명적인 sockd 오류 - main accept():** *system error message*.

설명: (SOCKS422) Sockd 서버 메인 루틴 실패, 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 해결하고 sockd를 재시작하십시오.

ICA3127 **Sockd 서버가 종료 신호를 수신했음.**

설명: root 또는 nobody가 프로세스를 종료했으며, 디먼이 종료되었습니다.

사용자 응답: 관리자 원하는 경우 sockd를 재시작하십시오(″sockd″를 입력하십시오).

ICA3128 **치명적인 sockd 초기화 오류 - socket():** *system error message*.

설명: Sockd 서버 초기화 실패, 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 해결하고 sockd를 재시작하십시오.

ICA3129 **치명적인 sockd 초기화 오류 -** *failing function*: *system error message*.

설명: 표시된 함수에서 Sockd 서버 초기화 실패, 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 해결하고 sockd를 재시작하십시오.

ICA3130 **Sockd 오류 -** *failing function*: *system error message*

설명: sockd 서버가 표시된 함수에서 오류를 감지했습니다. 디먼이 계속되지만, 연결이 거부되거나 종료될 수도 있습니다.

사용자 응답: 문제가 계속되면, sockd를 중지하고, 표시된 시스템 문제를 수정한 다음 sockd를 재시작하십시오.

ICA3131 **읽기 오류** *file name*. **이전에 캐쉬된 데이터를 사용함.**

설명: 파일을 읽을 수 없거나 잘못된 데이터를 포함합니다. 이전 메세지가 문제점을 설명합니다. Sockd는 이전 버전 파일에서 캐쉬된 데이터를 사용하여 작동을 계속합니다.

사용자 응답: 표시된 파일에서 오류를 수정하십시오.

ICA3132 **알 수 없는 플래그 -***value*.

설명: 표시된 플래그가 인식되지 않으며, 디먼이 종료되었습니다.

사용자 응답: 구문을 수정하고 sockd를 재시작하십시오.

ICA3133 **알 수 없는 매개변수** *value*.

설명: 표시된 매개변수가 인식되지 않으며, 디먼이 종료되었습니다.

사용자 응답: 구문을 수정하고 sockd를 재시작하십시오.

ICA3134 **상치되는 옵션** *option1* **and** *option2*.

설명: 표시된 옵션들은 함께 사용할 수 없음, 디먼을 종료합니다.

사용자 응답: 구문을 수정하고 sockd를 재시작하십시오.

ICA3135 **Sockd 오류 -** *failing function*: **리턴 코드 = 0x***function return code*

설명: sockd 서버가 표시된 함수에서 오류를 감지했습니다. 디먼이 종료됩니다.

사용자 응답: 표시된 시스템 문제를 해결하고 sockd를 재시작하십시오.

ICA3700 **WinSocket 초기화 오류 :** *WinSocket error*

설명: WinSocket을 초기화할 때 오류가 발생했습니다.

사용자 응답: 표시된 시스템 문제를 해결하고 sockd를 재시작하십시오.

ICA4000 *program* **- 경고: 수신된 신호** *signal***가 종료되고 있음 ...**

설명: 신호를 수신했으므로 종료됩니다.

ICA4001 **STOP** *processID*를 **PID로** *program*

설명: 완료된 디먼의 끝을 인쇄합니다. 정보용 메세지입니다.

ICA4002 **임시 ID**

설명: 정보용 메세지입니다.

ICA4003 **하위 프로세스** *processId* **문제.**

설명: 하위 프로세스를 작성할 수 없습니다.

ICA4004 **치명적인 오류. 신호** *signal***에 따라 fwpagerd 종료.**

설명: 신호 처리기입니다.

ICA4005 **fwpagerd 디먼이 실행되지 않음,** *program* **을 찾을 수 없음.**

설명: 디먼이 활성화되지 않았으므로 호출을 전송할 수 없습니다.

ICA4006 **프로세스 ID** *processId*를 **사용하여 실행되는 fwpagerd 디먼이 없음.**

설명: 디먼 프로세스의 프로세스 Id를 찾을 수 없습니다.

ICA4007 **START** *processID*를 **PID**로 *program*

설명: 시작 정보를 인쇄합니다. 정보용 메세지입니다.

ICA4008 **SIGPIPE에 대하여 sigignore**를 설정할 수 없음.

설명: 절단된 파이프 신호를 무시하기 위한 설정을 실패했습니다.

ICA4009 **SIGCHILD에 대한 sigset**를 설정할 수 없음.

설명: 종료 중인 하위 신호를 확보하기 위한 설정을 실패했습니다.

ICA4010 **종료 프로세스를 설정할 수 없음.**

설명: 종료 프로세스를 확보하기 위한 신호 설정을 실패했습니다.

ICA4011 **Socket**을 열 수 없음.

설명: Socket 열기가 실패했습니다.

ICA4012 **SIGTERM에 대한 sigset**를 설정할 수 없음.

설명: SIGTERM & SIGINT 신호를 확보하기 위한 설정을 실패했습니다.

ICA4013 **Socket 재사용 옵션을 설정할 수 없음.**

설명: Socket 재사용 옵션 설정을 실패했습니다.

ICA4014 **Socket 링거 옵션을 설정할 수 없음.**

설명: Socket 링거 옵션 설정을 실패했습니다.

ICA4015 **Socket**을 포트로 바인드할 수 없음.

설명: 포트로 socket 바인드를 실패했습니다.

ICA4016 **Socket 연결대기**를 설정할 수 없음.

설명: Socket 연결대기 설정을 실패했습니다.

ICA4017 **TCP socket** *socket*을 사용하는 서비스 *servName*.

설명: 정보용 메세지입니다.

ICA4018 **함수 호출 select() 실패.**

설명: 내부 함수 호출을 실패했습니다.

ICA4019 **new_work()에서 심각한 오류.**

설명: new_work 루틴에서 심각한 내부를 오류했습니다.

ICA4020 **오류(***program***): 스트림 socket에 쓸 수 없음:** *Socket*

설명: 시스템 오류 가능이 있습니다.

사용자 응답: Socket 상업을 확인하십시오.

ICA4021 **응답 수신 문제.**

설명: 모뎀에서 응답 수신 문제입니다.

사용자 응답: 모뎀 연결 및 초기화 문자열을 확인하십시오.

ICA4022 **요청 성공.**

설명: 정보용 메세지입니다.

ICA4023 **요청 실패.**

설명: 호출 전송 요청이 실패했습니다.

ICA4024 **오류(***program***): 범위 밖 우선순위(***minpri* - *maxpri***).**

설명: 우선순위 범위를 수정하십시오.

사용자 응답: 우선순위 범위를 수정하십시오. 유효한 값은 -1에서 5 사이입니다.

ICA4025 **오류(***program***): -n 옵션을 사용할 때 주소는 ID@carrier 형식이어야 함.**

설명: 잘못된 명령 사용법 구문입니다.

사용자 응답: 올바른 명령 사용법 구문.

ICA4026 오류(*program*): 알 수 없는 호스트 *hostname*.

설명: 호스트명을 해결할 수 없습니다.

사용자 응답: 호스트명을 확인하십시오.

ICA4027 오류(*program*): 스트림 **socket**을 열 수 없음: *errno*

설명: 새로운 socket을 작성할 수 없습니다.

ICA4028 오류(*program*): **socket** 옵션을 설정할 수 없음: *errno*

설명: Socket 링거 옵션을 설정할 수 없습니다.

ICA4029 오류(*program*): *host*에 연결할 수 없음: *errno*.

설명: 호스트에 연결할 수 없습니다.

사용자 응답: 직렬 포트 구성 및 장치 드라이버 파일 존재 여부를 확인하십시오.

ICA4030 오류(*program*): 스트림 **socket**에 쓸 수 없음: *errno*.

설명: 스트림 socket에 쓸 수 없습니다.

ICA4031 응답 수신 문제. 알 수 없는 메세지 조건.

설명: 모뎀에서 응답 수신 문제입니다.

ICA4032 메세지가 대기열에 성공적으로 전송되었음.

설명: 정보용 메세지입니다. 메세지가 대기열에 전송되었습니다.

ICA4033 메세지 실패. 메세지(들)가 전송되지 않음.

설명: 메세지를 호출기 대기열에 전송할 수 없습니다.

ICA4034 *date*이(가) 실패했습니다(*ID* **ID** *priority* 우선 *period* 초 *retryCount*번 시도) *fromEntry personName*: *mesage*.

설명: 호출이 성공적으로 전송되지 못하면 이 메세지를 표시합니다.

ICA4035 재대기행렬 메세지*mesg*을(를) *program*에서 *person*로 할 수 없습니다.

설명: 호출 대기열로 전송할 수 없습니다.

ICA4036 **SUCCEEDED (***ID* **ID** *priority* 우선 *period* 초 *retryCount*번 시도) *fromEntry personName*: *mesage*.

설명: 호출이 성공적으로 전송되며 이 메세지를 표시합니다. 정보용 메세지입니다.

ICA4037 *dumpFile*으(로) 덤프됩니다 (*ID* **ID** *priority*우선 *period* 초 *retryCount*번 시도) *fromEntrypersonName*: *mesage*.

설명: 즉시 전송되지 않는 호출은 나중에 시도하기 위하여 파일로 덤프됩니다.

ICA4038 덤프 파일 *dumpFile*에 쓸 수 없음.

설명: 덤프 파일을 작성할 수 없습니다.

사용자 응답: 시스템 권한을 확인하십시오.

ICA4039 **IpcKey: 0x***IpcKey*

설명: 정보용 메세지입니다.

ICA4040 *retryTime*분의 재시도 시간이 초과되었습니다.

설명: 지정된 분 이후 모뎀 초기화 실패입니다.

사용자 응답: 초기화 문자열을 확인하십시오.

ICA4041 숫자형 호출기에 대하여 영숫자 메세지를 발견했음.

설명: 숫자형 호출기는 영숫자 데이터를 포함할 수 없습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 수정하십시오.

ICA4042 호출을 수신할 수 없음.

설명: 아마도 호출기가 활성화되지 않았습니다.

사용자 응답: 호출기가 활성화되었는지 확인하십시오.

ICA4043 **반송자 *carrier*가 존재하지 않음.**

설명: 지정된 반송자가 존재하지 않습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 수정하십시오.

ICA4044 **반송자 *carrier*에 DTMF 전화번호가 없음.**

설명: 지정된 반송자에 DTMF 전화번호가 없습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 수정하십시오.

ICA4045 **호출기 번호 *pagerNumber*가 반송자의 최대 *carrLen*에 비하여 너무 김.**

설명: 호출기 번호가 반송자의 최대값에 비해 너무 깁니다.

사용자 응답: 반송자의 최대값보다 작은 다른 보다 짧은 호출기 번호를 사용하십시오.

ICA4046 **호출기 번호 *pagerNumber*가 *defaultCarrLen*의 디폴트 길이에 비하여 너무 김.**

설명: 이 메세지는 디폴트 길이가 너무 짧을 때 발생합니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 수정하십시오. 디폴트 길이를 증가시키십시오.

ICA4047 ***ModemfilePathname* 모뎀 파일의 *lineNumber* 라인에 문제가 있습니다.**

설명: 모뎀 정의 파일이 유효하지 않은 문자를 포함합니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 수정하십시오.

ICA4048 **장치 /dev/*deviceName*에서 모뎀을 열 수 없음.**

설명: 지정된 장치에서 모뎀을 열 수 없습니다.

사용자 응답: 직렬 포트를 확인하거나 다시 구성하십시오. 장치를 확인하십시오.

ICA4049 ***deviceName*/dev/에서 모뎀이 열렸습니다.**

설명: 정보용 메세지입니다. 모뎀이 직렬 포트에서 성공적으로 감지되었습니다.

ICA4050 **모뎀 특성을 설정할 수 없음.**

설명: 모뎀 특성 설정 시도를 실패했습니다.

사용자 응답: 모뎀 초기화 문자열을 확인하십시오.

ICA4051 ***numInitTries* 재시도 후 모뎀을 초기화할 수 없음.**

설명: 모뎀을 초기화할 수 없습니다.

사용자 응답: 모뎀 초기화 문자열 및 직렬 포트 구성을 확인하십시오.

ICA4052 **호출기 번호 *pagerNumber*를 다이얼할 수 없음**

설명: 호출기 번호를 다이얼할 수 없습니다.

사용자 응답: 호출기 번호 유효성을 확인하십시오.

ICA4053 **모뎀을 끊을 수 없음.**

설명: 모뎀을 끊을 수 없음.

사용자 응답: 모뎀 초기화 문자열 및 사용된 전화 끊기 명령을 확인하십시오.

ICA4054 **메세지 *message*를 다이얼할 수 없음**

설명: 메세지를 다이얼할 수 없습니다.

ICA4055 ***filename* 모뎀 파일의 *lineNumber* 라인에 문제가 있습니다.**

설명: 잘못된 모뎀 정의 파일입니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 수정하십시오.

ICA4056 ***carrier* 반송자의 DTMF 번호 (*DTMFnumb*)에 다이얼할 수 없습니다.**

설명: DTMF 번호를 변경했거나 해당 반송자에 대하여 유효하지 않습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 수정하십시오.

ICA4057 블록을 전송할 수 없음.

설명: 블록 전송 시도 실패.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4058 전송된 블록에 대한 응답이 없음.

설명: 블록을 전송한 후 반송자로부터 응답을 얻을 수 없습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4059 메세지 전달에 대한 응답을 수신할 수 없음.

설명: 메세지 전달 후 반송자로부터 응답을 얻을 수 없습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4060 호출기 id를 전송할 수 없습니다.

설명: 호출기 id를 전송할 수 없습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 호출기 번호와 반송자 매개변수를 점검하십시오.

ICA4061 자동 모드 요청의 종료 <CR>을 전송할 수 없습니다.

설명: 자동 모드 요청의 종료 <CR>을 전송할 수 없습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4062 자동 모드 요청을 전송할 수 없음.

설명: 자동 모드 요청 신호를 전송할 수 없습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4063 반송자 *carrier*로부터 *numTries* 재시도 후 go-ahead 수신 실패.

설명: 반송자가 현재 통화 중일 수도 있습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검한 다음 다시 시도하십시오.

ICA4064 반송자 *carrier*와의 프롬트동안 통신 오류 발생.

설명: 여러 가지 원인으로 통신 오류가 발생했습니다. 나중에 다시 시도하십시오.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검한 다음 다시 시도하십시오.

ICA4065 로그온 응답을 수신할 수 없음.

설명: 모뎀이 로그온에 대한 응답을 수신할 수 없습니다.

사용자 응답: 모뎀 초기화 문자열 및 반송자 매개변수를 확인하십시오.

ICA4066 반송자 *carrier*가 로그온 시도에 응답하지 않았음.

설명: 반송자가 로그온 시도에 응답하지 않았습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검한 다음 다시 시도하십시오.

ICA4067 *carrier* 반송자가 *receiveDataString*을(를) 나타냅니다.

설명: 반송자가 몇몇 오류 메세지 또는 통화 중 메세지를 전송했습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검한 다음 다시 시도하십시오.

ICA4068 반송자 *carrier*가 로그온 도중 단절을 시행했음.

설명: 반송자가 로그온 도중 단절을 시행했습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4069 반송자 *carrier*에 대한 메세지 덤핑이 *ConnectRetryMax* 재시도 루프에 의해 수행되었음.

설명: 반송자가 통화 중인 경우, 프로그램은 호출을 덤프하고 나중에 시도합니다.

ICA4070 반송자 *carrier*에 대한 메세지 생략이 *maxTotalTries* 세션 연결 시도에 의해 수행되었음.

설명: 재시도 회수 이후 반송자에 접속할 수 없습니다.

사용자 응답: 반송자 매개변수를 확인하고 나중에 다시 시도하십시오.

ICA4071 오류(*program*): 반송자 재시도를 위한 메모리를 할당할 수 없음: *errno*.

설명: 시스템 또는 메모리 할당 오류가 가능합니다.

ICA4072 오류(*program*): 반송자 재시도 리스트에 추가할 수 없음: *errno*.

설명: 아마도 반송자가 존재하지 않을 수도 있습니다.

사용자 응답: 반송자 유효성을 확인하고 다시 시도하십시오.

ICA4073 *phoneNumber*에서 반송자 *carrier*에 대한 데이터 연결이 *retryCount* 재시도 이후 실패했음.

설명: 데이터 연결이 실패했습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 모뎀 연결과 반송자 매개변수를 점검하십시오.

ICA4074 반송자 *carrier*의 ID 프롬트가 *numTries* 재시도 이후 수신되지 않았음.

설명: 반송자가 ID 또는 확인응답 프롬트에 대한 응답에 실패했습니다.

사용자 응답: 반송자가 TeleAlphanumeric 프로토콜을 사용하는지 확인하십시오.

ICA4075 반송자 *carrier*와의 로그온 도중 통신 오류.

설명: 여러 가지 원인으로 통신 오류가 발생할 수 있습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4076 반송자 *carrier*에 대한 최대 로그온 시도가 초과했음.

설명: 반송자가 지정된 시도 회수 이내에 응답하는데 실패했습니다.

사용자 응답: 반송자 매개변수를 확인하고 나중에 다시 시도하십시오.

ICA4077 메세지 **go-ahead**가 반송자 *carrier*로부터 수신되지 않음.

설명: 반송자가 go-ahead 프롬트에 대하여 응답하는데 실패했습니다.

사용자 응답: 반송자 매개변수를 확인하고 나중에 다시 시도하십시오.

ICA4078 블록을 작성할 수 없음.

설명: 반송자가 전송하기 위하여 블록을 작성할 수 없습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4079 반송자 *carrier*가 메세지 전달에 응답하지 않음.

설명: 반송자가 메세지를 전달하는데 문제가 있습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4080 반송자 *carrier*가 메세지 전달 도중 단절을 시행했음.

설명: 반송자가 메세지 전달 도중 단절을 시행했습니다.

사용자 응답: 반송자 매개변수 및 모뎀 초기화 문자열을 확인하십시오.

ICA4081 반송자 *carrier*가 메세지 또는 호출기 **ID**를 거부했음.

설명: 반송자가 호출기 메세지 또는 호출기 id를 거부했습니다.

사용자 응답: 호출기 id, 호출기 활성화 및 반송자 매개변수 유효성을 확인하십시오.

ICA4082 **반송자 *carrier*에 메세지 전달 도중 통신 오류.**

설명: 여러 가지 원인으로 통신 오류가 발생할 수 있습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4083 **반송자 *carrier*로부터 *maxTries* 재시도 후 확인 수신 실패.**

설명: 이 메세지는 반송자가 통화 중이거나 연결을 설정할 수 없는 경우 발생합니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검한 다음 잠시후에 다시 시도하십시오.

ICA4084 **<EOT>를 전송할 수 없음.**

설명: 모뎀이 <EOT>를 전송할 수 없습니다.

사용자 응답: 모뎀 연결 및 초기화 문자열을 확인하십시오.

ICA4085 **<EOT>에 대한 응답을 수신할 수 없음.**

설명: 모뎀이 <EOT>에 대한 응답을 수신할 수 없습니다.

사용자 응답: 모뎀 연결 및 초기화 문자열을 확인하십시오.

ICA4086 **반송자 *carrier*가 <EOT>에 응답하지 않음.**

설명: 반송자가 전송된 데이터에 응답할 수 없습니다.

사용자 응답: 반송자 유효성 및 모뎀 연결을 확인하십시오.

ICA4087 **반송자 *carrier*가 내용상 허용할 수 없는 오류를 가진 데이터로 응답했음.**

설명: 반송자가 전송된 데이터에 응답할 수 없습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 매개변수를 점검하십시오.

ICA4088 **디폴트 파일 *defaultPathname*을 열 수 없음.**

설명: 모뎀 디폴트 파일이 존재하지 않거나 잘못된 권한을 가지고 있습니다.

사용자 응답: 파일이 존재하는지 여부와 권한을 확인하십시오.

ICA4089 **완전하지 않은 디폴트 파일 *defaultPathname*.**

설명: 모뎀 디폴트 파일에 누락된 데이터가 있습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 수정하십시오.

ICA4090 **디폴트 파일 *defaultPathname*의 라인 *lineNumer*에 잘못된 외부 회선 번호.**

설명: 반송자 데이터베이스 파일에 잘못된 외부 회선 번호가 있습니다.

사용자 응답: 반송자 데이터베이스 파일을 지우십시오.

ICA4091 **디폴트 파일 *defaultFile*의 라인 *lineNumber*에 잘못된 보오드율 값.**

설명: 반송자 데이터베이스 파일에 잘못된 보오드율이 있습니다.

사용자 응답: 반송자 데이터베이스 파일을 지우십시오.

ICA4092 **디폴트 파일 *defaultFile*의 라인 *lineNumber*에 잘못된 데이터 비트 값.**

설명: 반송자 데이터베이스 파일에 잘못된 데이터 비트 값이 있습니다.

사용자 응답: 반송자 데이터베이스 파일을 지우십시오.

ICA4093 **디폴트 파일 *defaultFile*의 라인 *lineNumber*에 잘못된 패리티 값.**

설명: 반송자 데이터베이스 파일에 잘못된 패리티 값이 있습니다.

사용자 응답: 반송자 데이터베이스 파일을 지우십시오.

ICA4094 디폴트 파일 *defaultFile*의 라인 *lineNumber*에 잘못된 정지 비트 값.

설명: 반송자 데이터베이스 파일에 잘못된 정지 비트 값이 있습니다.

사용자 응답: 반송자 데이터베이스 파일을 지우십시오.

ICA4095 *defaultFile* 디폴트 파일의 *lineNumber* 라인에 잘못된 태그 *tag id*가 인식되지 않습니다.

설명: 반송자 데이터베이스 파일에 잘못된 태그가 있습니다.

사용자 응답: 반송자 데이터베이스 파일을 지우십시오.

ICA4096 매개변수 수가 잘못되었음.

설명: 정보용 메세지입니다.

ICA4097 오류(*program*): 반송자 리스트를 작성할 수 없음. 메모리 문제.

설명: 시스템 또는 메모리 문제일 가능성이 있습니다.

ICA4098 오류(*program*): 호출 반송자 파일 *carrierFile* 오류.

설명: 반송자 데이터베이스 파일에 몇몇 잘못된 데이터가 있습니다.

사용자 응답: 잘못된 태그가 있는지 반송자 데이터베이스 파일을 확인하십시오.

ICA4099 오류(*program*): IPC 토큰 *errno*을 얻을 수 없음.

ICA4100 오류(*program*): 재시도 리스트를 작성할 수 없음. 메모리 문제 가능.

설명: 시스템 오류 또는 메모리 문제일 가능이 있습니다.

ICA4101 오류(*carrier*): 대기열, **page_q_err**을 작성할 수 없음: *pageQErr*.

ICA4102 오류(*program*): SIGTERM/SIGINT에 대한 신호 캐치를 설정할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4103 오류(*program*): 반송자 *carrier*에 대한 모뎀 특성을 설정할 수 없음.

설명: 모뎀을 설정할 수 없습니다.

사용자 응답: 직렬 포트 구성 및 초기화 문자열을 확인하십시오.

ICA4104 반송자 *carrier*에 대한 *tag* 누락.

설명: 모뎀 정보가 누락되었습니다. 태그는 보오드율, 외부 회선 등등일 수 있습니다.

사용자 응답: 모뎀 구성 파일에서 잘못된 문자가 있는지 확인하십시오.

ICA4105 반송자 *carrier*가 적어도 하나의 전화번호를 나열해야 함.

설명: 반송자가 전화번호를 포함해야 합니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 전화 번호를 추가하십시오.

ICA4106 *CarrierFileName* 파일을 열 수 없습니다.

설명: 반송자 데이터베이스 파일이 존재해야 합니다.

사용자 응답: 아직 없으면 smitty/SMIT 메뉴를 사용하여 파일을 작성하십시오.

ICA4107 *lineNumber* 라인이 너무 깁니다.

설명: 반송자 데이터베이스 파일의 행이 너무 깁니다.

사용자 응답: 잘못된 행이 있는지 반송자 데이터베이스 파일을 확인하십시오.

ICA4108 라인 *lineNumber*에 알 수 없는 태그.

설명: 반송자 데이터베이스 파일에 알 수 없는 태그가 존재합니다.

사용자 응답: 잘못된 태그가 있는지 반송자 데이터베이스 파일을 확인하십시오.

ICA4109 라인 *lineNumber*에 잘못된 시퀀스.

설명: 반송자 데이터베이스 파일에 잘못된 시퀀스가 존재합니다.

사용자 응답: 잘못된 시퀀스가 있는지 반송자 데이터베이스 파일을 확인하십시오.

ICA4110 *carrier* 반송자가 유효하지 않으므로 생략됩니다.

설명: 반송자를 호출 목적으로 사용할 수 없습니다.

사용자 응답: 반송자의 유효성을 확인하십시오.

ICA4111 반송자를 리스트에 추가할 수 없음.

설명: 반송자를 리스트에 추가할 수 없습니다.

사용자 응답: 반송자 유효성 및 전화번호를 확인하십시오.

ICA4112 반송자 이름이 누락되었거나 라인 *lineNumber*가 너무 김.

설명: 반송자 이름이 누락되었습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자를 추가하십시오.

ICA4113 새로운 호출 반송자를 할당할 수 없음: *carrier*.

설명: 반송자를 리스트에 할당할 수 없습니다.

사용자 응답: 반송자 유효성 및 전화번호를 확인하십시오.

ICA4114 라인 *lineNumber*의 값이 너무 김.

설명: 반송자 데이터베이스 파일에서 너무 긴 행이 발견되었습니다.

사용자 응답: 반송자 데이터베이스 파일에서 긴 행을 지우십시오.

ICA4115 라인 *lineNumber*의 중복된 태그 *tag*가 무시됨.

설명: 중복된 태그가 발견되었습니다.

사용자 응답: 반송자 데이터베이스 파일에서 중복된 태그를 삭제하십시오.

ICA4116 라인 *lineNumber*의 값이 존재하지 않음.

설명: 공백 태그가 발견되었습니다.

사용자 응답: smitty/SMIT를 사용하여 빈 필드에 값을 추가하십시오.

ICA4117 값은 라인 *lineNumber*에서 **Y, Yes, N** 또는 **No** 여야 함.

설명: 이 필드는 Y, Yes, N 또는 No 중 하나를 필요로 합니다.

사용자 응답: smitty/SMIT를 사용하여 유효한 데이터를 추가하거나 변경하십시오.

ICA4118 값이 라인 *lineNumber*에서 **0**보다 커야 함.

설명: 이 필드는 양수여야 합니다.

사용자 응답: smitty/SMIT를 사용하여 값을 양수로 변경하십시오.

ICA4119 라인 *lineNumber*의 값이 잘못되었음.

설명: 지정된 행에서 잘못된 값이 발견되었습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 값을 변경하십시오.

ICA4120 *name* 반송자가 유효하지 않으므로 생략됩니다.

설명: 잘못된 반송자가 발견되었습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 유효한 반송자를 추가하십시오.

ICA4121 반송자를 리스트에 추가할 수 없음.

설명: 반송자를 호출 리스트에 추가할 수 없습니다.

사용자 응답: 반송자 유효성을 확인하십시오.

ICA4122 라인 *lineNumber*의 중복된 태그 *tag*가 무시됨.

설명: 반송자 스탠자에서 중복된 태그가 발견되었습니다.

사용자 응답: 중복된 값을 포함하는 반송자 스탠자를 지우십시오.

ICA4123 오류(*program*): **IPC** 토큰을 얻을 수 없음 : *errNo*

설명: 프로그램이 IPC 토큰을 얻을 수 없습니다.

ICA4124 오류(*program*): 대기열 읽기 도중 오류 *pageqErr*.

설명: 프로그램이 대기열을 읽을 수 없습니다.

ICA4125 *count* 대기열 항목.

설명: 정보용 메세지입니다.

ICA4126 **ID** *id*를 가진 메세지가 삭제되었음.

설명: 정보용 메세지입니다.

ICA4127 대기열에 **ID** *id*가 없음.

설명: 정보용 메세지입니다.

ICA4128 오류(*program*): **ID** *id* 삭제 시도 중 오류 *pageqErr*.

설명: 큐의 ID 삭제가 시도되었습니다.

ICA4129 **Key**는 *entryKey*이며 내용은 @ *ptr*: *ptr*입니다.

설명: 정보용 메세지에 불과합니다.

ICA4130 모뎀 특성:

설명: 모뎀 초기화 정보입니다.

ICA4131 이름: *modemName*

설명: 모뎀 초기화 정보입니다.

ICA4132 초기화 문자열: *initString*

설명: 모뎀 초기화 정보입니다.

ICA4133 명령 모드: *command*

설명: 모뎀 초기화 정보입니다.

ICA4134 명령 종료 : **0x***terminator*

설명: 모뎀 초기화 정보입니다.

ICA4135 다이얼: *dial*

설명: 모뎀 초기화 정보입니다.

ICA4136 다이얼 일시 정지: *pause*

설명: 모뎀 초기화 정보입니다.

ICA4137 다이얼 #: *diallb*

설명: 모뎀 초기화 정보입니다.

ICA4138 다이얼 *: *dialstar*

설명: 모뎀 초기화 정보입니다.

ICA4139 전화끊기 명령: *hangup*

설명: 모뎀 초기화 정보입니다.

ICA4140 유효한 명령 응답: *validCommandresp*

설명: 모뎀 초기화 정보입니다.

ICA4141 유효한 연결: *validConnect*

설명: 모뎀 초기화 정보입니다.

ICA4142 반향: *echo*

설명: 모뎀 초기화 정보입니다.

ICA4143 모뎀 디버그 레코드: **PUTS(***id***) txd->** *outStr*

설명: 모뎀 handshaking 정보입니다.

ICA4144 모뎀 디버그 레코드: **PUTC(***id***) txd->** *outStr*

설명: 모뎀 handshaking 정보입니다.

ICA4145 모뎀 디버그 기록: **GET rxd->** *record id*

설명: 모뎀 handshaking 정보입니다.

ICA4146 모뎀 디버그 레코드: **INPUT(***record id*

설명: 모뎀 handshaking 정보입니다.

ICA4147 모뎀 디버그 레코드: **) rxd->**

설명: 모뎀 handshaking 정보입니다.

ICA4148 모뎀 디버그 레코드: **WAITFOR(***record id*

설명: 모뎀 handshaking 정보입니다.

ICA4149 하위 신호를 블록 해제할 수 없음.

설명: SIGCHLD 신호를 블록 해제하십시오.

ICA4150 하위 신호를 블록화할 수 없음.

설명: SIGCHLD 신호를 블록화하십시오.

ICA4151 웜시동 파일 *filePathname*이 존재하지 않음.

설명: 정보용 메세지입니다.

ICA4152 웜시동 파일 *filePathname*을 열 수 없음.

설명: 정보용 메세지입니다.

ICA4153 웜시동 파일 *filePathname*의 행이 너무 김.

설명: 웜시동 파일이 몇몇 잘못된 문자를 포함합니다.

ICA4154 웜시동 파일 *filePathname*에 사용되지 않는 데이터가 있음.

설명: 정보용 메세지입니다.

ICA4155 *filePathname* 웜시동 파일이 비어있습니다.

설명: 정보용 메세지입니다.

ICA4156 *filePathname* 웜시동 파일의 *lineNumber* 라인에 잘못된 주소 *address*이(가) 있으며 무시됩니다.

설명: 웜시동 파일에 몇몇 잘못된 문자가 있습니다. 정보용 메세지입니다.

ICA4157 웜시동 파일 *filePathname*의 라인 *lineNumber*에 잘못된 형식이 있으므로, 무시됨.

설명: 웜시동 파일에 몇몇 잘못된 문자가 있습니다. 정보용 메세지입니다.

ICA4158 웜시동 파일 *filePathname*의 라인 *lineNumber*에 메세지가 없으므로, 무시됨.

설명: 웜시동 파일에 메세지가 없습니다. 정보용 메세지입니다.

ICA4159 웜시동 파일 *filePathname*의 라인 *lineNumber* 대기 오류, 무시됨.

설명: 웜시동 파일에 몇몇 잘못된 문자가 있습니다. 정보용 메세지입니다.

ICA4160 *filePathname* 파일의 *count* 메세지가 완료됩니다.

설명: 정보용 메세지입니다.

ICA4161 오류(*program*): 너무 많은 연속 하위 오류.

설명: 너무 많은 연속적인 하위 오류. 이것은 반송자나 모뎀 정의 파일에 몇몇 잘못된 문자가 있는 경우 발생합니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 데이터베이스 파일과 모뎀 정의 파일을 점검하십시오.

ICA4162 하위는 *program*을(를) **exec**할 수 없습니다. : *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4163 오류(*errno*): 하위에서 하위를 분기할 수 없음. *program name*.

설명: 시스템 오류 가능이 있습니다.

ICA4164 호출 반송자 리스트를 작성할 수 없음.

설명: 내부 프로그램 오류입니다.

ICA4165 호출 반송자 파일 오류 *carrierFile* 오류.

설명: 반송자 데이터베이스에 몇몇 잘못된 데이터가 들어 있습니다.

사용자 응답: smitty/SMIT 메뉴를 사용하여 반송자 데이터베이스 파일을 점검하십시오.

ICA4166 정보용 메세지입니다. IPC 키는 : 0x*IpcKey*입니다.

설명: 정보용 메세지입니다.

ICA4167 대기열, page_q_err을 작성할 수 없음: *pageQerr*.

설명: 대기열 작성 시도가 실패했습니다.

ICA4168 호출 웜시동 파일이 시(*time*)에 작성되었습니다.

설명: 정보용 메세지입니다.

ICA4169 *objfrom message*의 *priority numPager*우선순위-p

설명: 정보용 메세지입니다.

ICA4170 *frommessage*에서 *alpaPager@carrier priority* 우선순위-p

설명: 정보용 메세지입니다.

ICA4171 **priority -p** *priority* **-n** *numPager@carrier* **from** *from message*

설명: 정보용 메세지입니다.

ICA4172 호출기 웜시동 파일 끝.

설명: 정보용 메세지입니다. 메세지의 끝을 나타냅니다.

ICA4173 웜시동 파일 *warmstrtFile*에 쓸 수 없음.

설명: 웜시동 파일이 존재하지 않을 수도 있습니다.

ICA4174 *user@ host*에서 *time* STATUS-REQUEST

설명: 상태 요구 정보를 표시합니다.

ICA4175 *user@ host*에서 *time* SUMMARY-REQUEST

설명: 요약 요구 정보를 표시합니다.

ICA4176 대기열 항목 *count*.

설명: 호출기 대기열의 대기열 항목 수를 계산합니다.

ICA4177 가장 오래된 항목: *time*에 ID *id* 수신.

설명: 대기열의 가장 오래된 항목을 표시합니다.

ICA4178 확장 후 재접속 메모리 실패.

설명: 시스템 오류 가능이 있습니다.

ICA4179 확장 후 재접속 메모리 정렬 실패.

설명: 시스템 오류 가능이 있습니다.

ICA4180 page_q_print()에서 PAGE_Q 세마포어를 다운로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4181 page_q_print()에서 PAGE_Q 세마포어를 업로드할 수 없음. *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4182 링크 *headLink* -> 메세지 ID: *id*.

설명: 정보용 메세지입니다.

ICA4183 우선순위: *priority*.

설명: 정보용 메세지입니다.

ICA4184 이름: *name*.

설명: 정보용 메세지입니다.

ICA4185 반송자: *carrier*.

설명: 정보용 메세지입니다.

ICA4186 메세지: *message*.

설명: 정보용 메세지입니다.

ICA4187 공유 **RAM**을 가져올 수 없음. *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4188 공유 **RAM**에 접속할 수 없음. *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4189 **PAGE_Q** 세마포어를 가져올 수 없음.

설명: 시스템 오류 가능이 있습니다.

ICA4190 **page_q_create()**에서 **PAGE_Q** 세마포어를 초기화할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4191 **page_q_create()**에서 **PAGE_Q** 세마포어를 설정할 수 없음. *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4192 **page_q_empty()**에서 **PAGE_Q** 세마포어를 다운로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4193 **page_q_empty()**에서 **PAGE_Q** 세마포어를 업로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4194 **page_q_enq(***name,message***)**에서 **PAGE_Q** 세마포어를 다운로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4195 **page_q_enq()**에서 **PAGE_Q** 세마포어를 업로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4196 **page_q_enq(): ID(***id***)** 우선순위**(***priority***)** 이름**(***name***)** 메세지**(***message*.

설명: 정보용 메세지입니다.

ICA4197 **page_q_head()**에서 **PAGE_Q** 세마포어를 다운로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4198 **page_q_head()**에서 **PAGE_Q** 세마포어를 업로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4199 **page_q_first()**에서 **PAGE_Q** 세마포어를 다운로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4200 **page_q_first()**에서 **PAGE_Q** 세마포어를 업로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4201 **page_q_next()**에서 **PAGE_Q** 세마포어를 다운로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4202 **page_q_ next()**에서 **PAGE_Q** 세마포어를 업로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4203 **page_q_tail()**에서 **PAGE_Q** 세마포어를 다운로드할 수 없음: *errno*.

설명: 시스템 오류 가능이 있습니다.

ICA4204 **page_q_tail()에서 PAGE_Q 세마포어를 업로드할 수 없음: *errno*.**

설명: 시스템 오류 가능이 있습니다.

ICA4205 **page_q_del()에서 PAGE_Q 세마포어를 다운로드할 수 없음: *errno*.**

설명: 시스템 오류 가능이 있습니다.

ICA4206 **page_q_del()에서 PAGE_Q 세마포어를 업로드할 수 없음: *errno*.**

설명: 시스템 오류 가능이 있습니다.

ICA4207 **page_q_del(*ID*).**

설명: 디버그 정보입니다.

ICA4208 **page_q_deq()에서 PAGE_Q 세마포어를 다운로드할 수 없음: *errno*.**

설명: 시스템 오류 가능이 있습니다.

ICA4209 **page_q_deq()에서 PAGE_Q 세마포어를 업로드할 수 없음: *errno*.**

설명: 시스템 오류 가능이 있습니다.

ICA4210 **page_q_del(): ID(*id*) 우선순위(*priority*) 이름(*name*) 메세지(*message*).**

설명: 정보용 메세지입니다.

ICA4211 **page_q_walk()에서 PAGE_Q 세마포어를 다운로드할 수 없음: *errno*.**

설명: 시스템 오류 가능이 있습니다.

ICA4212 **page_q_walk()에서 PAGE_Q 세마포어를 업로드할 수 없음: *errno*.**

설명: 시스템 오류 가능이 있습니다.

ICA4213 **PAGE_Q가 가득 참.**

설명: 호출 대기열이 가득찼습니다.

사용자 응답: 잠시후에 해당 호출 내용을 전송하십시오.

ICA4300 **전화를 끊는 중.**

설명: 전화를 끊는 중입니다.

ICA4301 **모뎀 초기화 중...**

설명: 초기화 문자열을 사용하여 모뎀을 초기화 중입니다.

ICA4302 **다이얼 중 .....**

설명: 전화번호를 다이얼 중입니다.

ICA4303 **연결 대기 중.**

설명: 모뎀 연결을 대기 중입니다.

ICA4304 **CONNECTED** *speed*

설명: peedbaud 율에 연결

ICA4305 **연결되었음!!!!!!!**

설명: 호출기 서비스 제공자에 연결되었습니다.

ICA4306 **자동 모드에 대한 프롬트 요청 중.**

설명: 자동 모드에 대한 프롬트를 요청 중입니다. ″ID=″ 대기 중

ICA4307 **프롬트 OK.....**

설명: 제공자로부터 ″ID=″가 다시 표시되었습니다.

ICA4308 **자동 모드 요청 전송 중.**

설명: ID 및 SST를 호출기 서비스 제공자에게 전송 중입니다.

ICA4309 **자동 모드 요청 전송 .....OK!**

설명: 복귀 완료. 통신이 성공했음을 의미합니다.

ICA4310 **메세지 전송 중**

설명: 메세지 블록을 전송 중입니다.

ICA4311 **결과 대기 중**

설명: 확약을 대기 중입니다.

ICA4312 **Ack 수신. 호출 성공**

ICA4313 **Nak를 수신했음, 블록을 재전송하십시오. *NakTries*시도**

설명: Nak를 수신했음. 호출기 제공자가 재전송을 요구 중입니다.

ICA4314 **트랜잭션 오류. 블록을 재전송하십시오. *RsTries*시도**

설명: 트랜잭션 오류. 블록을 재전송 중입니다.

ICA4315 **반송자 연결 종료.**

설명: 호출기 제공자가 대화를 종료했습니다. 문제점에 대해 제공자에게 문의하십시오.

ICA4350 **fwpage arrier="..."odem="..."D="..." sg="..."h/msgtext>**

설명: fwpage 사용법. 매개변수를 확인하고 다시 시도하십시오.

ICA4351 ***This* 파일이 없습니다**

설명: 파일이 올바른 디렉토리 밑에 있는지 보려면 파일을 확인하십시오. 이 코드를 사용하려면 carriers.cfg, modems.cfg 및 pager.cfg를 작성해야 합니다.

ICA4352 ***What* 파일이 손상됨**

설명: 파일을 사용자가 수정했으며 스탠자 형식이 아닙니다. 모든 속성은 GUI를 통하여 입력해야 합니다.

ICA4353 ***What*이 너무 깁니다, 줄여서 다시 시도하십시오.**

설명: hat이 너무 깁니다. 줄이고 다시 시도하십시오.

ICA4354 ***What* 잘못.**

설명: 보오드율이 잘못된 경우 유효한 옵션은 600, 1200, 2400, 4800, 9600, 14400입니다. 바이트당 데이터 비트가 잘못된 경우 유효한 옵션은 7, 8입니다. 정지 비트가 잘못된 경우 유효한 옵션은 1,2입니다. 아웃라인 접두어가 잘못된 경우 입력은 숫자로만 이루어져야 합니다. 호출 방법이 틀린 경우, TAP만이 이 버전에서 지원됩니다. 호출기 ID 오류인 경우, 모두 숫자인지 확인하십시오. 패리티가 틀린 경우, 유효한 옵션은 O(홀수), E(짝수), N(없음), S(공백), M(마크)입니다. COM 포트가 틀린 경우, 유효한 옵션은 COM1, COM2 ...입니다. COM 포트는 이 버전에서 10보다 작아야 합니다. 메세지 문자가 틀린 경우, 특수 문자가 있는지 메세지를 확인하십시오.

ICA4355 ***where* 오류에 매개변수를 설정하십시오.**

설명: here에 매개변수를 설정할 수 없습니다. 매개변수를 확인하고 다시 시도하십시오.

ICA4356 ***When*에서, COM 포트 읽기 오류.**

설명: COM 포트 읽기 오류입니다. 모뎀 반향을 설정하고 다시 시도하십시오.

ICA4357 ***Where*에서, COM 포트 쓰기 오류.**

설명: COM 포트 쓰기 오류.

ICA4358 ***What* 설정 오류.**

설명: haterror 설정. 로그 파일을 확인하고 오류를 해결하십시오.

ICA4359 **Max 시도가 *Where*을(를) 초과했습니다. 프로그램 중단 중.....**

설명: com 포트를 60분에 60회 열어 보십시오. 모두 실패했습니다. 이 경우 하드웨어 연결을 점검하십시오. 호출 메세지를 10분에 10회 전송해 보십시오. 모두 실패했습니다. 호출 제공자가 다운되었을 수 있습니다.

ICA4360 **반송자 전화번호에 알 수 없는 문자: **pCarrierPhoneNum***

설명: 반송자 전화번호에 인식되지 않는 문자가 발견되었습니다. 숫자를 확인하고 다시 시도하십시오.

ICA4361 **경고!!! 호출 제공자의 모뎀이 일반적으로 2400 미만이어야 합니다.**

설명: 이것은 단지 경고일뿐입니다. 호출 제공자의 모뎀 속도는 일반적으로 2400 미만으로 설정됩니다.

ICA4362 **모뎀을 초기화할 수 없음.**

설명: 모뎀 초기화 문자열을 변경하고 다시 시도하십시오.

ICA4363 **모뎀이 오류를 리턴했습니다.**

설명: 모뎀 통신 오류

ICA4364 **Com 포트 열기 *tries* try 오류. 1분내에 재시도**

설명: com 포트 열기 오류. 아마도 다른 프로그램에서 사용 중입니다. 자동으로 1분내에 다시 시도합니다.

ICA4365 ***tries* 시도에서 호출 전송 실패. 1분내에 재시도.**

설명: 호출 전송 실패. 정확한 원인을 알려면 로그 파일을 확인하십시오.

ICA4366 **메세지가 너무 길어서, 잘림.**

설명: 단지 경고일뿐입니다. 메세지 길이가 너무 깁니다. 알맞게 자르십시오.

ICA4367 **내부 정의 값으로 최대 메세지 길이 재설정: *msg-length***

설명: 사용자 정의 메세지 길이가 80으로 정의된 내부 정의 값보다 크므로, 최대 메세지 길이를 디폴트 길이로 재설정하십시오.

ICA4368 **조치: *Where* 오류**

설명: COM 포트 열기 오류의 경우, 구성을 확인하고 다시 시도하십시오. COM 처리 닫기 오류의 경우, 시스템 문제입니다. COM 퍼지 오류의 경우, 시스템 문제입니다. 다이얼 명령 전송 오류인 경우, 다이얼 명령 문제입니다. Haye 호환 모뎀인지 확인하십시오. 전송 ID 요청 오류인 경우 호출기 제공자가 TAP 프로토콜을 지원하는지 점검하십시오. 자동 프롬트 전송 오류인 경우, 호출기 서비스가 제대로 작동하는지 확인하십시오. 메세지 전송 오류인 경우, 로그 파일을 확인하여 실패 원인을 해결하십시오. 프롬트 오류인 경우, 호출기 제공자로부터 프롬트를 다시 얻을 수 없습니다.

ICA4369 **트랜잭션 오류가 너무 많음. 중단합니다 ....**

설명: 트랜잭션 오류가 너무 많으므로, 이 시도를 중단합니다.

ICA4370 **너무 많은 Nak가 수신되었으므로, 프로그램을 중단합니다 .....**

설명: 호출기 제공자로부터 너무 많은 Nak가 수신되었으므로, 이 시도를 중단합니다.

ICA4371 **함수 *FunctionName*을 사용하여 COM 포트에서 *szComPort*가 *Error Number*를 전송했음**

설명: 매개변수를 확인하고 다시 시도하십시오.

ICA4372 **모뎀이 오류 메세지를 전송했습니다. .....** ***ReturnMessage***

설명: 메세지는 다음과 같습니다. 연결되지 않았습니다. 벨은 울리나 연결되지 않았습니다. 반송자가 없습니다. 다이얼톤이 없습니다. 통화 중입니다. 응답이 없습니다.

ICA4373 **(*function name*) 모뎀 또는 반송자로부터 알 수 없는 응답이 제공되었음. *char1*, *char2*.**

설명: 이 메세지는 Firewall의 호출 기능이 인식하지 못하는 모뎀이나 반송자로부터 온 응답을 보고합니다. char1 및 char2는 응답의 처음 2문자에 대한 ascii(hex) 코드를 나타냅니다.

사용자 응답: 모뎀 지침이나 반송자를 검토하여 알 수 없는 응답의 의미를 이해할 때는 이 정보를 사용하십시오.

ICA5005 **SKIT 초기화에 실패했습니다. 리턴 코드는 *return code*임.**

설명: 보안 socket 초기화가 실패했습니다. SKIT로부터 리턴 코드가 표시됩니다.

ICA5014 원격 클라이언트 터널 서버가 포트 *server port #*와의 연결을 대기하고 있음.

설명: sslrctd에 대해 구성된 포트 번호가 표시됩니다.

ICA5015 *chp0.chp1.chp2.chp3*에서의 연결 수용

설명: 클라이언트의 IP 주소가 표시됩니다.

ICA5017 보안 **socket**을 확보할 수 없음. 함수 **skit_secure_soc_init retcode**는 *function retcode*.

설명: skit_secure_soc_init()가 실패했으므로, 보안 socket을 확보할 수 없습니다.

ICA5018 사용된 수신**(slave)** 서버 **cipher** 스펙은 *spec1 spec2 spec3*.

설명: Cihper 스펙이 표시됩니다.

ICA5019 **Free Homenet IP** 풀을 확보할 수 없음.

설명: 동적 필터 문제점.

ICA5020 원격 클라이언트 구성 파일을 열 수 없음.

설명: 파일 /etc/security/rcsfile.cfg를 사용할 수 없습니다.

사용자 응답: 파일 표시와 그 내용을 점검하십시오.

ICA5021 '*keyword*' 키워드가 없습니다.

설명: 파일 /etc/security/rcsfile.cfg에 해당 키워드가 없습니다.

사용자 응답: /etc/security/rcsfile.cfg를 점검한 후 정정하십시오.

ICA5024 *routine name*에서 함수 **skit_secure_soc_write()** 오류.

설명: 이 루틴에서 skit_secure_soc_write()가 실패했습니다.

ICA5025 **ACKClient()**에서 함수 **skit_secure_soc_write()** 오류.

설명: ACKClient() 루틴에서 skit_secure_soc_write()가 실패했습니다.

ICA5026 *routine name*에서 클라이언트로부터 유효하지 않은 리턴 코드를 수신했음.

설명: 이 루틴의 클라이언트로부터 예기치못한 리턴 코드를 수신했습니다.

ICA5027 *routine name*에서 클라이언트로부터 틀린 요청에 대한 리턴 코드를 수신했음.

설명: 이 루틴에서 리턴 코드 메세지의 요청 코드를 예기치 못했습니다.

ICA5028 잘못된 로그인 요청.

설명: 로그인 요청 메세지의 형식이 유효하지 않습니다.

ICA5030 알 수 없는 원격 클라이언트 **ID**. *remote client ID*

설명: Firewall 시스템에서는 이 시스템 ID를 알 수 없습니다.

사용자 응답: 이 원격 클라이언트에 대한 사용자 정보를 정정하십시오.

ICA5031 함수 **skit_secure_soc_write** 오류가 **RCTLoginPhase**에서 발견되었음.

설명: 로그인 페이즈에 대해 skit_secure_soc_write()가 실패했습니다.

ICA5035 유효하지 않은 로그아웃 요청.

설명: 로그아웃 요청 메세지의 형식이 유효하지 않습니다.

ICA5067 유효하지 않은 패킷이 수신되었음.

설명: 수신된 패킷 형식이 유효하지 않습니다.

ICA5078 **SvrReqHandler()**에서 인식되지 않는 요청이 확보되었음.

설명: 인식되지 않은 요청이 수신되어 무시됩니다.

ICA5082 *remote client ID* **클라이언트에 대한 터널이 단절되었습니다.**

설명: 이 ID를 갖는 원격 클라이언트에 대한 터널이 단절되었습니다.

ICA5086 *userid* **ID가 정의되었습니다.**

설명: Firewall 시스템에 이 사용자 ID가 없습니다.

ICA5087 **'***userid***'에 대한 사용자 확인이 실패했습니다.**

설명: 이 사용자 ID에 대한 사용자 확인이 실패했습니다.

ICA5089 **함수 rcFilterClear()가 실패했음. 리턴 코드는** *return code***입니다.**

설명: 이 리턴 코드로 rcFilterClear()가 실패했습니다.

사용자 응답: IPSEC LAN 클라이언트 존재를 점검하십시오. 이러한 제품은 공존할 수 없습니다.

ICA5090 **함수 rcFilterInit()가 실패했습니다. 리턴 코드는** *return code***입니다**

설명: 이 리턴 코드로 rcFilterInit()가 실패했습니다.

ICA5091 **함수 TunnelUp()이 실행 가능한 파일** *command line***을 실행할 수 없음.**

설명: 표시된 명령 행에서 system() 호출에 실패했습니다.

ICA5092 **recoverstash 함수 호출로부터 키링 암호를 확보할 수 없음.**

설명: stash 파일에서 키링 암호를 복구할 수 없습니다.

ICA8001 **SYSLOG/udp: 알 수 없는 서비스**

ICA8002 *function_name* **기능이 실패했습니다 -** *errno*, **errno2 = 0x***errno2*

설명: syslogd가 지정된 기능을 수행할 수 없으므로 처리가 중단됩니다. errno 정보가 오류 메세지 뒤에 추가됩니다.

사용자 응답: 시스템 프로그래머에게 연락하십시오. 시스템 프로그래머 :errno 정보를 사용하여 실패의 원인을 판별하십시오.

ICA8004 **AF_INET socket에서 오류가 발견되었음. [ ]slogd는 더 이상 Socket을 모니터하지 않음.**

ICA8006 **알 수 없는 우선순위 이름** *\"priority\"*

설명: 구성 파일에서 발견된 우선순위 이름이 유효하지 않습니다.

사용자 응답: 시스템 프로그래머에게 연락하십시오. 시스템 프로그래머 :구성 파일을 확인해 보십시오.

ICA8007 **알 수 없는 기능 이름** *\"facility\"*

설명: 구성 파일에서 발견된 기능 이름이 유효하지 않습니다.

사용자 응답: 시스템 프로그래머에게 연락하십시오. 시스템 프로그래머 :구성 파일을 확인해 보십시오.

ICA8008 **%2$.24s의 SYSLOG@***hostname***에서 \bMessage ...**

설명: syslog 디먼 구성 파일에 모든 로그온 사용자에게 syslog 메세지를 송신할 항목이 들어 있습니다. 이 메세지는 현재 syslog 디먼이 실행되고 있는 시스템에 로그온 한 모든 사용자들에게 송신됩니다.

사용자 응답: 시스템 프로그래머 없음 :없음

ICA8009 *signal***신호에 있는 SYSLOGD**

설명: syslog 디먼이 syslog 디먼을 종료시킨 신호를 수신하였습니다.

사용자 응답: 시스템 프로그래머 없음 :없음

ICA8010 **SYSLOGD가 재시작됨.**

ICA8012 **SYSLOGD이 SMF로 기록할 수 없습니다 -** *error_text*

설명: 레코드를 SMF로 기록하는 중에 오류가 발생했습니다. 오류 텍스트 정보가 오류 메세지 뒤에 추가됩니다.

사용자 응답: 시스템 프로그래머에게 연락하십시오. 시스템 프로그래머 :오류 텍스트 정보를 사용하여 SMF 기록 실패의 원인을 판별하십시오.

ICA8013 프로세스 상태 갱신에 실패했습니다. 리턴 코드 = **0x***return_code*

설명: Firewall 커널 프로세스에 대한 syslogd 프로세스의 상태를 갱신하려고 시도하는 중에 오류가 발생했습니다. 리턴 코드를 사용하여 갱신 프로세스 상태 호출로부터 리턴된 특정 오류를 대략 판별할 수 있습니다.

사용자 응답: 시스템 프로그래머에게 연락하십시오. 시스템 프로그래머 :서비스 담당자에게 연락하십시오.

ICA8014 SYSLOGD 호출에 지정된 알 수 없는 옵션 (*-startup_option*)

설명: syslogd 디먼 프로세스를 시작하려고 하는 중에 오류가 발생했습니다. 지정된 옵션이 syslogd 호출에서 지원되지 않는 것입니다.

사용자 응답: 시작 옵션을 확인하고 syslogd 디먼을 재시작 하십시오. 시스템 프로그래머 :문제가 계속되면 서비스 담당자에게 연락하십시오.

ICA8015 구성 파일 항목(*config_data*)이 유효하지 않습니다

설명: SYSLOG 구성 파일로부터 구성 항목을 분석(parse)하려고 하는 중에 오류가 발생했습니다.

사용자 응답: 구성 파일 항목을 확인하고 syslogd 디먼을 재시작 하십시오. 시스템 프로그래머 :문제가 계속되면 서비스 담당자에게 연락하십시오.

ICA8016 *function_name*이(가) *filename*에 대해 실패했습니다 - *errno*

설명: 지정된 장치에 대하여 지정된 기능을 수행하려고 하는 중에 오류가 발생했습니다. errno 정보가 오류 메세지 뒤에 추가됩니다.

사용자 응답: 지정된 장치가 존재하는지 확인한 후 요구된 내용을 다시 시도해 보십시오. 문제가 계속되면 시스템 프로그래머에게 문의하십시오. 시스템 프로그래머 :문제가 계속되면 서비스 담당자에게 연락하십시오.

ICA8050 *function*이(가) 실패했습니다. *error_text*

설명: 메세지에 표시된 함수를 실행하는 중에 오류를 만났습니다. 오류가 대한 추가 정보는 오류 텍스트에서 제공합니다.

사용자 응답: 메세지에 지정된 오류를 정정하고 필요에 따라 조작을 재시도하십시오.

ICA8051 *function*이 실패했습니다: 리턴 코드 = **0x***return_code*

설명: 메세지에 표시된 함수를 실행하는 중에 오류를 만났습니다. 지정된 함수의 리턴 코드도 표시됩니다.

사용자 응답: 메세지에 지정된 오류를 정정하고 필요에 따라 조작을 재시도하십시오.

ICA8052 FWSTACKD가 *stack_name*에 대해 필터 로깅을 활성화함.

설명: FWSTACKD는 패킷 필터 로깅을 시도 중입니다.

시스템 조치: 프로그램이 계속 진행됩니다.

ICA8053 FWSTACKD가 *stack_name*에 대해 필터 로깅을 활성화하지 못했습니다. *error_text*

설명: 패킷 필터 로깅은 첨부된 오류 메세지에서 설명된 이유로 활성화되지 못했습니다.

시스템 조치: 필터 로깅은 수행되지 않습니다.

사용자 응답: 오류 메세지를 사용하여 오류를 정정하고 **fwfilter cmd=startlog**로 필터 로깅을 재활성화시키십시오.

ICA8054 FWSTACKD가 *stack_name*에 대해 NAT 로깅을 활성화함.

설명: FWSTACKD는 네트워크 주소 변환 (NAT) 로깅을 활성화하려고 합니다.

시스템 조치: 프로그램이 계속 진행됩니다.

ICA8055 FWSTACKD가 *stack_name*에 대해 NAT 로깅을 활성화하지 못했습니다. *error_text*

설명: 네트워크 주소 변환 (NAT) 로깅은 첨부된 오류 메세지에서 설명된 이유로 활성화되지 못했습니다.

시스템 조치: 네트워크 주소 변환 로깅은 수행되지 않습니다.

사용자 응답: 오류 메세지를 사용하여 오류를 정정하고 **fwnat cmd=startlog**로 네트워크 주소 변환 로깅을 재활성화시키십시오.

ICA8056 **FWSTACKD가 *stack_name*에 대해 NAT를 활성화함.**

설명: FWSTACKD는 네트워크 주소 변환 (NAT)을 활성화하려고 합니다.

시스템 조치: 프로그램이 계속 진행됩니다.

ICA8057 **FWSTACKD가 *stack_name*에 대해 NAT을 활성화하지 못했습니다.** *error_text*

설명: 네트워크 주소 변환 (NAT)은 첨부된 오류 메세지에서 설명된 이유로 활성화되지 못했습니다.

시스템 조치: 네트워크 주소 변환은 수행되지 않습니다.

사용자 응답: 오류 메세지를 사용하여 오류를 정정하고 **fwnat cmd=update**로 네트워크 주소 변환을 재활성화시키십시오.

ICA8058 **FWSTACKD가 *stack_name*에 대한 터널 정의를 재활성화하고 있음.**

설명: FWSTACKD는 시스템이 중단되었을 때에 활성화 상태에 있었던 터널 정의를 재활성화하려고 합니다.

시스템 조치: 프로그램이 계속 진행됩니다.

ICA8059 **FWSTACKD가 *stack_name*에 대한 터널 정의를 재활성화할 수 없습니다.** *error_text*

설명: 터널 정의는 첨부된 오류 메세지에서 설명된 이유로 활성화되지 못했습니다.

시스템 조치: 터널 정의는 활성화되지 않습니다.

사용자 응답: 오류 메세지를 사용하여 오류를 정정하고 **fwtunnl cmd=activate**로 터널 정의를 재활성화시키십시오.

ICA8060 **FWSTACKD가 *stack_name*에 대한 필터 및 Socks 규칙을 활성화함.**

설명: FWSTACKD는 현 패킷 필터 규칙 및 Socks 규칙 세트를 활성화하려고 합니다.

시스템 조치: 프로그램이 계속 진행됩니다.

ICA8061 **FWSTACKD가 *stack_name*에 대한 필터 및 Socks 규칙을 활성화 할 수 없습니다.** *error_text*

설명: 필터 규칙 및 Socks 규칙은 첨부된 오류 메세지에서 설명된 이유로 활성화되지 못했습니다.

시스템 조치: 디폴트 필터 규칙이 적용됩니다. 로컬 액세스는 허용되며 다른 모든 액세스는 거부됩니다.

사용자 응답: 오류 메세지를 사용하여 오류를 정정하고 **fwfilter cmd=update**로 필터 및 Socks 규칙을 재활성화시키십시오.

ICA8062 **FWSTACKD가 *stack_name*에 대해 RealAudio 지원을 활성화함.**

설명: FWSTACKD는 RealAudio 지원을 활성화하려고 합니다.

시스템 조치: 프로그램이 계속 진행됩니다.

ICA8063 **FWSTACKD가 *stack_name*에 대해 RealAudio 지원을 활성화할 수 없습니다.** *error_text*

설명: RealAudio 지원은 첨부된 오류 메세지에서 설명된 이유로 활성화되지 못했습니다.

시스템 조치: RealAudio 서비스를 사용할 수 없습니다.

사용자 응답: 오류 메세지를 사용하여 오류를 식별하고 오류를 정정한 후 **fwaudio cmd=change**로 RealAudio를 재활성화시키십시오.

ICA8064 ***function*이(가) 실패했습니다.** *error_text*

설명: 메세지에 표시된 함수를 실행하는 중에 오류를 만났습니다. 오류가 대한 추가 정보는 오류 텍스트에서 제공합니다.

사용자 응답: 메세지에 지정된 오류를 정정하고 필요에 따라 조작을 재시도하십시오.

ICA9000 **IBM Firewall 평가가 일(*date*) 이내에 만료됨.**

설명: 이 소프트웨어는 평가 사본으로 브랜드되었으며 표시된 대로 자체적으로 비활성화됩니다.

ICA9001 **파일 시스템 안전성 검토 프로그램 경고 - *warning description text***

설명: fwfschk가 파일 시스템에서 문제점을 발견했습니다.

ICA9002 **마지막 메세지가 %1$d회 반복되었음.**

설명: 동등한 메세지가 개입 메세지 없이 로그된 경우 AIX syslogd에서 생성한 메세지. 조건을 감지할 수 없는 로그 모니터에 대한 메세지가 여기에 기록됩니다. 이 메세지는 실제 syslogd 메세지가 작성된 언어로 기록되어야 합니다.

ICA9003 **구성 서버에서 사용자 *name*에 대한 사용자 확인 실패.**

설명: FW 구성 서버가 표시된 사용자를 확인할 수 없습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9004 **사용자 *name*이 구성 서버에서 성공적으로 사용자 확인되었음.**

설명: FW 구성 서버가 표시된 사용자를 확인했습니다.

ICA9005 **원격 구성 서버 시작.**

설명: 구성 서버가 시작되었습니다.

ICA9006 **원격 구성 서버 종료.**

설명: 구성 서버를 종료 중입니다.

ICA9007 **원격 구성 서버가 메세지 카탈로그를 열 수 없음.**

설명: 원격 구성 서버에서 사용하는 하나 이상의 메세지 카탈로그가 누락되었습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9008 **원격 구성 서버가 getpeername()에서 실패했음: 오류 *errno*.**

설명: 구성 서버가 클라이언트에 관한 정보를 얻을 수 없습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9009 **원격 구성 서버가 getsockname()에서 실패했음: 오류 *errno*.**

설명: 구성 서버가 자신에 관한 정보를 얻을 수 없습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9010 **원격 구성 서버가 어댑터 정보를 얻는 데 실패했음.**

설명: 구성 서버가 어댑터 정보를 얻을 수 없습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9011 **구성 서버가 원격 구성 서버에 대하여 활성화되지 않음.**

설명: 구성 서버가 구성 파일에 local=yes를 설정했으며 클라이언트가 원격 시스템에 있습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9012 **원격 구성 서버가 로그온 요청을 읽을 수 없음.**

설명: 구성 서버가 클라이언트 로그온 요청을 읽을 수 없습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9013 **원격 구성 서버가 잘못된 로그온 요청을 수신했음.**

설명: 로그온 요청이 잘못된 정보를 포함합니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9014 **원격 구성 서버가 파이프를 작성할 수 없음.**

설명: 구성 서버가 사용자 확인을 위한 파이프를 작성할 수 없습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9015 **원격 구성 서버가 프로세스를 작성할 수 없음.**

설명: 구성 서버가 사용자 확인을 위한 프로세스를 작성할 수 없습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9016 **EFM 디먼 시작 중.**

설명: EFM 디먼이 관리되는 Firewall에서 시작되었습니다.

ICA9017 **EFM 디먼 종료; rc = *value*.**

설명: 지정된 리턴 코드로 EFM 디먼을 종료 중입니다.

ICA9018 **EFM 디먼이 메세지 카탈로그를 열 수 없음.**

설명: EFM 디먼에서 사용하는 하나 이상의 메세지 카탈로그가 누락되었습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9020 **실행 중인 사용자 ID를 전환할 수 없음.**

설명: 실행 중인 사용자 ID를 전환하기 위한 시스템 호출 실패.

사용자 응답: FW 관리자를 참조하십시오.

ICA9021 **이 Firewall은 *logon* 모드를 지원하지 않음.**

설명: 해당 Firewall이 이러한 특수한 모드를 지원하지 않습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9022 ***user*가 *lgon* 모드로 Firewall에 로그온하도록 사용자 확인되지 않음.**

설명: 해당 사용자명이 이러한 특수한 모드를 사용하여 로그온하도록 사용자 확인되지 않습니다.

사용자 응답: FW 관리자를 참조하십시오.

ICA9023 **EFM DLL을 로드할 수 없음.**

설명: efm dll 로드 실패.

사용자 응답: FW 관리자를 참조하십시오.

ICA9024 **전송 요청이 *user*에 의해 Firewall *machine*으로 시작되었음.**

설명: 전송 조작이 시작되었습니다.

ICA9025 **전송 요청이 리턴 코드 *return code*로 종료되었음.**

설명: 전송 조작이 완료되었습니다.

ICA9026 **파이어월 *machine*의 *user*에게서 *time*에 전송 요청이 수신되었습니다.**

설명: 전송 조작이 지정된 시간에 시작되었습니다.

ICA9027 **함수 *function*의 파일 *filename*이 전송 요청에 추가되었음.**

설명: 지정된 파일이 전송될 예정입니다.

ICA9028 **활성화 요청이 *user*에 의해 Firewall *machine*으로 시작되었음.**

설명: 활성화 조작이 시작되었습니다.

ICA9029 **활성화 요청이 리턴 코드 *return code*를 나타내며 종료되었음.**

설명: 활성화 조작이 완료되었습니다.

ICA9030 **Firewall*machine*의 *user*에게서 *time*에 활성화 요청이 수신되었습니다.**

설명: 활성화 조작이 지정된 시간에 시작되었습니다.

ICA9031 **함수 *function*의 활성화가 리턴 코드 *return code*로 종료되었음.**

설명: 지정된 함수의 활성화가 완료되었습니다.

ICA9032 **NAT 구성이 *datee time*에 갱신되었습니다.**

설명: NAT 구성이 갱신되었습니다.

ICA9033 **NAT 지원 (*version.release*레벨)이 *date time*에 초기화되었습니다**

설명: Firewall NAT 지원이 초기화되었습니다.

ICA9034 **NAT 지원이 *datee time*에 비활성화되었습니다.**

설명: NAT 지원을 사용할 수 없습니다.

ICA9035 **NAT가 보안 주소 *Secured IP Address*에 대하여 등록된 주소를 할당할 수 없음.**

설명: 보안 주소는 등록된 주소 풀에 사용할 수 있는 주소가 없으므로 변환되지 않습니다.

ICA9036 **NAT가 등록된 주소 *Registered IP Address*를 주소 풀로 해제했음.**

설명: 등록된 주소는 등록된 IP 주소 풀로 릴리스되었습니다.

ICA9037 **Firewall 인터페이스가 *time_and_date*에 자동으로 갱신되고 있음.**

설명: Firewall 초기화 프로그램이 Firewall 인터페이스 파일 fwadpt.cfg의 갱신을 트리거하기 위해 **UpdateInterfaces()**를 호출했습니다.

시스템 조치: none

사용자 응답: none

ICA9038 **인터페이스 *address*가 Firewall 구성에서 삭제되었음.**

설명: 나열된 점분리 십진 주소가 Firewall 구성 파일 fwadpt.cfg에 나열되어 있으나 TCP 스택에 알려지지 않았으므로 구성 파일에서 삭제되었습니다.

시스템 조치: none

사용자 응답: none

ICA9039 **인터페이스 *address*가 Firewall 구성에 추가되었음.**

설명: 나열된 점분리 십진 주소가 TCP 스택에 의해 발견되었으나 Firewall 구성 파일 fwadpt.cfg에 없으므로 구성 파일에 추가되었습니다.

시스템 조치: none

사용자 응답: none

ICA9040 **인터페이스 *address* 마스크가 *oldmask*에서 *newmask*(으)로 갱신되었습니다.**

설명: fwadpt.cfg 파일의 마스크는 하드웨어에 설치된 것과 일치하지 않습니다. fwadpt.cfg 파일에서 올바른 마스크 필드가 갱신되었습니다.

시스템 조치: none

사용자 응답: none

ICA9041 **이 시스템에서 인터페이스를 찾을 수 없음.**

설명: 이 시스템에서 어댑터 인터페이스를 찾을 수 없습니다.

시스템 조치: none

사용자 응답: none

ICA9042 **NAT는 작업 중인 다-대-일 주소 *many-to-one address*와 함께 활성화됨.**

설명: NAT는 성공적으로 초기화되어 이제 활성화되었습니다. 주소가 0이라는 것은 다-대-일 변환이 비활성화 상태에 있다는 것을 의미합니다.

시스템 조치: none

사용자 응답: none

ICA9043 **NAT는 리턴 코드 *rc*와(과) 함께 초기화에 실패함.**

설명: NAT는 초기화에 실패하여 비활성화 상태에 있습니다.

시스템 조치: 호출되는 NAT 함수가 없습니다.

사용자 응답: NAT 기능성이 필요하면, 리턴된 코드를 보고 이를 적절히 정정하십시오. 문제가 해결되지 않을 때는 IBM 서비스로 문의하십시오.

ICA9044 **NAT가 비활성화됨.**

설명: NAT는 성공적으로 비활성화되었으므로 이제 비활성화 상태에 있습니다.

시스템 조치: none

사용자 응답: none

ICA9045 **NAT는 *secured address*:*port* 보안 주소:포트에 대해 *address*:*port* 주소:포트를 할당하였습니다.**

설명: NAT는 보안 호스트 대신 주소 포트에서 주소:포트를 할당했습니다.

시스템 조치: none

사용자 응답: none

ICA9046 **NAT는 보안 주소 *secured address*에 다-대-일 주소를 할당할 수 없습니다.**

설명: NAT는 다-대-일 주소의 포트를 다 사용했습니다.

시스템 조치: 로컬 호스트의 패킷은 삭제되었습니다.

사용자 응답: 이는 미해결 연결이 너무 많다는 것을 의미합니다. 관리자는 유휴 상태에 있는 변환 테이블 항목을 더 빨리 제거하기 위해 다-대-일 주소와 관련된 시간-초과를 줄이고 싶을 수도 있습니다.

ICA9047 **NAT는 *secured address*:*port* 보안 주소:포트에서 *address*:*port* 주소:포트를 비할당하였습니다.**

설명: NAT는 지정된 주소:포트 쌍을 사용가능한 풀로 리턴했습니다.

시스템 조치: none

사용자 응답: none

ICA9048 **NAT는 프로토콜:*protocol* 주소:포트 *address*:*port* 보안 주소:포트 *secured address*:*port*와 함께 분할된 패킷을 발견하였습니다.**

설명: NAT는 분할된 패킷 제어 패킷 또는 분할된 ICMP 오류 오류 메세지를 발견했습니다. NAT는 분할된 FTP 제어 패킷을 변환하지만 자료부분은 조사되지 않습니다. 이것이 분할된 PORT 명령이었다면, FTP 데이터는 메세지에 있는 IP 주소가 변환되지 않으므로 실패합니다. 패킷이 분할된 ICMP 오류 메세지일 때는 삭제됩니다.

시스템 조치: 설명을 참조하십시오.

사용자 응답: 이런 상황이 반복적으로 발생하면, IBM 서비스에 알리십시오.

ICA9049 **NAT는 *source address*에서 *destination address*중에 변환될 수 없는 무순의 분할 부분을 발견했습니다.**

설명: NAT는 dategram의 첫 번째 분할부분에 앞서 도착한 분할된 데이터그램을 발견했습니다.

시스템 조치: NAT는 분할부분을 올바로 변환할 수 없으므로 데이터그램이 삭제됩니다.

사용자 응답: 이런 상황이 반복적으로 발생하면, IBM 서비스에 알리십시오.

ICA9050 **NAT는 보안 주소:포트*secured address*:*port*에서 주소:포트 *address*:*port*로 리턴 코드 *rc*로 프로토콜 :*protocol*과 함께 패킷을 전송하는데 실패했습니다.**

설명: NAT는 패킷을 변환하지 못했습니다.

시스템 조치: 패킷이 삭제됩니다.

사용자 응답: 이런 상황이 반복적으로 발생하면, IBM 서비스에 알리십시오.

ICA9051 **NAT는 보안 주소:포트*secured address*:*port*에서 주소:포트 *address*:*port*로 프로토콜 :*protocol*과 함께 도착한 패킷을 감지했습니다.**

설명: NAT는 패킷의 도착을 감지했습니다.

시스템 조치: none

사용자 응답: none

ICA9052 **NAT는 보안 주소:포트*secured address*:*port*에서 주소:포트 *address*:*port*로 프로토콜 :*protocol*과 함께 출발한 패킷을 감지했습니다.**

설명: NAT는 패킷의 출발을 감지했습니다.

시스템 조치: none

사용자 응답: none

ICA9053 **%3$d 내의*stringValue filename***

설명: 디버그 중

시스템 조치: none

사용자 응답: none

ICA9054 ***address*:IP 주소는 비보안/보안 인터페이스 주소와 다-대- 일 주소로 동시에 사용될 수 없습니다.**

설명: 이는 똑 같을 수 없습니다.

시스템 조치: 요청된 조치는 수행되지 않습니다.

사용자 응답: 다른 비보안/보안 주소나 다른 다-대-일 주소를 선택하십시오.

ICA9060 **치명적인 구성 서버 초기화 오류 - socket():***system error message*

설명: 구성 서버 초기화 실패로 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 정정하고 구성 서버를 다시 시작하십시오.

ICA9061 **치명적인 구성 서버 초기화 오류 - listen()n:***system error message*

설명: 구성 서버 초기화 실패로 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 정정하고 구성 서버를 다시 시작하십시오.

ICA9062 **치명적 구성 서버 오류 - main accept():** *system error message*

설명: 구성 서버 기본 루틴의 실패로 디먼이 종료되었습니다.

사용자 응답: 표시된 시스템 문제를 정정하고 구성 서버를 다시 시작하십시오.

ICA9063 **치명적 서버 오류 -** *failing function***: 리턴 코드 = 0x***function return code*

설명: 구성 서버는 표시된 함수에서 오류를 발견했습니다. 디먼이 종료됩니다.

사용자 응답: 표시된 시스템 문제를 정정하고 구성 서버를 다시 시작하십시오.

ICA9064 **알 수 없는 옵션 -***value***은(는) 무시됩니다.**

설명: 표시된 옵션은 지정되었지만 인식되지는 않습니다.

ICA9065 **구성 서버 오류 -** *failing function***:** *system error message*

설명: 구성 서버는 표시된 함수에서 오류를 발견했습니다. 디먼이 종료됩니다.

사용자 응답: 표시된 시스템 문제를 정정하고 구성 서버를 다시 시작하십시오.

ICA9066 **메모리 부족: 구성 서버: malloc(***bytes***)은** *function_name***기능 내의 NULL 값을 리턴합니다.**

설명: 충분한 메모리를 할당할 수 없음 - malloc이 NULL을 전송했습니다.

ICA9067 **바인드에 실패했습니다. 주소:** *port***은(는) 이미 사용중입니다.**

설명: 주어진 포트 주소는 현재 사용 중입니다.

시스템 조치: 구성 서버가 종료합니다.

사용자 응답: 다른 포트 주소를 사용하여 구성 서버에 연결하거나 Firewall 관리자에게 문의하십시오.

ICA9068 **-***value* **옵션은 실패했거나 잘못 지정되었습니다.**

설명: 표시된 옵션은 실패했거나 또는 잘못 지정되었습니다.

시스템 조치: 구성 서버가 종료합니다.

사용자 응답: 표시된 옵션의 사용법을 정정하고 구성 서버를 다시 시작하십시오.

ICA9069 **SSL 초기화 실패.**

설명: SSL 암호화 환경은 초기화에 실패하거나 또는 상대방과의 핸드쉐이크에 실패했습니다.

시스템 조치: 구성 서버가 종료합니다.

사용자 응답: SSL 환경을 검증하기 위해 Firewall 관리자를 만나십시오.

부록B. Windows NT 시스템 구성 강화

강화는 불필요한 디먼을 작동 중지하고 허가되지 않은 사용자 ID를 사용하지 않음으로써 보안 및 효율성을 최대화하는 프로세스입니다. 강화는 IBM Firewall 소프트웨어 설치의 일부로 보안을 위협할 수 있는 시스템 자원을 편집합니다.

IBM Firewall 구성에 필요하지 않으며 보안을 위협할 수 있는 서비스는 사용이 중단됩니다. TCP/IP 이외의 모든 프로토콜은 삭제됩니다.

부록C. 주석 요청(RFC) 얻기

주석 요청(RFC)은 새로운 프로토콜을 표시하고 인터넷 프로토콜 조에 대한 표준을 설정하는 문서입니다. 모든 RFC의 하드카피를 개별적으로 또는 예약에 근거하여, 네트워크 정보 센터(NIC)에서 얻을 수 있습니다. 이런 책은 다음 주소에서 얻을 수 있습니다.

Government Systems, Inc.
Attn: Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

이 URL에서 RFC를 액세스할 수 있습니다.

http//www.cis.ohio-state.edu/hypertext/information/rfc.html.

ds.internic.net에 연결하여 FTP를 사용 중인 NIC로부터 온라인 복사본을 얻을 수 있습니다. 다음 형식으로 파일을 전송할 수 있습니다.

```
RFC:RFCnnnn.TXT
RFC:RFCnnnn.PS
```

여기서:

nnnn Is the RFC number

TXT Is the text format

PS Is the PostScript format

RFC 색인의 형식은 다음과 같습니다.

```
RFC:RFC-INDEX.TXT
```

주: 대부분의 RFC는 텍스트 형식으로만 사용 가능합니다. 포스트스크립트 파일을 요청하기 전에, 먼저 RFC 인덱스를 검토하여 RFC가 해당 형식으로 사용 가능한지 확인하십시오. NIC 자동 전자우편 서버에서 메세지를 mailserv@ds.internic.net로 보내 RFC의 온라인 사본을 전자우편을 통해 요청할 수도 있습니다. 주석의 본문에 다음 명령 중 하나를 포함시켜야 합니다.

```
SEND RFCnnnn.TXT
```

또는

```
SEND RFCnnnn.PS
```

여기서:

nnnn Is the RFC number

TXT Is the text format

PS Is the PostScript format

예를 들어, RFC 812 텍스트 형식을 요청하려면, 주석 본문에 다음을 지정해야 합니다.

```
SEND RFC812.TXT
```

RFC 인덱스의 온라인 복사본을 요청하려면, 주석 본문에 다음과 같은 명령을 포함시켜야 합니다.

```
SEND RFC-INDEX.TXT
```

부록D. IBM eNetwork Firewall Socks5.conf 구성 파일 형식

구성 파일 **socks5.conf**는 디폴트로 IBM Firewall 설치 디렉토리에 있습니다. 원할 경우, 텍스트 편집기를 사용하여 파일을 편집할 수 있습니다.

처음으로 서버가 호출될 때 **socks5.conf** 구성 파일이 읽혀집니다 (socks5.config 유형을 중단하지 않고 최신으로 고치기 위해). 이 파일에는 주어진 주소에 도달하기 위해 어떤 인터페이스를 사용하는지, 주어진 주소에 직접 연결할 것인지 아니면 프록시 서버를 사용할 것인지 및 프록시 연결이 이루어지기 위해서는 어떤 요구조건이 필요한지 등을 판별하기 위해 IBM Firewall이 필요로 하는 모든 정보가 들어 있습니다.

다음 섹션은 구성 파일에 나와 있습니다.

- 별명
- 변수
- 모듈
- 사용자 확인
- 경로지정
- 프록시
- 액세스 제어

사용자 확인, 경로지정, 프록시 및 액세스 제어 섹션에서 그 섹션에 대해 일치가 이루어질 때까지 순서대로 행을 읽습니다(행의 순서가 매우 중요). 행이 일치하려면, 행 안의 각 항목이 일치해야 합니다.

포트 지정

이름, 번호 또는 범위를 사용하여 포트를 지정할 수 있습니다. 범위가 포괄적인가에 따라 범위는 [또는 (로 시작되며)또는]로 끝납니다. 범위 구분자 안에는 쉼표로 구분된 두 개의 포트 지정자(이름 또는 번호)가 있어야 합니다. 포트 지정 방법을 포트 *패턴*이라 합니다.

호스트 지정

호스트 주소와 네트마스크는 보통 주어진 규칙에 적용되는 호스트 지정에 필요합니다. 이 호스트 지정 방법을 호스트 패턴이라 합니다. 호스트/마스크 쌍을 지정하는 데에는 몇 가지 방법이 있습니다.

매개변수	설명
hostIP/ mask	마스크를 포함한 호스트 주소 ″ANDed″는 마스크를 포함한 호스트 IP ″ANDed″와 동일해야 합니다. 이것은 보통 네트워크나 서브네트워크 일부로부터 주소의 호스트 부분을 숨기는 데 사용됩니다.
-	모든 것이 일치합니다. 모든 호스트가 허용됩니다.

매개변수	설명
n1	n1.0.0.0/255.0.0.0에 해당합니다.
n1.n2	n1.n2.0.0/255.255.0.0에 해당합니다.
n1.n2.n3	n1.n2.n3.0/255.255.255.0에 해당합니다.
.domain.name	호스트명은 *.domain.name* 스트링으로 끝나야 합니다.
a.host.name	호스트명은 정확히 *a.host.name*과 일치해야 합니다.

또한 아래에 설명된 것처럼 이전 호스트 패턴 구문에 대한 지원도 있습니다. 그러나 더 새로운 방법이 추천되고 읽기에도 쉽습니다.

매개변수	설명
hostIP/a	모든 것이 일치합니다(″-″와 동일). 모든 호스트가 허용됩니다.
hostIP/n	네트워크 일치입니다. 주소에서 네트워크 부분만을 남겨두고 호스트와 서브네트 부분을 숨깁니다. 여기에 사용되는 마스크는 호스트 IP 주소의 클래스에 따라 달라집니다.
hostIP/s	서브네트 일치입니다. 주소에서 서브네트와 네트워크 부분만을 남겨두고 호스트 부분을 숨깁니다. 여기에 사용되는 마스크는 호스트 IP 주소의 클래스에 따라 달라집니다.
hostIP/h	호스트 일치입니다. 호스트 IP에 해당합니다.

사용자 확인 방법 지정

우리가 제공하는 사용자 확인 방법은 *ibmcram*과 *ibmpwd*입니다. 다른 것들이 추가될 수도 있습니다.

사용자 확인 방법은 쉼표로 구분된 방법 리스트로서 지정할 수 있습니다. 행의 일치를 위해서는 선택된 사용자 확인 방법이 리스트 안의 방법 중 하나로 표시되어야 합니다. 이 구문을 auth 패턴이라 합니다. 사용자 확인 방법 NULL은 디폴트에 따라 정의됩니다. 기타 방법은 적절한 모듈(들)을 로드하여 포함할 수 있습니다. ″-″는 NULL을 포함하는 임의 사용자 확인 방법이 수용될 수 있음을 나타냅니다.

사용자 확인 항목

사용자 확인 항목은 사용할 수 있는 사용자 확인의 유형을 지정합니다. 형식은 다음과 같습니다.

```
auth/ban   source-address  source-port
auth-methods
```

매개변수	설명
auth/ban	사용자 확인 항목이 허가되었는지(auth) 허가되지 않았는지(ban) 여부를 나타냅니다.

매개변수	설명
source-address	유효한 호스트 패턴입니다.
source-port	유효한 포트 패턴입니다.
auth-methods	유효한 auth 패턴입니다.

키워드 ″ban″은, 사용자 확인이 이 호스트에 시도되지 못하며 지정된 서버에 유효한 용법을 포함하지 않음을 지정합니다.

auth/ban 행이 지정되지 않은 경우, 디폴트에 따라 모든 사용자 확인을 수용할 수 있습니다. 연결의 허용이 *deny*(디폴트)에 설정된 경우, 사용자 확인이 적용된 후까지 연결이 거부됩니다. SOCKS5 프로토콜에서, 허가 전에 사용자 확인이 일어납니다. 호스트에 기반해서만 그 호스트의 사용자 확인 방법을 판단해야 합니다.

명령 지정

또한 명령을 쉼표로 구분된 리스트로 지정할 수 있습니다. 이 구문을 명령 패턴이라 합니다. 정의된 명령은 connect, bind, udp, ping 및 traceroute입니다. 기타 명령은 모듈을 통해 추가할 수 있습니다. ″-″(대시)는 모든 명령을 수용할 수 있음을 나타냅니다.

모듈 로딩

모듈을 사용하면, 새로운 사용자 확인 방법, 명령, 허가 검토 및 내용 필터를 추가하여 서버 기능으로 사용자 확장할 수 있습니다. 형식은 다음과 같습니다. *module stub filename options*

매개변수	설명
module	로드할 모듈의 식별자입니다.
stub	함수명 액세스에 사용되는 접두사이며 모듈에 따라 달라지는 이름입니다.
filename	로드할 모듈의 파일명입니다.
options	모듈에 고유한 구성 정보입니다(있다면).

모듈은 다른 곳에서 사용되는 필드를 정의할 수 있으므로, 먼저 모듈 행을 넣는 것이 좋습니다. 예를 들어, 사용자 확인 모듈은 auth 및 permit 행에 사용되는 사용자 확인 방법명을 정의합니다.

경로지정 항목

복수 네트워크 인터페이스(따라서, IP 주소)를 갖춘 시스템에서, 특정 네트워크 인터페이스가 특정 주소와 결합하여 사용되는지 확인하는 것이 좋습니다. 이것은 내부 시스템이 내부 네트워크 인터페이스를 사용하고 외부 시스템이 외부 네트워크 인터페이스를 사용하는지 확인하여 ″IP 속이기″(네

트워크 외부 시스템이 네트워크 내부에 있는 기계처럼 행세하는)를 방지합니다. 또한 SOCKS 서버가 BIND 요청을 수용할 때 또는 SENDTO 요청을 발행할 때 바인드할 네트워크 인터페이스를 판별하는 데 사용합니다. 어떤 항목도 일치하지 않을 경우, INADDR_ANY가 바인드하는 데 사용되며 임의 인터페이스가 수신하는 데 사용될 수 있습니다. 단일 홈(homed) 호스트는 경로지정 항목을 포함할 필요가 없습니다. 이들은 하나 이상의 네트워크 인터페이스를 갖춘 시스템에만 필수입니다. 형식은 다음과 같습니다. **route** *dest-address dest-port interface-address*

매개변수	설명
route	경로지정 항목을 지정하는 키워드입니다.
dest-address	유효한 호스트 패턴입니다.
dest-port	유효한 포트 패턴입니다.
interface-address	네트워크 인터페이스 카드의 IP 주소 또는 네트워크 인터페이스명(예를 들어, elnk31)입니다.

변수 항목

로깅 및 정보 메세지의 양 및 유형은 구성 파일 안의 특정 변수 및 플래그로 제어할 수 있습니다. 형식은 다음과 같습니다. **set** *variable value*

매개변수	설명
set	로컬용으로 환경 변수 항목을 설정하는 키워드입니다.
variable	유효한 환경 변수입니다. 사용가능한 변수 나열에 대해서는 아래의 138페이지의 『환경 변수』를 참조하십시오.
value	할당할 값입니다.

환경 변수

환경 변수	설명
SOCKS5_BINDPORT [port]	디폴트 포트 1080 외에 지정된 포트를 사용하도록 IBM Firewall을 구성합니다.
SOCKS5_RECVFROMANYONE	UPD 지원이 사용가능일 경우, UPD 클라이언트가 알 수 없는 송신자로부터 메세지를 수신할 수 있습니다.
SOCKS5_USECLIENTSPORT	클라이언트가 메세지를 송신하는 데 사용하는 동일 포트에 바인드할 수 있는 경우에만 IBM Firewall을 프록시에 구성합니다. 이것은, 서버가 데이터를 클라이언트에 흘려보내고(streaming) 있을 때 UDP 연결 프록싱에 필요합니다(클라이언트가 서버로 메세지를 송신하기 전에 클라이언트로 송신되고 있는 메세지). 이 사용법의 예는 RealAudio입니다.

환경 변수	설명
SOCKS5_MAXCHILD	동시 진행되는 쓰레드의 최대 수.
SOCKS5_NOREVERSEMAP	IP 주소를 호스트명에 대응하지 못합니다. 별명이 구성 파일에 할당된 경우, 이것은 정보 로깅을 희생시켜 성능을 늘립니다.
SOCKS5_NOSERVICENAME	포트 번호를 서비스명에 대응하지 못합니다. 별명이 구성 파일에 할당된 경우, 이것은 정보 로깅을 희생시켜 성능을 늘립니다.
SOCKS5_NOIDENT	컴파일된 경우에도 IDENT 요청을 사용하지 못합니다. 클라이언트에 대한 느린 링크를 가진 경우 그리고 클라이언트가 IDENTD를 사용하지 않을 경우에 유용합니다. 이것은 시간종료 기간을 감소시킵니다.
SOCKS5_DEMAND_IDENT	클라이언트로부터 IDENT 응답이 없을 경우 실패하도록 NULL 사용자 확인을 구성하십시오. 이것은, 사용자명이 항상 연결 요청과 관련되는지 확인하는 데 유용합니다.

프록시 항목

프록시 항목은 SOCKS 프록시 서버의 주소를 기술합니다. 이러한 행은 주어진 호스트에 연락하는 방법을 서버에게 알려 줍니다. 어떤 행도 호스트와 일치하지 않을 경우, 호스트에 직접 연락됩니다. 이 형식은 다음과 같습니다. *proxy-type dest-addr dest-port proxy-addr proxy-port*

매개변수	설명
proxy_type	프록시 서버의 유형입니다. 유효한 입력은 다음과 같습니다. • socks5 • socks4 • no proxy
dest-address	유효한 호스트 패턴입니다.
dest-port	유효한 포트 패턴입니다.
proxy-address	IP 주소 또는 프록시 서버의 이름입니다.
proxy-port	SOCKS 디먼이 연결을 수용하고 있는 프록시 서버 포트입니다.

제어 항목 액세스

액세스 제어 섹션은 연결 설정에 대한 요청이 허용되었는지 또는 거부되었는지를 판별합니다. 여기에는 permit 행과 deny 행, 두 가지 유형의 행이 있습니다. 항목 행이 일치하려면 행에 있는 각 행이 일치해야 합니다. 형식은 다음과 같습니다.

```
permit auth cmd src-host dest-host src-port dest-port [userlist]
deny auth cmd src-host dest-host src-port dest-port [userlist]
```

매개변수	설명
auth	유효한 auth 패턴 및 auth 항목으로 지정된 사용자 확인 방법 리스트입니다.
cmd	이 행으로 일치되는 명령을 지정하는 유효한 명령 패턴입니다.
scr-host	출발지 호스트의 유효한 호스트 패턴입니다.
dest-host	목적지 호스트의 유효한 호스트 패턴입니다.
scr-port	출발지 호스트 포트의 유효한 포트 패턴입니다.
dest-port	목적지 호스트 포트의 유효한 포트 패턴입니다.
userlist	유효한 사용자 패턴입니다.

필터

로드된 모듈을 통한 필터링은 필터 지정문에 의해 수행됩니다. 형식은 다음과 같습니다.

```
filter  name auth cmd src-host dest-host src-port dest-port [userlist]
```

매개변수	설명
name	필터 모듈의 식별자입니다.
auth	유효한 auth 패턴 및 auth 항목으로 지정된 사용자 확인 방법 리스트입니다.
cmd	이 행으로 일치되는 명령을 지정하는 유효한 명령 패턴입니다.
scr-host	출발지 호스트의 유효한 호스트 패턴입니다.
dest-host	목적지 호스트의 유효한 호스트 패턴입니다.
scr-port	출발지 호스트 포트의 유효한 포트 패턴입니다.
dest-port	목적지 호스트 포트의 유효한 포트 패턴입니다.
userlist	유효한 사용자 패턴입니다.

참고 문헌

인터넷 보안에 대한 추가 정보는 **http://www.software.ibm.com/enetwork/Firewall**에서 IBM Firewall 홈 페이지를 찾아 보십시오.

IBM 서적에 포함된 정보

Firewall, 인터넷 보안 및 일반 보안 항목에 대한 기타 IBM 정보 소스가 여기에 나열되어 있습니다.

Firewall 항목

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 보호하기*, SG24-5209

인터넷 및 월드 와이드 웹 항목

- *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 출판물에 대한 정보

이들 산업 출판물은 sendmail, 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

이들 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)

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 출원 중일 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
Tel: 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
Tel: 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 및 Windows 95 로고는 Microsoft Corporation의 등록상표 또는 독점 등록된 등록상표입니다.

UNIX는 X/Open Company Limited에 의해 독점적으로 사용되는 등록상표입니다.

Java 및 HotJava는 Sun Microsystems, Inc.의 등록상표입니다.

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

용어

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

색인

F

H

I

M

N

P

S

T

U

Printed in Australia

SC31-8659-01