IBM eNetwork Firewall Windows NT 版

参考大全

版本 3 发行版 2.1.1

SA31-1911-01

IBM eNetwork Firewall Windows NT 版

参考大全

版本 3 发行版 2.1.1

SA31-1911-01

注

在使用此信息和它支持的产品之前，请确保阅读第123页的『注意事项』下的一般信息。

第二版(1998 年 6 月)

本版本适用于 IBM eNetwork Firewall Windows NT 版的版本 3 发行版 2.1.1（产品号 5765-C16）。用该版本代替 SC31-8659-00。

目录

关于本书

本书所针对的读者是那些在 Windows NT** 机器上安装、管理和使用 IBM eNetwork Firewall 版本 3.2 的网络或系统安全管理员。如果想使用诸如 Telnet 或 FTP 等客户程序，请参阅用户指南了解有关的 TCP/IP 客户程序。

必备知识

在安装和配置 IBM eNetwork Firewall 之前，具有一定的 TCP/IP 和网络管理知识是非常重要的。因为您将设置和配置一个防火墙并用它控制出入您网络的访问，所以您首先得理解网络是如何工作的。特别是您需要理解 IP 地址、全限定名和子网掩码的基本知识。

TCP/IP 网络管理（TCP/IP Network Administration） 是一本非常有用的关于 TCP/IP 的书，它包括 netstat, arp, ifconfig, ping, nslookup, DNS, sendmail, routing 以及更多的详细内容。参阅 *Bibliography* 以得到详细信息。

UNIX 系统管理手册（UNIX System Administration Handbook） 是一本对于 UNIX 管理者十分有用的书，同时也提供了很好的 TCP/IP 、路由选择、网络硬件、DNS 以及 sendmail 的概述。参阅 *Bibliography* 以得到详细信息。

此发行版中的功能

IBM eNetwork Firewall NT 版提供了种类繁多的功能。它包括所有三大防火墙体系结构。

1. 应用代理
   - FTP
   - HTTP，包括 Gopher 和 WAIS
   - Telnet
   - SafeMail

   HTTP、Telnet 和 FTP 具有认证能力。
2. 通过 Socks 协议的电路级网关，一种 Internet 标准
3. 过滤 -- 一组扩展和健壮的标准，这些标准可允许或拒绝通信量。此标准包括 TCP/IP 地址、端口、协议、指导、适配器（安全/非安全）等等。

   许多预定义的服务使设置更快。

Socks 协议版本 5

除了简单和灵活，Socks 协议版本 5 还存在下列优点:

- 容易的认证和加密方法部署
- UDP 关联，它为通过基于 UDP 的代理电路创建虚拟的代理电路
- Socks V5 监视器，显示实时 socks 性能信息

网络地址转换

随着 Internet 的爆炸式增长，IP 地址的枯竭问题已经变得越发重要。网络地址转换（NAT）基于地址的再使用，为 IP 地址枯竭问题提供了一个解决方案。

NAT 的优点在于它透明地允许使用专用或非法地址的网络与 Internet 主机进行通信，从而有效地使专用网络拥有广阔的地址空间。而且，使用了 NAT，专用网络中的地址对于外部世界是隐藏的，这就提供了安全性的附加级别。

简单管理

通过使用 Java** 的应用程序，您可简便地更新防火墙配置。并且，不同的管理员可以指定不同层次的权限以进一步控制对防火墙的访问。这种独特的易于理解的图形用户界面（GUI）可用于管理 Firewall Windows NT 版及 AIX 版。

NT 的加固

安装好 Firewall 后，无 TCP/IP 协议是禁用的，不需要的系统服务器是禁用的，从非管理员帐户的本地登录是禁用的。

强大的认证

支持所有流行的基于令牌的认证机制，如 SecurID、SecureNet Key 等等。

报告实用程序

一旦将报告实用程序导出至数据库引擎后，将允许您运行 SQL 查询以更改系统日志。

报警，监控和记录

可扩展的和详细的记录包括所有的防火墙活动和 TCP/IP 地址、用户标识符、TOD、文件名及端口号。日志监视器也观察可疑活动而且当超过阈值时，它将报警。

隔绝多个网络

通过在防火墙中使用多个网络接口卡（NIC），您可以隔离多个子网。

国家语言支持

国家语言支持提供了英语、日语、韩语、法语、简体中文、繁体中文、意大利语、西班牙语和巴西的葡萄牙语。

输入 IP 地址

在配置防火墙时，会要求您输入 IP 地址。 应按以下格式输入一个完整的点十进制 IP 地址，它带所有 4 个八位位组:

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

这里的每个 nnn 都是一个范围在 000-255 的三位数字。

如何向 IBM 寻求服务

IBM 支持中心在问题的诊断与解决方面将向您提供电话帮助。您可以在任何时间致电 IBM 支持中心；在八个工作时内您将会收到回电（周一至周五的上午 8:00 至下午 5:00，本地客户时间）。电话号码是 1-800-237-5511。

在美国或波多黎哥以外，请联系您当地的 IBM 代理或 IBM 授权的供应商。

第1章 使用 IBM Firewall 命令行界面

本章将讨论 IBM Firewall 命令行中可以使用的命令。

以下信息适用于这些命令:

- 本书列举的命令使用下列语法规则:
  - *下划线* 表示这是用户输入的数据。
  - [] 指可选参数。
  - {} 指用户对参数的一种选择。
  - | 分开选项。
- 所有参数都使用 keyword=value 的格式。
- 如果一个参数拥有多个值，则应当将其置于双引号内并用空格分隔，例如:

  ```
  secaddr="11.22.33.1 11.22.33.2"
  ```
- 除了在双引号之内，请不要在任何参数中包含空格。
- 如果您遗漏了一个或多个必要参数，命令行实用程序将列出这些遗漏的参数。
- 如果输入了一个无效的参数值，命令行实用程序将报告该项错误。
- 有些防火墙精灵程序在其配置文件作了更改时，将动态地更新其运行状况。其中一些需要更新的子命令。 update 子命令就是为那些要执行指令的防火墙服务器所提供的。
- 只有主防火墙管理员才可以在命令行执行程序。
- 由于其复杂性及文件的相互依存性，**请不要直接编辑任何配置文件**。

配置服务器

命令 fwcfgsrv 用于列出或更改配置服务器的选项。使用此命令的管理员必须拥有管理通信量控制功能的权限。

要列出配置服务器选项，使用下列命令。

```
fwcfgsrv cmd=list
```

以下为命令 fwcfgsrv 的输出结果:

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

要更改配置服务器选项，使用下列命令。

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

参数定义为:

localonly

说明防火墙是否仅可以从本地的机器上进行管理。有效值为 yes 或 no。

encryption
说明配置服务器是否要求进站数据进行 ssl 加密。有效值为 none 或 ssl。

sslfile 指出用于 ssl 加密的 ssl 密钥文件名。参阅 第49页的『第6章 使用 Make Key File Utility（MKKF）』。

域名服务

域名服务（DNS）向安全网络内的主机提供完整的域名服务，而对安全网络外的主机提供极少的信息。需要用三个域名来完成它:

- 一个位于防火墙上
- 一个位于安全网络内
- 一个位于安全网络外。

请参阅 *IBM eNetwork Firewall 用户指南*以获取更多的信息。

注:

1. x.x.x.x 代表一个用点十进制格式书写的 IP 地址。
2. 参数 secaddr 和 remaddr 的值可以是一个单独的 IP 地址或一组 IP 地址。如果是指一组 IP 地址，它们应该用空格分隔并包含在双引号之内。
3. 检测到或标记重复地址都是错误的。
4. 首次配置 DNS 时，`fwdns cmd=change` 将创建一个新文件。防火墙将一直精确地保留一个 DNS 配置记录。该值可能为空。子命令 change 可用于更改 DNS 记录中任何或所有的值。

下列命令表列出了当前的 DNS 配置。

```
fwdns cmd=list
```

若要更改 DNS 配置项并创建新的文件，则:

```
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"
```

参数定义为:

secdomain=*SecureDomainName*
指内部安全网络的域名

secaddr=*SecureDNSaddr[,...]*
指安全域名服务器的 IP 地址

remaddr=*NonSecureDNSaddr[,...]*
指安全网络外的域名服务器（由 Internet 连接服务供应商提供）的 IP 地址。

过滤器

使用 `fwfilter` 命令激活和释放过滤器规则。

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

参数定义为:

fwfilter cmd=update
重新创建配置并激活规则集。

fwfilter cmd=verify
执行一个配置的“构造测试”，但并不激活任何更改。

fwfilter cmd=list
列举出最近建立的配置

fwfilter cmd=shutdown
释放过滤器机制

fwfilter cmd=startlog
将选定的通信量记录到防火墙日志设施内

fwfilter cmd=stoplog
停止防火墙过滤器记录

HTTP 代理

HTTP 代理通过 IBM Firewall 有效地处理浏览器请求，而不需要为 Web 浏览而使用 socks 服务器。 用户可在 Internet 上访问有用的信息，而不泄露内部网络的安全性并且不用改变其客户环境来实现 HTTP 代理。

`fwhttp` 命令列出和更改当前的 HTTP 代理配置。

要列出当前 HTTP 代理配置，使用下列命令。

```
fwhttp cmd=list
```

要更改当前 HTTP 代理配置，使用下列命令。

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

参数定义为:

port 指 http 代理服务将要侦听的端口。

maxcontentlengthbuffer
指返回文档的最大缓冲区以允许返回附加的 content-length 标题。

minactivethreads
在初始化和运行时保持活动的最少工作线程数。

maxactivethreads
可在同一时刻运行的最多线程数。

idlethreadtimeout
保持空闲线程可用的时间长度。

logging
说明记录是否满足 HTTP 活动的要求。其值为 on 或 off。

authenticate
指要认证的用户级别。值为 all、none 或 new。

authenticatetimeout
建立持续连接后等待客户程序请求的时间。

maxpersistrequests
指持续连接中接收到的最多请求数。

persisttimeout
维持持续连接的时间。

接口

安全接口把 IBM Firewall 连接到您想保护的内部网络中主机的网络。 **至少必须有一个安全接口为防火墙工作。** 非安全接口把 IBM Firewall 连接到一个或多个外部网络或 Internet 上。IBM Firewall 至少必须有一个非安全接口。

本命令将列出防火墙上的网络接口。使用此命令的管理员必须拥有管理接口功能的权限。

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

参阅 *IBM eNetwork Firewall 用户指南* 中的管理章节以获取有关管理员权限的详细信息。

参数定义为:

addr=x.x.x.x
将列出所有已在防火墙上配置的网络接口并指出每一个接口是安全的还是非安全的。同时还将标识出名字。如果指定了可选的 addr 参数，则只列出指定的接口。如果为 addr 指定了一个点十进制 IP 地址，列表中将包括该指定地址的地址、状态、名称，假设它已在防火墙配置过。

本命令将允许您定义至防火墙的网络接口。使用此命令的管理员必须拥有管理接口功能的权限。

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

参数定义为:

addr=x.x.x.x
包含要更改的点十进制接口地址。如果该接口未在防火墙上定义过，将报告出错。

state={secure|nonsecure}
包含“安全”和“非安全”这两个关键字之一，用以区分与指定接口相连的网络。

name 指用来标识接口或网络的名称。可包含空格，但必须用双引号括起。

虽然参数 state 和 name 都是可选项，但必须指定其中的任何一个。

日志归档程序

下列命令调用了日志文件归档程序以维护为归档而配置的日志设施。

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

将该命令放入 Windows NT 预定服务中是很有用的。请参阅 *IBM eNetwork Firewall 用户指南*以获取更多的信息。

日志文件管理

日志文件管理定义和管理了日志和归档文件。命令 fwlog 用于添加、修改和删除日志设施。

要添加日志设施，使用下列命令。

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

facility 的有效值是:

- firewall (local4) - 包括过滤器记录的常规防火墙日志
- alert (local1) - 日志监视器精灵程序的状态和用来居于报警显示器中的阈值违反警告
- adminaudit (local0) - 管理的审查日志
- mail - 邮件日志

priority 的有效值是:

- debug
- info
- warning
- error
- crit

参数 logfile 说明了 firewall 日志项应该发送到的地方。一个全限定文件名的有效值（按格式 （drive:\directory））指出了日志项应写入的文件。

注: 标识为报警日志或防火墙日志的文件应彼此不同，并且如果防火墙功能被用于处理这些文件，它们则应不同于任何其它的日志设施文件。

非常重要的是“仅有”防火墙日志信息出现在输入至报告实用程序的文件中。没有其它的设施作为防火墙日志或报警日志直接写入同一个文件。

参数 arcfile、logtime 和 arctime 都是可选项并且只有当参数 logfile 指定了一个文件名时它们才有效。如果指定了其中任何一个参数，则所有这三个参数都必须指定。这些参数控制记录的归档。对于要产生的实际归档，须周期运行 fwlogmgmt 命令。参阅第5页的『日志归档程序』。

缺省地，防火墙使用这些参数来指示把归档运行记录存储在哪里和归档应该间隔多久发生一次。需要指定这三个参数来启用归档。

归档设施可通过写出一个防火墙归档插件来替换。参阅第41页的『第4章 日志归档程序插件软件开发包』。

参数 **arcfile** 必须包含一个全限定路径。

参数 **logtime** 说明了将防火墙记录项移至归档文件之前它将在日志文件内保留的最小天数。

参数 **arctime** 说明在清除防火墙记录记录之前它将在归档文件内保留的最小天数。

要更改日志设施，使用下列命令。

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

如果一项更改，特别是在初始情况下，未能创建一个语法正确的配置文件（例如，创建的日志文件丢失字段），那么将发出一条警告并且防火墙将不记录数据。

如果想进行记录但不进行归档，则只需要使用参数 **facility**、 **priority** 和 **logfile**。如果希望日志在启动时不归档，则使参数 **archive**、 **logtime** 和 **arctime** 置空。如果已预定了归档作业，删除它。

要列出当前日志文件配置数据，使用下列命令。

```
fwlog cmd=list
```

删除由 fwlog cmd=list 命令返回的索引号所指定的防火墙日志项，则使用下列命令。

```
fwlog cmd=delete
      index=index of entry to delete
```

日志监视器

使用日志监视器命令告诉日志监视器何时，如何触发警报。当在指定的间隔内达到此命令（或相应的配置客户面板）中指定的阈值时，发生报警。当报警发生时:

1. 在防火墙报警设施和防火墙日志设施中写入一条记录。
2. 运行指定的命令

3. 将通知发送到一个或一个以上的用户标识符
4. 将信息发送到寻呼设备

以上三个操作由指定值的适当配置控制。

列出日志监视器设置选项

```
fwlogmon cmd=list
```

指定用户标识符在发生任何警报时接收邮件通知

要指定用户标识符在发生任何警报时接收邮件通知（通知发送到您添加的每个标识符上）：

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

指定在任何警报发生时运行的命令

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

fwlogmon cmd=delete
         type=command
```

指定一个警报应该基于未成功登录尝试数而触发的阈值

```
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
```

指定一个警报应该基于特定防火墙信息 ID 发生数而触发的阈值

```
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=
```

参数定义为:

type 标识了正在添加或修改的日志监视器命令特性的类型。

可以是 id、command、single、multi、host 或 msg。

id 影响用户标识符发送通知。

command
指要执行的命令。

msg 影响特定日志信息的监控。

single 影响基于单个用户标识符的监控。为每个有失败尝试的标识符都保留了计数。如果任何标识符的计数达到在此命令中指定的阈值，则触发警报。

multi 影响基于多个用户标识符的监控。如果所有计数（对于所有具有失败尝试的用户标识符来说），达到了在此命令中指定的阈值，则触发警报。

host 影响了基于主机名的监控。为每个有失败尝试的主机名都保留了计数。如果任何主机名的计数达到在此命令中指定的阈值，则触发警报。

username
是防火墙管理员或其它通知任何报警的用户的邮件 ID。只要正确配置安全方服务器，则报警通知都将成功发送。

command
在任何报警发生时执行的命令名称。它必须是可执行文件的全路径名称。它可以是 .bat 文件，允许在该文件中执行多个命令，然而，如果 .bat 文件引用了其它文件，则必须是全路径名称的引用。

count 设置故障数或者特定日志信息发生（报警将使用的）的阈值。

time 以分钟为单位设置时间间隔。为了触发的事件，必须在第一次发生的时间间隔内达到计数值。比当前时间上一个间隔还要早的（故障）发生将从计数值中删除。

pager 指定在关联阈值触发报警时是否使用寻呼机。活动寻呼机用来发送页面。

tag 要监视的日志信息标记 （具有信息前缀 ICA）。日志监视信息（低于 1000 的 ICA 标记）不能监视。

邮件

使用 fwmail 命令来映射公用和安全域。

```
fwmail cmd=list
```

```
fwmail cmd=add
        secdomain=
        mail=
        remdomain=
```

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

fwmail cmd=delete
        secdomain=
```

参数定义为:

secdomain
指防火墙安全方用户的已知名字，由此名字来描述邮件域。

mail 指邮件服务器地址。

remdomain
指防火墙非安全方用户的已知名字，由此名字来描述邮件域。

网络地址转换

网络地址转换（NAT）允许其安全 IP 网络内的地址为任何其它 IP 网络再使用，以此为 IP 地址枯竭的问题提供了一个解决方案。

NAT 支持四种类型的配置:

- 多对一注册地址 - 多对一转换把包的安全地址和端口号码转换为许多(至多 65536)内部地址可以共享一个注册的 IP 地址。 这个共享的注册 IP 地址将隐藏本地地址而不是在它之上添加，您需要为 Firewall 使用另一个注册的唯一 Internet 地址。
- 转换安全 IP 地址 - 转换安全 IP 地址项定义了一个需要 NAT 来执行 IP 地址转换的安全网络地址集。 缺省时，网络地址转换器对所有的安全 IP 地址进行地址转换。
- 排除安全 IP 地址 - 排除安全 IP 地址项定义了一个无需 NAT 执行 IP 地址转换的安全网络地址集。 缺省时，网络地址转换器对所有的安全 IP 地址进行地址转换，除非该地址在排除安全 IP 地址指定的范围之内。
- 映射安全 IP 地址 - 映射安全 IP 地址项定义了从一个安全 IP 地址至一个已注册 IP 地址的一对一的映射。 这种一对一的 IP 地址映射允许外部应用程序客户（例如 FTP 或 Telnet 客户程序）与安全网络内的服务器建立 TCP 会话。

NAT 命令的语法如下:

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

参数定义为:

fwnat cmd=list
列出当前的 NAT 配置

fwnat cmd=update
刷新 NAT 引擎

fwnat cmd=verify
对配置进行语法检查

fwnat cmd=shutdown
停止所有的地址转换

fwnat cmd=startlog
停止记录每个转换包

fwnat cmd=stoplog
停止记录每个转换包

要添加多对一项至 NAT 配置，请使用 **type=many-to-one**:

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

参数定义为:

type=many-to-one
指添加一个 many-to-one 项

addr=*Addr*
指 IP 地址，它标识了添加至已注册地址池的已注册 IP 地址的范围

timeout=*minutes*
指在 NAT 可以释放已注册 IP 地址之前，地址转换可保持空闲的分钟数。缺省值是 15，范围是 5-45。

要修改在 NAT 配置使用中的多对一项，请使用下列语法:

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

参数定义为:

索引 当执行 fwnat cmd=list 时，在左边栏中有特定 NAT 项的号。将特定 NAT 号用于索引参数。

addr=*Addr*
指 IP 地址，它标识了添加至已注册地址池的已注册 IP 地址的范围

timeout=*minutes*
指在 NAT 可以释放已注册 IP 地址之前，地址转换可保持空闲的分钟数。缺省值是 15，范围是 5-45。

要添加转换项到 NAT 配置文件中，使用 **type=translate** ，要从 NAT 配置文件中删除一个项，则使用 **type=exclude**:

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

参数定义为:

type=translate
指添加一个 translate 项

type=exclude
指添加一个 exclude 项

addr=*Addr*
指 IP address，它标识了需要转换的安全 IP 地址的范围。

mask=*Mask*
指出了一个 IP 地址范围

要修改在 NAT 配置中的转换或排除项，请使用下列语法:

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

参数定义为:

索引 当执行 fwnat cmd=list 时，在左边栏中有特定 NAT 项的号。将特定 NAT 号用于索引参数。

addr=*Addr*
指 IP address，它标识了需要转换的安全 IP 地址的范围。

mask=*Mask*
指出了一个 IP 地址范围

要添加一个映射项至 NAT 配置，请使用 **type=map**:

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

参数定义为:

type=map
指添加一个 map 项

secaddr
指应该转换成指定的已注册地址的 IP 地址

remaddr
指应该由指定的安全地址转换成的已注册地址

要修改在 NAT 配置中的映射项，请使用下列语法:

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

参数定义为:

索引 当执行 fwnat cmd=list 时，在左边栏中有特定 NAT 项的号。将特定 NAT 号用于索引参数。

secaddr
指应该转换成指定的已注册地址的 IP 地址

remaddr
指应该由指定的安全地址转换成的已注册地址

寻呼

当防火墙上出现入侵报警时，可激活寻呼机布告支持使防火墙可通过发送一信息至其寻呼机来寻呼系统管理员。要使它正常工作，必须使用 fwpgr、fwcarrier 和 fwmodem 命令来配置寻呼机、通信公司服务和调制解调器。

寻呼机配置

fwpgr 命令设置了活动寻呼机的参数，它是防火墙将发出的信号。

要列出寻呼机，使用下列命令。

```
fwpgr cmd=list
```

要添加寻呼机，使用下列命令。

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

要修改寻呼机，使用下列命令。

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

参数定义为:

carrier

是通信公司服务的名称，如在通信公司数据库中定义（通过 fwcarrier 命令）的那样。

modem

是调制解调器的名称，如在调制解调器数据库中定义（通过 fwmodem 命令）的那样。

pagerid

是通信公司分配的，唯一标识的寻呼设备的号码或名称。

message

在寻呼设备上发送和显示的信息。或者是数字或者是文本，取决于通信公司提供的服务。如果超过通信公司长度设置的较小值或 200 个字符，则将截断它。

通信公司

使用 fwcarrier 命令设置任何正在使用的寻呼服务的参数。

要列出通信公司，使用下列命令。

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

要添加通信公司，使用下列命令。

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

要修改通信公司，使用下列命令。

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

要删除通信公司，使用下列命令。

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

参数定义为:

carrier
指通信公司的名称。

dial 必须为已联系的 TAP 服务指定通信公司的调制解调器电话号码。

method
值必须是 TAP。

password
它是可选的，除非对通信公司服务是必要的。

length 您的通信公司服务器允许的最大信息长度。

baud 指定通信公司服务支持的最可靠的波特率。

parity 指定通信公司服务支持的奇偶校验类型。这通常是 TAP 协议的偶校验。

databits
指定通信公司服务支持的数据位数。对于 TAP 协议通常为 7。

stopbits
指定通信公司服务支持的停止位数。对于 TAP 协议通常为 1。

调制解调器配置

要建立寻呼机通知支持。需要配置调制解调器。

要发送寻呼请求至您的寻呼通信公司，请使用调制解调器命令配置调制解调器。

要列出调制解调器，使用下列命令。

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

要添加调制解调器，使用下列命令。

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

要修改调制解调器参数，使用下列命令。

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

要删除调制解调器，使用下列命令。

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

参数定义为:

modem

调制解调器的名称。

comport

与调制解调器相连的串行 COM 端口。在该 COM 端口上的调制解调器不能定义到 Windows NT 系统。

initstring

指调制解调器的初始化字符串。在字符串中的参数必须与 AT 调制解调器命令相配，但 AT 不应该作为字符串的一部分而被包括。指定的参数应该与您通信公司的调制解调器的通信需求相协调。

outsideline

指拨通出站线路的号码。

测试寻呼机配置

要确保已正确配置了活动寻呼机，使用下列命令。

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

参数定义对于 fwpgr 命令的来说是恒等的。

多个寻呼机

如果要经常更改活动寻呼机，则:

- 确认已定义了所有必需的通信公司和调制解调器。
- 使用 fwpgr 或配置客户来定义和保存寻呼机配置。
- 复制 ROOTDIR\config\pager.cfg 文件，给它取一个可以认出的名字
- 定义另一个寻呼机配置并复制它，重复这些操作直到复制所有需要的 pager.cfg 文件
- 复制想要在 ROOTDIR\config\pager.cfg 后激活的配置文件。

如果尝试处理移位更改，则使用 Windows NT at 命令建立预定作业，自动重复在每个移位开始处的最后一个插塞（bullet）。

用户

该命令用于添加一个新用户或为一个已存在的防火墙用户修改一至若干个属性。所有参数或者有缺省值或者在某些情况是不必要的。当 cmd=add 时，将保留缺省值；当 cmd=change 时，将保留当前值。

```
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}]
```

基本参数

username

指用户的登录名。

fullname

指用户全名或一些与该用户有关的其它一些简短（一行）信息。如果该值中包含空格，则必须用双引号将它括起。

level 缺省级别为 proxy，说明正在创建的用户是一个简单的代理或 Socks 用户。管理功能组与管理认证不适用于代理用户。

key 密钥用于认证用户的 Digital Pathways' SecureNet Key 卡。由于该值必须包含空格，所以它必须用双引号括起。

认证

以下是认证字符串和它们相应的认证方式。使用下面表示的 `fwuser` 命令各种参数的认证字符串。

- permit-permit all
- deny-deny all
- password-Firewall password
- NT-NT logon password
- snk-SNK
- sdi-SDI
- user-user-supplied authentications
- userauth2-user-supplied authentications
- userauth3-user-supplied authentications

secftp 指用于从安全接口实现 FTP 登录的认证方法。有效值为 deny、permit、password、NT、snk、sdi、user、userauth2 和 userauth3。其缺省值是 deny。

remftp

指用于从非安全接口实现 FTP 登录的认证方法。有效值为 deny、permit、password、NT、snk、sdi、user、userauth2 和 userauth3。其缺省值是 deny。

secauth

指用于从安全接口实现 telnet 登录的认证方法。有效值为 deny、permit、password、NT、snk、sdi 和 user。其缺省值是 deny。

remauth

指用于从非安全接口实现 telnet 登录的认证方法。有效值为 deny、permit、password、NT、snk、sdi、user、userauth2、userauth3。其缺省值是 deny。

secadmin

指用于从安全接口实现 Firewall 配置客户登录的认证方法。有效值为 deny、permit、password、NT、snk、sdi、user、userauth2 和 userauth3。 缺省值对于代理用户为 deny ， 对于主 Firewall 管理员为 NT 。

remadmin

指用于从非安全接口实现 Firewall 配置客户登录的认证方法。有效值为 deny、permit、password、NT、snk、sdi、user、userauth2、userauth3。缺省值对于代理用户为 deny ， 对于主 Firewall 用户为 NT 。

secsocks

来自防火墙非安全方的 Socks 客户程序连接的 Socks5 认证方式。有效值为 deny、permit、password、NT、snk、sdi、user、userauth2 和 userauth3。

如果 Socks5 服务器配置为 User ID/Password 风格的认证方式，而不是 Challenge Response Authentication Methods (CRAM)，SNK 将不工作，因为 Socks5 User ID/Password 协议不能显示 SNK chal

其缺省值是 deny。

remsocks

来自防火墙非安全方的 Socks 客户程序连接的 Socks5 认证方式。有效值为 deny、permit、password、NT、snk、sdi、user、userauth2 和 userauth3。

如果 Socks5 服务器配置为 User ID/Password 风格的认证方式，而不是 Challenge Response Authentication Methods (CRAM)，SNK 将不工作，因为 Socks5 User ID/Password 协议不能显示 SNK chal

其缺省值是 deny。

sechttp

指用于从安全接口实现 HTTP 请求的认证方法。有效值为 deny、permit、password、NT、sdi、user、userauth2 和 userauth3。

HTTP 协议不支持 SNK，因为它未提供显示 SNK 口令查问给用户的方法。HTTP 协议支持 SDI，但是用户将由口令提示，而不是 SDI 通行码。用户应该输入自己的 SDI 通行码。

注: `fwdfuser` 不能在任何其认证方法字段中设置 SNK 或 Firewall 口令。

Firewall 口令参数

password

表明是否提示用户输入口令。缺省情况下，如果已指定了任何一种认证方法或允许口令缺省都将向您作出提示。

pwdvalue

多数情况下用于脚本程序设计，该参数允许在命令行中指定一个参数的值。请注意，该值是在清除文本（即不显示）的状态下输入的并且不可以窃取该值。无缺省值。

userchng

确定在用户数据库中对管理员更改标志作何种设置。设置为 yes 时，管理员更改标志为要求用户在其首次注册时更改口令。缺省值为 No。本参数仅当参数 password=yes 和 pwdvalue=″ 时才有效。

pwlocked

说明口令是否已锁定。当超过最大失败登录数或在封锁前没有使用在最大时间内指定周数的口令，则这将设置成为 yes 。

histexpire

定义了一段时间（用周表示），用户在此段时间内不能再使用口令。其值是一个整数串。有效值为 0 - 52。 0 代表未设置时间限制。缺省值为 0。

histsize

定义了用户不能再使用的前续口令数。其值是一个整数串。 有效值为 0 - 20。只有 `histexpire=0` 时有效。缺省值为 5。

loginretries

定义了系统锁住帐户之前最近一次成功登录之后，尝试登录未成功的次数。其值是一个整数串。 有效值为 0 - 20。缺省值为 10。零或负数表示无限制。一旦用户帐户被锁住，用户只有在系统管理员把 `pwlocked` 设置为 no 时才能登录。

maxage

定义了口令的最长寿命（用周表示）。必须在到期前更改口令。其值是一个整数串。有效值为 0 - 52。0 表示无最长寿命。缺省值为 13。

maxexpired

定义了一个用户能更改已到期口令的最长时间（用周表示），其值大于 maxage 的值。超出该定义时间后，只有管理用户才可以更改此口令。其值是一个整数串。 有效值是 -1 - 26。如果 maxexpired 属性为 0，则表示口令在达到 maxage 的值时期满。如果 maxage 属性为 0，则忽略 maxexpired 属性。缺省值为 3。

maxrepeats

定义了在一个新口令中一个字符可重复的最多次数。有效值为 0 - 8，但 0 是无意义的。8 表示无此最多次数的限制。缺省值为 2。

minalpha

定义了一个新口令中必须存在的字母字符的最少个数。其值是一个整数串。有效值为 0 - 8。0 表示无最少个数。 缺省值为 4。

mindiff

定义了一个新口令中需存在的而老口令中没有的字符的最少个数。其值是一个整数串。有效值为 0 - 8。0 表示无最少个数。 缺省值为 3。

minlen

定义了一个口令的最小长度。其值是一个整数串。有效值为 0 - 8。0 表示无最少个数。 缺省值为 8。

minother

定义了一个新口令中必须存在的非字母字符的最少个数。其值是一个整数串。有效值为 0 - 8。0 表示无最少个数。缺省值为 1。

pwdwarntime

定义了系统在发布口令必需更改的警告之前的天数。其值是一个整数串。 有效值为 0 - 30。零或负数表示将不发布信息。缺省值为 5。

管理功能组

fg_all 如果允许该管理员管理防火墙的各个方面，则输入 yes。缺省值为 no。

fg_dns

如果允许该管理员管理域名服务，则输入 yes。缺省值为 no。

fg_interfaces

如果允许该管理员定义防火墙界面，则输入 yes。缺省值为 no。

fg_logmonitor

如果允许该管理员管理日志监视器阈值，则输入 yes。缺省值为 no。

fg_logs

如果允许该管理员管理日志设施，则输入 yes。缺省值为 no。

fg_mail

如果允许该管理员管理防火墙邮件网关，则输入 yes。缺省值为 no。

fg_netobjs1

如果允许该管理员对网络对象进行基本管理，则输入 yes。缺省值为 no。

fg_netobjs2

如果允许该管理员对网络对象进行高级管理，则输入 yes。缺省值为 no。

fg_pagers

如果允许该管理员管理寻呼机设置，则输入 yes。缺省值为 no。

fg_proxyserver

如果允许该管理员配置防火墙代理精灵程序，则输入 yes。缺省值为 no。

fg_traffic

如果允许该管理员对通信量控制进行管理，则输入 yes。缺省值为 no。

fg_user

如果允许该管理员管理防火墙用户，则输入 yes。缺省值为 no。

要列举出所有防火墙用户或一个指定的防火墙用户的全部属性，请使用:

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

type={short|long}

如果使用用户名，则 type 的缺省值为 long。如果不使用用户名，则其缺省值为 short。

要从防火墙删除一个用户，请使用:

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

第2章 使用报告实用程序

该章讨论了 IBM Firewall 的报告实用程序的使用。 报告实用程序的主要目的是从防火墙日志文件生成管理信息的制表文件。

制表文本文件可被生成并输入到数据库系统，例如 DB2/6000 或 DB2/2 的表中。 管理员然后可以使用结构化查询语言 （SQL） 查询数据并生成报告。实用程序也允许管理员创建一个防火墙日志信息的可读文本文件。

报告实用程序包含了以下程序和文件:

fwlogtxt
从一个防火墙日志文件生成全文本的信息的程序

fwlogtbl
从一个防火墙日志和一个 su 日志以 DEL（定界）格式，生成数据库输入文件的程序。

要使用 fwlogtbl 程序、DDL、DML、以及 DEL 文件，应该有一些关系数据库的知识并使用过适当的关系数据库产品。

fwschema.ddl
适用于定义数据库表的 SQL 数据定义语言（DDL）语句的文件

fwimport.dat
适用于把 DEL 文件输入数据库表的 DB2 输入语句的文件

fwqrysmp.dml
适用于生成采样报告的 SQL 数据操作语言（DML）语句的文件

fwlogcvrt
把 NT 防火墙日志格式转换为 AIX 防火墙日志格式的程序。这使其它供应商的报告工具除了不能识别的新信息外就和以前一样操作。

DDL 和 DML 文件是特定于 DB2 系列的，但可修改以用于其它数据库管理系统。 DEL 格式文件可容易地输入（装入）到 DB2/6000、DB2/2 和其它数据库和文件系统中。它们的简单格式应该允许转换为其它格式（如果必需的话）。

报告实用程序用法

该信息说明了如何从命令行使用报告实用程序。对于从配置客户程序使用报告实用程序的有关信息，请参阅 *IBM eNetwork Firewall 用户指南*

要从命令行查看防火墙日志文件，可使用 **fwlogtxt** 实用程序。 对于更多信息，参阅第22页的『从防火墙日志文件生成消息』。

生成基于日志消息的报告:

1. 安装关系数据库产品。
2. 创建一个空的数据库。
3. 在数据库中创建空防火墙日志表。
4. 从命令行运行 **fwlogtbl** 以产生制表文件。

5. 输入结果文件以构成带日志数据的数据库表。
6. 通过运行 SQL 语句或 SQL 程序产生报告。

注: 开始三步需要做一次，而剩余的步骤每有一新的日志数据就要重复一次。

IBM Firewall 日志格式

防火墙日志文件的每一项有以下格式:

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

其中

- 开始三字段，**date**，**time** 和 **firewall-name** 由防火墙记录设施添加。
- **year** 是四个字符长的年份。
- **pid** 是项申请的线程 ID。
- **Amsg_num** 是连续的整数，报告实用程序用它来从 fw_log.cat 文件访问适当的，转译的消息正文。日志层指示符字母（A）要紧接在数字的 msg_num 之前。该指示符区分生成日志的平台和日志格式中的差异。
- **msg_ID** 是消息的外部号（例如 ICA0001e）。
- **var_1-n** 表示消息变量的值，其中 **n** 是消息定义中的变量号。

注: 不要指示其它记录放至与防火墙日志相同的文件中。 这样的记录将与报告实用程序所要求的的格式不一致并且结果是不可预料的。

使用命令 `fwlogcvrt` 来把该 Windows NT 发行版的日志格式转换为 AIX 的日志格式。可能需要通过这些来使用支持 IBM Firewall AIX 版日志的其它供应商的报告工具。该转换将删除在 msg_num 前的'A'日志层指示符并在 firewall_name 和年份间的冒号两边插入两个空白符。

参数包括:

input 从 Windows NT Firewall 日志重定向标准输入。

output
标准输出，可能重定向至某一文件。

fwlogcvrt syntax

```
fwlogcvrt
```

例子:

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

从防火墙日志文件生成消息

使用命令 **fwlogtxt** 来从防火墙日志文件生成可读的消息。

参数包括:

input 来自防火墙日志文件的标准输入

output
标准输出

fwlogtxt 语法

```
fwlogtxt
```

例子:

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

fwlogtxt 没有参数; 它从标准输入获取信息并把结果放至标准输出。

生成数据库输入文件

使用命令 **fwlogtbl** 来创建, 覆盖或添加至制表文件, 从其用户可构成用于报告生成的数据库表。

参数包括:

input 防火墙日志文件。

output
文件名:

- 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 语法

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

例子:

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

-w 指定应该替换的现存的输出文件。如果该文件不存在，fwlogtbl 创建它。

-a 指定应该添加至现存的输出文件的所生成的文件。如果该文件不存在，fwlogtbl 创建它。

-d 标识输出目录。

OutDir
指定存储所有输出文件的目录。如果没有指定目录，输出文件将存储在当前目录。

-su 指定 LogName 是一个 AIX su 日志文件的名称。这样您的 Windows NT Firewall 可处理从早期的 AIX Firewall 来的防火墙和 su 日志文件。

LogName
指定一个防火墙日志文件或一个 AIX su 日志文件。

输出文件名称为预先定义的，但可在运行 fwlogtbl 后拷贝或重新命名。输出文件为无字符串定界符的定界 ASCII（DEL）文件格式，并使用分号（;）作为列定界符。

对于有关消息的更多信息，参阅第65页的『附录A. 信息』。

使用带报告实用程序的数据库

该章节说明了防火墙提供的用于创建数据库，输入信息到数据库并查询报告的文件。如果有 DB2，则 db2 命令可用于这些文件。（与 db2 命令相似的功能可能存在于其它数据库管理器中。在用于这样的功能时，文件可能需要改动。）

要运行 db2 命令，您必须已安装了 DB2 并定义了一个实例。参阅 DB2 安装文档。最初，你必须使用 DB2 的创建数据库命令来创建一个空数据库。（我们建议叫它'fwlog'。）要这样做，在命令行输入:

```
db2cmd
```

然后在结果 DB2 命令窗口输入:

```
db2 create database fwlog
```

您必须然后连接至 fwlog 数据库:

```
db2 connect to fwlog
```

然后 db2 命令的 -vf 选项可按照以下方法使用:

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

在以下章节中详细说明了这些步骤。在每种情况下，用户应该仔细检查标准输出（在每个例子中重定向至一个文件）。对于输入，有必要检查每个单独输入语句产生的 .msg 文件。

创建表

命令 **db2 -vf fwschema.ddl > schema.out** 创建所需的所有表和索引。最好在安装 Firewall 后不久发出该命令一次。在该例子运行时的当前用户 ID 将是表的建立者 ID。该 ID 可能在以后的 SQL 语句中需要用作一个表名限定词（例如 creatorid.tableName），除非它们在建立者的 ID 下运行。这样，如果不使用建立者的 ID，用户将需要编辑 fwimport.dat 和 fwqrysmp.dml 文件来在每个表名前放置建立者 ID。

ROOTDIR\sample\report\fwschema.ddl 文件包含创建数据库表的 DDL 语句，这些数据库表是用来从 **fwlogtbl** 创建的制表文件接受记录的。 在安装进程期间，*ROOTDIR* 是被选为 IBM Firewall 目标位置的目录。应该查看 schema.out 以确定操作是否成功。在 fwschema.ddl 文件中的语句可用于或修改后用在各种的数据库系统上。（用户不应该更改表和列名。）

输入数据

命令 **db2 -vf fwimport.dat** 从所有 DEL 文件装入数据到由 **db2-vf fwschema.ddl** 命令创建的表中。

ROOTDIR\sample\report\fwimport.dat 文件包含了用于从 *.tbl 文件输入数据到 DB2 数据库的采样语句。就如 第25页的『创建表』 中提到的，如果输入的用户不是表的建立者，建立者 ID 必须放置在每个表名前。

每个输入语句在标准输出产生信息并在 tblname.msg 文件中产生附加的信息，其中 tblname.msg 是特定于每个输入语句的。用户应该检查输出的表格以确定输入是否成功。当用一个程序例如 DB2，在该文件中的所有输入语句时，用户应该指示标准输出为一个文件，然后检查那文件和每个 .msg 文件。每个输入命令产生一个独立的 .msg 文件。同样，用户应该在任何他们要在数据库中有一个用于反映的新日志的时候，重新发出 **db2 -vf fwimport.dat > import.out** 命令。

当输入大的日志文件时，您可能接收到带有指示需要更多内存或磁盘空间的说明的 SQL 错误代码。例如，消息可能是不足的堆空间或事务日志空间。这些错误需要对数据库产品的参数设置选项进行调整或 fwlog 数据库。要获取更多的信息，请参阅 DB2 文档。一个调整 DB2 参数设置选项的临时替代方法把大日志或大制表文件分割为较小的文件。

运行采样查询

db2 -vf fwqrysmp.dml > report.out 命令运行了采样查询。ROOTDIR:\sample\report\fwqrysmp.dml 文件包含了可提供有用的报告数据的基于一些查询需求的采样 SQL 语句。可以这些例子为基础创建你自己的报告。就如 第25页的『创建表』 中提到的，如果输入的用户不是表的建立者，建立者 ID 必须放置在每个表名前。

当从命令行运行查询时，DB2 对于每个输出列分配它可能需要的最大的空间。这可产生一个难以阅读的报告。可能要通过在每个查询中请求较少的列，或在可更好地控制显示的程序中嵌入这些查询语句来实现更多可满意的结果。

在报告实用程序中的用户界面

报告实用程序作为 Firewall 安装的一部分进行安装。他们也可分开安装并在非防火墙主机上运行。配置客户程序或 `fwlogtbl` 命令可用来在防火墙上运行报告实用程序。在非防火墙上，使用命令行。

SQL 表

该章节定义了 SQL 表的布局。

每个防火墙日志消息或 AIX su 日志消息被映象至下列表格之一:

```
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
SESSION
SOCKS_FTP
SOCKS_INFO
SSL_INFO
SU
TUNNEL_CONTEXT
TUNNEL_POLICY
TUNNEL_STATUS
```

您不应该更改表和列名。然而，如果发现截断了其值则可以增加字符列的宽度。

索引

表示一个特定的防火墙事件的运行记录应该在数据库中仅出现一次。如果管理员输入相同的制表文件多次或输入从相同的日志文件派生的另一个制表文件，则一个运行记录可出现多次。

要帮助避免该问题，数据库定义采样文件 fwschema.dll 通过使用这三个字段定义了每个表上的唯一索引:

- 为该记录的源的日志文件的文件名（LOG_FILE）
- 在那日志文件中的该记录的行号（LINE_NUM）
- 该行的重复数，基于 syslog ’上次消息重复 n 次’ 的消息（REPEAT_NUM）

该索引防止您从相同的命名文件装入相同的行号多次。这样，与您的日志文件的细心管理相结合，应该防止了在数据库中日志事件的重复。

添加其它索引至数据库中可能增强大多数普通查询的性能。对于更多信息，咨询数据库文档。

表说明

该章节映象防火墙日志消息至表和列中并指出您可能希望用于报告查询的信息。映象至特定的表的所有消息列出在表的结尾的注释处。为特殊列提供数据的信息列示在该列的说明中。该表包含 IBM Firewall AIX 版的 IBM Firewall NT 版的信息，还有关于两个防火墙的公共信息。

对于有关防火墙日志消息的更多信息，参阅第65页的『附录A. 信息』。

在下列说明的数据类型列中，'int' 意味着 DB2 的 SMALLINT 列类型； 'long int' 意味着 DB2 INTEGER 类型。date-time 数据类型意味着 DB2 TIMESTAMP。在 timestamp，微秒值将总为 ″000000″。

如果说明标记为*必需的*，则必须指定一个值以在表中输入一个记录。

作为唯一索引的三个列和接收日志层指示符的一列从这些表说明中省略，因为它们的定义是恒等的并且通常没有查询它们的缘由。

表 1. ADMIN_ALERT. 该表包含了 a_alert.tbl 文件中的与侵入警报的相关信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID，NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
USERID	char(16)	用户 ID（ICA0001、ICA0002、ICA0003、ICA0004、ICA2001、ICA2002、ICA2003、ICA2026、ICA2043、ICA2068、ICA2167、ICA2168、ICA2170、ICA2173、ICA3001、ICA3012、ICA3018）
ACTION	char（7）	连接 （ICA3012） 或联接 （ICA3018）
NUM_COUNT	int	认证失败数 ICA0001、 ICA0002、ICA0003）；TAG_MSG_NUM 的记录项号（ICA0004）；（ICA9000）的天数
TAG_MSG_NUM	char（8）	标记消息号（ICA0004）
SRC_IP	char（15）	源 IP 地址（ICA2001、ICA2028、ICA2079、ICA2167、ICA3012、ICA3018）
DST_IP	char（15）	目的地 IP 地址（ICA2028、ICA2079、ICA3012、ICA3018）
AUTH_METHOD	char（20）	认证方式（ICA2002、ICA2167、 ICA2170）
NETWORK	char（25）	网络名称 （ICA2001、ICA2002、ICA2167）
HOST_NAME	char（100）	主机名（ICA0003、ICA2002）
TIMEOUT_SEC	int	超时的秒（ICA2026）
CONN_USERID	char(16)	Socks 连接用户名（ICA3001）
APPLICATION	char(30)	应用程序名称，如 telnet、ftp...（ICA2167、ICA2168、ICA2170、ICA3012）

表 1. ADMIN_ALERT (续). 该表包含了 a_alert.tbl 文件中的与侵入警报的相关信息。

列	数据类型	简短说明
注: 相关信息: 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		

表 2. FILTER_ACTIVE_RULE. 该表包含了 f_rule.tbl 文件中的活动 FILTER 规则。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
RULE_NUM	int	规则号（必需的）
RULE	char（150）	规则（必需的）
注: 相关信息: ICA1037		

表 3. FILTER_INFO. 该表包含了 f_info.tbl 文件中的相关于 FILTERS 的错误或一般的资料信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
RULE_NUM	int	过滤器规则号（ICA1005）
ERROR_NUM	int	系统错误号 -- AIX errno 或 Windows NT 上次错误（ICA1007、ICA1008、ICA1009、ICA1011、ICA1013、ICA1015、ICA1021、ICA1023、ICA1024） 与该错误号相应的的文本可通过 _strerrorText 功能获得。Windows NT 最近错误的文本可在格式信息函数或 Win32 程序员参考大全卷 2 的附录 A 处找到。
LOAD_PATH	char（100）	内核扩展装入路径（ICA1011、ICA1012）
DVC_DRV	char（25）	设备驱动程序（ICA1021）
TERM_SIG	char（25）	终止信号（ICA1260）
FILE_NAME	char（100）	文件名（ICA1024）
RC	int	内部的防火墙返回码（ICA1019）
注: 相关信息: ICA1001 ICA1002 ICA1003 ICA1005 ICA1007 ICA1008 ICA1009 ICA1011 ICA1012 ICA1013 ICA1014 ICA1015 ICA1016 ICA1017 ICA1019 ICA1021 ICA1022 ICA1023 ICA1024 ICA1200 ICA1260		

表 4. FILTER_MATCH. 该表包含了 f_match.tbl 文件中的匹配的过滤器规则。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）

表 4. FILTER_MATCH (续). 该表包含了 f_match.tbl 文件中的匹配的过滤器规则。

列	数据类型	简短说明
RULE_NUM	int	规则号（必需的）
ACTION	char（6）	规则类型: 允许, 拒绝等
DIRECTION	char（8）	包传递入站或出站的方向（必需的）
SRC_IP	char（15）	发送人的 IP 地址（必需的）
DST_IP	char（15）	收件人的 IP 地址（必需的）
PROTOCOL	char（7）	高层协议, 如 UDP, IPIP, ICMP, TCP 或 TCP/ACK（必需的）
SRC_PORT	int	• ICMP 的 IP 包类型 • 其它的资源协议端口号（必需的）
DST_PORT	int	• ICMP 的 IP 包代码 • 其它的目的地协议端口号（必需的）
ROUTING	char（5）	包的路由选择溯源: 路由或局域（必需的）
INTERFACE	char（10）	接口类型: 安全或非安全（必需的）
FRAGMENT	char（8）	如果包为片段的或非片段时的标识（必需的）
TUNNEL_ID	int	隧道 ID（必需的）
ENCRYPTION	char（7）	加密算法: DES_CBC 或 CDMF 或无
BYTES	long int	特定包的长度（必需的）
注: 相关信息: ICA1036		

表 5. FILTER_STATUS. 该表包含了 f_stat.tbl 文件中的过滤器的状态更改的信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
DAEMON	char（25）	AIX 过滤器日志精灵程序 （ICA1004）, 或 Windows NT 过滤器记录服务器。
VERSION	int	版本号（ICA1004、ICA1033）
RELEASE	int	发行号（ICA1004、ICA1033）
PACKET_LOGGING	char（8）	信息包日志启用或禁用状态（ICA1035）
注: 相关信息: ICA1004 ICA1032 ICA1033 ICA1034 ICA1035。过滤器规则更新（ICA1032）的细节可从 FILTER_ACTIVE_RULE 表中得到。		

表 6. INTERFACES. 该表包含了 interface.tbl 文件中的接口（适配器）配置消息信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
IP	char（15）	适配器的 IP 地址 （ICA9038、 ICA9039、ICA9040）

表 6. INTERFACES (续). 该表包含了 interface.tbl 文件中的接口（适配器）配置消息信息。

列	数据类型	简短说明
OLD_MASK	char（15）	上一个掩码值 （ICA9040）
NEW_MASK	char（15）	新的掩码值 （ICA9040）
注: 相关信息: ICA9037、ICA9038、ICA9039、ICA9040、ICA9041		

表 7. NAT_INFO. 该表包含了 nat_info.tbl 文件中的网络地址转换消息信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
VERSION	int	NAT 版本号（ICA9033）
RELEASE	int	NAT 发行号（ICA9033）
IP	char（15）	IP 地址（ICA9035、ICA9036）
注: 相关信息: ICA9032、ICA9033、ICA9034、ICA9035、ICA9036		

表 8. PAGER_INFO. 该表包含了 pgr_info.tbl 文件中有关 Firewall 的寻呼功能的信息,

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
USERID	char(16)	用户 ID（ICA4036、ICA4174、ICA4175）
ERROR_NUM	int	系统错误号 - AIX errno 或 Windows NT 上次错误（ICA4371）
PROGRAM	char（25）	程序名（ICA4000）
SIGNAL	int	终止信号（ICA4000）
ID	int	标识符（ICA4036）
PRIORITY	int	优先级（ICA4036）
PERIOD	int	周期（ICA4036）
RETRY_COUNT	int	重试数 （ICA4036、ICA4313、ICA4314、ICA4364、ICA4365）
FROM_ENTRY	char（15）	功能名（ICA4036）
HOST_NAME	char（100）	主机名（ICA4174、ICA4175）
MESSAGE_TEXT	char（250）	页面的文本 （ICA4036、ICA4353 - 4360、ICA4368、ICA4372）
SERVICE	char（25）	服务名（ICA4017）
SOCKET	int	套接字号（ICA4017）
FILENAME	char（100）	文件名 （ICA4154、ICA4351、ICA4352）
注: 相关信息: ICA4000 ICA4001 ICA4007 ICA4017 ICA4036 ICA4154 ICA4168 ICA4174 ICA4175、ICA4300 - 4303、ICA4305 - 4315、ICA4351 - 4360、ICA4362 - 4372）		

表 9. PROXY_FTP. 该表包含了 p_ftp.tbl 文件中的 FTP 会话中 FTP 操作信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID，NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
USERID	char(16)	用户 ID（必需的）
SRC_IP	char（15）	用户的 IP 地址（必需的）
DST_IP	char（15）	远程机器的 IP 地址（必需的）
ACTION	char（5）	文件传送操作: put 或 get （必需的）
FILE_NAME	char（100）	文件名
BYTES	long int	传送的数据量。
SID	long int	唯一的会话 ID（必需的）
注: 相关信息: ICA2075		

表 10. PROXY_HTTP. 该表包含了 p_http.tbl 文件中的代理会话中的 HTTP 操作信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID，NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
STATUS	int	状态（必需的）
SRC_IP	char（15）	用户的 IP 地址（必需的）
REQUEST	char（250）	HTTP 请求的内容（必需的）
BYTES	long int	传送的数据量。
注: 相关信息: ICA2099		

表 11. PROXY_INFO. 该表包含了 p_info.tbl 文件中的相关于 PROXY 的错误或一般的资料信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID，NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
USERID	char(16)	用户 ID （ICA2018、ICA2019、ICA2057、ICA2058、ICA2166、ICA2177、ICA2172）

表 11. PROXY_INFO (续). 该表包含了 p_info.tbl 文件中的相关于 PROXY 的错误或一般的资料信息。

列	数据类型	简短说明
ERROR_NUM	int	系统错误号 - AIX errno 或 Windows NT 上一次错误（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） errno（AIX 系统错误）的文本可经由 _strerror 功能获得。 Windows NT 最近错误的文本可在格式信息函数或 Win32 程序员参考大全卷 2 的附录 A 处找到。
OPTION_VAL	char（20）	选项标志或参数值（ICA2014、ICA2015、ICA2049、ICA2050）
TIME	char（15）	无效时间间隔 （ICA2044、ICA2202）
RC	int	内部的防火墙返回码（ICA2007、ICA2030、ICA2031、ICA2033、ICA2034、ICA2054、ICA2057、ICA2058、ICA2065、ICA2120、ICA2166、ICA2203）
INVOC_NAME	char（20）	在系统错误发生时套接字或端口的调用名称（ICA2055、ICA2056）
AUDIT_TYPE	char（7）	未知 audit-type（7 位十六进制数字） （ICA2004）
HOST_NAME	char（100）	主机名（ICA2106、ICA2107、ICA2126）
FILE_NAME	char（100）	文件名 （ICA2029、ICA2030、ICA2072、ICA2183、ICA2204、ICA2205、ICA2206、ICA2207）
LINE_NUM	int	行号（ICA2029、ICA2030）
PROTOCOL	char（25）	无效协议名称（ICA2112、ICA2116）
CUSTOMIZED_ATTR	char（25）	行号 （ICA2105、ICA2106、ICA2125、 ICA2166）
ODM_ERR_NUM	int	从目标数据管理器来的错误号（ICA2102、ICA2103、ICA2104、ICA2105、ICA2107、ICA2108、ICA2109、ICA2125）
APPLICATION （仅 NT）	char(30)	应用程序名称 （ICA2200、ICA2201、ICA2202、ICA2203、ICA2204、ICA2205、ICA2206、ICA2207）
CALLER (仅 NT)	char（25）	调用函数 （ICA2200、ICA2201、ICA2202、ICA2203、ICA2204、ICA2205、ICA2206、ICA2207）
FAILED_IN （仅 NT)	char（25）	失败的函数 （ICA2201、ICA2203）
注: 相关信息: 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		

表 12. PROXY_LOGIN. 该表了 p_login.tbl 文件中的有关成功的 PROXY 注册的信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
USERID	char(16)	用户 ID（必需的）
APPLICATION	char(30)	应用程序名称 - telnet、ftp, ...（必需的）
AUTH_METHOD	char（15）	认证方式（必需的）
NETWORK	char（25）	网络（安全/非安全 - 也可有附加的信息）（必需的）
HOST_NAME	char（100）	主机名（必需的）
注: 相关信息: ICA2024 ICA2025 ICA2169		

表 13. PROXY_STATUS. 该表包含了 p_stat.tbl 文件中的 PROXY 状态信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
USERID	char(16)	用户 ID（ICA2008、ICA2016、ICA2021）
SRC_IP	char（15）	源 IP 地址 （ICA2000、ICA2008、ICA2010、ICA2011、ICA2012、ICA2013、ICA2141、ICA2180）
DST_IP	char（15）	目的地 IP 地址（ICA2000、ICA2010、ICA2011、ICA2012、ICA2013）
REMOTE_HOST	char（100）	远程主机名称（从防火墙机器的透视） （ICA2021、ICA2022、ICA2027）
SID （仅 NT）	int	会话标识符 （ICA2177、ICA2180、ICA2181 ICA2182）
SOCKET （仅 NT）	char（25）	套接字名称 （ICA2177）
RC （仅 NT）	int	返回或原因码 （ICA2181、ICA2182）
CMD （仅 NT）	char（36）	SMTP 卡 （ICA2182）
注: 相关信息: ICA2000 ICA2010 ICA2011 ICA2012 ICA2013 ICA2016 ICA2021 ICA2022 ICA2027 ICA2097 ICA2098 ICA2141 ICA2163 ICA2164 ICA2165 ICA2177 ICA2180 ICA2181 ICA2182		

表 14. SERVER_INFO. 该表包含了 srv_info.tbl 文件中的有关配置服务器状态和活动的信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
USERID	char(16)	用户 ID（ICA9003、ICA9004）

表 14. SERVER_INFO (续). 该表包含了 srv_info.tbl 文件中的有关配置服务器状态和活动的信息。

列	数据类型	简短说明
ERROR_NUM	int	系统错误号 - AIX errno 或 Windows NT 上次错误（ICA9008、ICA9009） 通过 strerro 功能，errno（AIX 系统错误）的文本是可获得的。 Windows NT 最近错误的文本可在格式信息函数或 Win32 程序员参考大全卷 2 的附录 A 处找到。
注: 相关信息: ICA9003 ICA9004 ICA9005 ICA9006 ICA9007 ICA9008 ICA9009 ICA9010 ICA9011 ICA9012 ICA9013 ICA9014 ICA9015		

表 15. SESSION. 该表包含了 session.tbl 文件中的 SOCKS 和 PROXY 会话启动／停止信息。

列	数据类型（长度）	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX AIX 进程 ID，NT 线程 ID，NT 线程 ID （必需的）
MSG_NUM	int	消息号（必需的）
USERID	char(16)	用户 ID（必需的）
SERVICE_TYPE	char（10）	服务器类型: socks 或代理（必需的）
APPLICATION	char(30)	应用程序名称 - telnet、ftp，....（必需的）
SRC_IP	char（15）	用户的 IP 地址（必需的）
DST_IP	char（15）	远程机器的 IP 地址（必需的）
SESSION_EVENT	char（5）	• 当一个会话建立时开始。 • 当一个会话终止时结束。 （必需的）
BYTES	long int	在会话期间传送的数据量。如果应用程序为 telnet，则这将为 0。
SID	long int	唯一的会话标识符，由 Firewall 生成，基于时钟时间。
注: 相关信息: • Safemail 会话开始: ICA2178 • Safemail 会话停止: ICA2179 • Socks 会话开始: ICA3011 • Socks 会话停止: ICA3015 • 代理 Telnet 会话开始: ICA2036 （AIX 日志） ICA2208，ICA2218 （NT 日志） • 代理 Telnet 会话停止: ICA2077 （AIX 日志） ICA2209，ICA2219 （NT 日志） • 代理 FTP 会话开始: ICA2041 （AIX 日志） ICA2208、ICA2218 （NT 日志） • Proxy FTP 会话停止: ICA2076 （AIX 和 NT 日志） Socks FTP 会话操作的细节在 SOCKS_FTP 表中。代理 FTP 会话操作的细节在 PROXY_FTP 中。		

表 16. SOCKS_FTP. 该表包含了 s_ftp.tbl 文件中的 FTP 会话中的 SOCKS FTP 操作信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX AIX 进程 ID，NT 线程 ID （必需的）
MSG_NUM	int	消息号（必需的）
USERID	char(16)	用户 ID（必需的）
SRC_IP	char（15）	用户的 IP 地址（必需的）
DST_IP	char（15）	远程机器的 IP 地址（必需的）
DATA_BIND	char（5）	• 当数据联接建立时，'开始'（ICA3010）。 • 当数据联接终止时，'停止'（ICA3014）。 （必需的）
BYTES	long int	传送的数据量。
注: 相关信息: ICA3010 ICA3014		

表 17. SOCKS_INFO. 该表包含了 s_info.tbl 文件中的相关于 Socks 的错误或一般的资料信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID，NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
USERID	char(16)	用户 ID（ICA3044、ICA3045、ICA3046、ICA3047、ICA3049）
ACTION	char（7）	连接（ICA3044、ICA3049）或联接（ICA3046、ICA3047）
ERROR_NUM	int	系统错误号 - AIX errno（ICA3013、 ICA3019、ICA3031、ICA3032、ICA3040、ICA3044、ICA3101、ICA3102、ICA3103、ICA3104、 ICA3106、ICA3107、ICA3108、ICA3122、ICA3124、ICA3125、ICA3126、ICA3128）
SRC_HOST	char（25）	源主机名（ICA3019、ICA3035）
DST_HOST	char（25）	目的地主机名（ICA3016、ICA3045）
SRC_IP	char（15）	源地址（ICA3042、ICA3043、ICA3044、ICA3045、ICA3046、ICA3047、ICA3049）
DST_IP	char（15）	目的地地址（ICA3044、ICA3045、ICA3046、ICA3047、ICA3049）
LINE_NUM	int	行号（ICA3022、ICA3023、ICA3024、ICA3025、ICA3026、ICA3109、ICA3110、ICA3111、ICA3112、ICA3115、ICA3116、ICA3117、ICA3118、ICA3119、ICA3120）； 或行数（ICA3113）
EXEC_STATUS	int	Exec 状态（ICA3027）

表 17. SOCKS_INFO (续). 该表包含了 s_info.tbl 文件中的相关于 Socks 的错误或一般的资料信息。

列	数据类型	简短说明
CMD	char（36）	命令，例如登录（ICA3027、ICA3039、ICA3042、ICA3044、ICA3048）注意：对于 ICA3042，命令为十六进制数格式
FILE_NAME	char（100）	文件名（ICA3030、ICA3032、ICA3105、ICA3109、ICA3110、ICA3111、ICA3112、ICA3113、ICA3114、ICA3115、ICA3116、ICA3117、ICA3118、ICA3119、ICA3120）
APPLICATION	char(30)	应用程序名称 - telnet、ftp....（ICA3044、ICA3045、ICA3049）
VERSION	char（10）	十六进制的 Socks 版本号（ICA3043）
注: 相关信息: 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		

表 18. SSL_INFO. 该表包含了 ssl_info.tbl 中的有关 SSL 状态和活动的信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID，NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
Client_IP	char（15）	客户的 IP 地址
注: 相关信息: ICA5015 ICA5022 ICA5023 ICA5028 ICA5029 ICA5036 ICA5039 ICA5060 ICA5063 ICA5082 ICA5120		

表 19. SU. 如果正在加载 AIX su 日志，则该表包含了 su.tbl 文件中的有关 SU 活动的细节。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的） 因为 AIX 不在 su 日志文件中记录年份，所以 DATE_TIME 列的年部分被设置为当前年或上一年，这基于月/日的设置选项（如果月/日晚于当前的月/日，那么它就是上一年。）
FROM_USERID	char(16)	用户 ID（必需的）
TO_USERID	char(16)	用户 ID（必需的）
LOGIN_STATUS	char（7）	登录尝试的状态: 成功或失败（必需的）

表 20. TUNNEL_CONTEXT. 该表包含了 t_cntxt.tbl 文件中的活动 TUNNEL 上下文说明。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID，NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）

表 20. TUNNEL_CONTEXT (续). 该表包含了 t_cntxt.tbl 文件中的活动 TUNNEL 上下文说明。

列	数据类型	简短说明
TUNNEL_ID	long int	隧道 ID（必需的）
SRC_IP	char（15）	源 IP 地址（必需的）
DST_IP	char（15）	目的地 IP 地址（必需的）
ENCRYPTION	char（7）	加密算法 DES_CBC 或 CDMF
注: 相关信息: ICA1043		

表 21. TUNNEL_POLICY. 该表包含了 t_policy.tbl 文件中的 TUNNEL 策略语句。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
POLICY	char（60）	从 fwpolicy 文件读出的策略语句（必需的）
注: 相关信息: ICA1040		

表 22. TUNNEL_STATUS. 该表包含了 t_stat.tbl 文件中的有关 TUNNELS 的状态更改的信息。

列	数据类型	简短说明
DATE_TIME	date_time	操作的日期和时间（必需的）
FIREWALL	char（100）	防火墙机器的全限定名称（必需的）
PID	int	AIX 进程 ID, NT 线程 ID (必需的)
MSG_NUM	int	消息号（必需的）
SESSION_SCKT	long int	会话套接字端口（对于 ICA1038）
MASTER_SCKT	long int	主套接字端口（对于 ICA1038）
TUNNEL_ID	long int	删除的隧道 ID（对于 ICA1041）

注:

相关信息: ICA1038 ICA1039 ICA1041 ICA1042

- 定义的策略细节（ICA1039）可从 TUNNEL_POLICY 表中得到。
- 定义的隧道上下文的细节（ICA1042）可从 TUNNEL_CONTEXT 表中得到。

第3章 SafeMail 插件软件开发包

IBM Firewall SafeMail 网关的主要目的是在安全和非安全网络间转发邮件，同时隐藏安全主机上的名称。

SafeMail 网关不提供任何内容过滤能力。然而，可以编写一个 SafeMail 内容筛选程序，并将它安装在防火墙上作为 SafeMail 网关的插件。 SafeMail 网关插件有能力查看整个电子邮件信息并根据建立的标准来筛选电子邮件。 SafeMail 网关插件可以告诉 SafeMail 网关中止信息的传送或允许信息在网关间流动。

SafeMail 处理概述

当 SMTP 客户连接到 SafeMail 网关时， SafeMail 网关就连接到目的 SMTP 服务器并在接收到客户端的电子邮件行时，同时将电子邮件信息从客户传递到目的服务器。如果必要的话，SafeMail 网关将重写特定电子邮件的标题行来掩盖安全网络主机的名称。

如果安装了内容筛选程序插件， SafeMail 网关将在电子邮件信息通过网关时调用内容筛选程序来筛选电子邮件信息的每一行。 SafeMail 网关同样传递了电子邮件信息的源和目的信息以及其它信息，使得内容筛选程序可以使多个调用各自相关。这在某些地方，如在内容筛选程序决定是否允许信息在防火墙间流动前，分析整个信息时是有用的。

如果 SafeMail 网关必须重写任何标题，以掩盖安全网络上的主机名称，则内容筛选程序插件将在重写标题前调用。

创建 SafeMail 网关插件

要创建和安装 SafeMail 网关插件，则要:

- 为插件 DLL 编写源代码
- 建立 DLL
- 在 Firewall 上安装 DLL

`ROOTDIR\samples\safemail` 包含内容筛选程序插件、必要的头文件以及 IBM Visual Age 和 Microsoft Visual C++ 样本 make 文件的样本代码。在安装进程期间，*ROOTDIR* 是被选为 IBM Firewall 目标位置的目录。

编写源代码

内容筛选程序插件实现了称为 UsrCheck 的功能，它具有下列原型:

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

在 SafeMail 网关有一行电子邮件信息等待内容筛选程序校验时，它是 SafeMail 网关调用的入口点。该功能负责检查电子邮件信息行，如果允许电子邮件信息继续在 SafeMail 网关间流动，则返回 0；如果要 SafeMail 终止信息处理，则返回非零。

参阅在 `ROOTDIR\samples\safemail` 中的 usrcheck.c，以得到在 SafeMail 网关和内容筛选程序间的接口的完整说明。

在校验函数上的 pCheckData 参数是在 ROOTDIR\samples\safemail 的 usrcheck.h 中说明的 C 结构。该结构包含正在处理的电子邮件信息的重要信息，如 SMTP 服务器的源和目的地址，和用于发送和接收 SMTP 服务器的网络（安全和非安全）类型。该结构同样包含会话相关器，允许内容筛选程序将多个调用与相同的电子邮件信息彼此相关。

建立 DLL

当已编写出内容筛选程序的插件时，必须要将它编译和连接到 DLL 中。 DLL 必须命名为 smusr.dll。并且 UsrCheck 入口点必须从 DLL 中调出。参阅 ROOTDIR\samples\safemail 中的样本 make 文件，以得到需要正确建立 DLL 所需的合适的编译和连接切换的示例。样本 make 文件是提供给 IBM VisualAge C++ 和 Microsoft Visual C 的。

安装 DLL

一旦成功建立 smusr.dll，则需要在 Firewall 上安装它。将 smusr.dll 拷贝到 Firewall 的 \bin 中。然后，使用 Windows NT 控制面板中的服务控制管理器来停止和重新启动 IBM Firewall SafeMail 服务器，从而可以装入插件。

IBM Firewall 带有 Firewall \bin 目录中的 smusr.dll。在将 smusr.dll 复制到该目录中时重新命名该 DLL，从而如果将来要删除插件时可以将它恢复。

在本章和下两章中，编译器在实例间分别命名。所有三章都参考相同的两个编译器。

第4章 日志归档程序插件软件开发包

IBM Firewall 日志精灵程序将记录信息写入到用配置客户的 **Log Facilities** 对话框指定的文件中。然后，使用 fwlogmgmt 命令来分阶段归档旧日志记录。典型地，从 Windows NT 调度程序中运行 fwlogmgmt。缺省的， fwlogmgmt 命令将旧日志记录归档到目录中，并使用 Windows NT 压缩命令进行压缩。然而，可以编写一个日志归档程序插件来替换缺省的档案操作程序。

怎样创建日志归档程序的插件

要创建日志归档程序的插件，则要:

1. 为插件 DLL 编写源代码
2. 建立 DLL
3. 在 Firewall 上安装 DLL

ROOTDIR\sample\logarch 目录包含日志归档程序插件的样本代码，它复制了 Firewall 的缺省操作程序和 IBM Visual Age for C++ 的 make 文件。在安装进程期间，*ROOTDIR* 是被选为 IBM Firewall 目标位置的目录。

编写源代码

日志归档程序插件必须实现一系列函数，它们是 Firewall 用来执行归档功能的。这些函数的原型是在 ROOTDIR\sample\logarch 目录中的 fwarch.h 中定义的。

这些函数实现了基本的归档功能，如添加文件到档案中、从档案中抽取文件、刷新档案和在档案中列出文件。

参阅 ROOTDIR\sample\logarch 目录中 fwarch.h 的样本代码以得到这些函数的详细信息。

建立 DLL

当已编写入日志归档程序插件时，必须要将它编译和连接到 DLL 中。 DLL 必须命名为 fwarch.dll。所有在 fwarch.h 中列出的函数必须从 DLL 中调出。

IBM VisualAge for C++ 的样本 make 文件（用来将样本代码建立到适当的 DLL 中），在 ROOTDIR\sample\logarch 目录中提供。

安装 DLL

在成功建立 fwarch.dll 后，将它安装到 Firewall 中。将 fwarch.dll 复制到 ROOTDIR\bin 目录中。

Firewall 的缺省 fwarch.dll 同样在该目录中。在将替换 DLL 复制到该目录中以前，备份或重新命名该 DLL。

同样，确保在替换缺省 DLL 以前，没有运行 fwlogmgmt 且没有运行 IBM Firewall 日志精灵程序。使用服务控制管理器来停止 IBM Firewall 日志精灵程序，然后在替换 DLL 后重新启动它。

第5章 提供各自的认证方式

本章给出了有关提供各自认证方式的信息。

用户提供的认证

提供一用户认证的样本，它位于目录 ROOT_DIR\bin\authsdk 中。包括的文件有:

- authschm.h - 界面定义文件
- authus.cpp - 样本方案的源文件
- gwauth4.lib - Firewall 库
- msvc++.mak - Microsoft Visual C 编辑文件
- schmname.h - 界面定义文件
- vac++.mak - IBM Visual Age 编辑文件

使用下列命令来编译 IBM 的 Visual Age 的用户认证样本:

- nmake -f vac++.mak - 建立 DLL
- nmake -f vac++.mak install - 建立和安装 DLL
- nmake -f vac++.mak clean - 清除本地目录

使用下列命令来编译 Mircosoft 的 Visual C 的用户认证样本:

- nmake -f msvc++.mak - 建立 DLL
- nmake -f msvc++.mak install - 建立和安装 DLL
- nmake -f msvc++.mak clean - 清除本地目录

使用软件开发包来创建用户提供的认证方案

IBM Firewall 提供插件接口使第三方认证安全性产品的集成生效。通过写出插入 Firewall 认证方案接口的认证方案 .dll 来做到这一点。

Firewall 认证处理概述

下列防火墙服务必须在允许用户访问防火墙服务之前认证用户:

- IBM Firewall 配置服务器
- IBM Firewall 代理 FTP 精灵程序
- IBM Firewall 代理 HTTP 精灵程序
- IBM 防火墙 Telnet 精灵程序
- IBM 防火墙 Socks 服务器

Firewall 提供了下列认证方案:

Deny All
总是拒绝用户访问服务器。

Permit All
无需任何查问地允许用户访问服务器。

防火墙口令

用在 Firewall 用户数据库中定义的口令查问用户。

NT 注册口令

查问用户（他或她）的 Windows NT 注册口令。

SecureNetKey

用 AssureNet Pathways SecureNet Key 认证用户。

SecurID Card

用 Security Dynamics SecurID 安全性卡认证用户。

使用的认证方案可基于每个和每个服务器而定义。例如，Firewall 可配置为这样：当用户 *John* 尝试注册至 IBM Firewall 配置服务器时，查问他的 Windows NT 注册口令。但是当 *John* 想使用 IBM Firewall Telnet 代理时，他使用 SecurID Card 认证。然而，当用户 *Mary*，尝试注册至 IBM Firewall 配置服务器时，将查问她的 Firewall Password。参阅 *IBM eNetwork Firewall 用户指南* 的管理章节以获取有关 Firewall 提供的认证方案和如何为每个用户定义它们的详细信息。

除了 IBM Firewall 提供的认证方案，还可最多安装三个用户提供的认证方案。您可以写下这些方案来与已经存在的安全性基础进行交互，或者从第三方安全性供应商那儿获得它们以使用 Firewall 来集成其产品。

Firewall 中包括用户提供的每个认证方案，由实现认证方案 API 的 DLL 表示。该 API 定义如何用 Firewall 使认证方案注册自己和 Firewall 如何传递认证请求给它。

创建用户提供的认证方案

创建用户提供的认证方案包括下列步骤:

- 编写源代码来实现认证方案 API
- 编译和链接源代码至 DLL
- 在 Firewall 上安装 DLL

需要用来创建用户提供的认证方案的 C 源代码头文件和库文件，同样的还有 Microsoft Visual C++ 和 IBM Visual Age for C++ 的样本代码和样本制作文件，都可在 `ROOTDIR\bin\authsdk` 中找到。

编写源代码

所有认证方案必须做两件事:

1. 用 Firewall 注册它们自己
2. 实现 AuthSchmFn

用 Firewall 注册: Firewall 服务器启动之前，Firewall 尝试加载每个在 `\bin\authschm` 子目录中找到的 DLL。每个 DLL 加载后，其初始化例行程序必须调用 Firewall 中名为 registerAuthSchm 的函数以向 Firewall 注册。

registerAuthSchm 函数原型定义在 authschm.h 头文件中。它带有单个指向 AuthSchmInfo 结构的参数，该函数也定义在 authschm.h 中。 AuthSchmInfo 结构把认证方案名称与适当的 Firewall 为了传递认证请求至认证方案而调用的 AuthSchmFn 地址关联在一起。

用户提供的认证方案必须使用下列三个名称之一:

1. 用户
2. 用户认证2
3. 用户认证3

在头文件 schmname.h 中为这些名称定义了符号名。用户提供的认证方案应该设计为允许端点用户指定使用三个名称中的那个，这样多个用户提供的认证方案可以安装在相同的 Firewall 上，而不必担心两个不同的方案需要相同的名称。

DLL 初始化例行程序成功调用注册 AuthSchm 并返回至调用者之后， DLL 应该准备处理认证请求。由于该原因，有必要在 DLL 初始化例行程序中也进行一些方案指定的初始化。

实现 AuthSchmFn: 每个认证方案 DLL 都必须使用在 authschm.h 中定义的原型来实现称为 AuthSchmFn 的功能。AuthSchmFn 函数有一个参数，是指向 AuthReq 结构的指针。AuthReq 结构是简单的 C 结构，它包含所有关于当前认证请求的信息。AhthReq 在 authschm.h 中定义。 AuthReq 结构包含进行认证用户的名称、请求认证的 Firewall 组件/服务器以及其它有关请求的信息。要获取 AuthReq 结构中信息的完整列表和说明，请参阅 authschm.h 中的注解。

除了用户名和 Firewall 组件，在 AuthReq 结构中还有三个对于实现认证方案特别重要的参数:

gwaput

这是 Firewall 提供的调用返回例行程序的地址，在认证方案需要发送信息至用户的任何时侯都可以使用。例如，如果认证方案需要发出提示信息给用户，它需要调用在 gwaput 参数中提供的入口点来做到这一点。gwaput 调用返回函数是在 authschm.h 中由 AuthSchmPut 类型定义的原型。参阅 AuthSchmPut 类型定义的注解以获取完整的参数列表，这些参数 AuthSchmFn 必须在该调用进行传递。

gwaget

这是 Firewall 提供的调用返回例行程序的地址，在认证方案需要检索来自进行认证的最终用户响应的任何时侯都可以使用。例如，如果认证方案需要从用户处得到口令，它需要调用在 gwaget 参数中提供的入口点来做到这一点。gwaget 调用返回函数是在 authschm.h 中由 AuthSchmGet 类型定义的原型。参阅 AuthSchmGet 类型定义的注解以获取完整的参数列表，这些参数 AuthSchmFn 必须在该调用进行传递。特别重要的一个参数是回送参数。AuthSchmFn 可以使用该参数来指示是否应该把用户响应回送他。

opaque_data

Firewall 使用 opaque_data 字段来把至 AuthSchmFn 的调用和至其调用返回例行程序的调用关联起来。调用 gwaget 或 gwaput 例行程序时， AthSchmFn 应该传入与在 AuthReq 结构中被传入的值相同的 opaque_data 的值。

注意: 认证方案必须能与所有 Firewall 组件进行交互。一些 Firewall 组件可支持多个与最终用户的口令/应答对话。这些组件称为交互式 Firewall 组件。由于其协议的性质，一些 Firewall 组件只可支持单个口令查问/应答。这些称为非交互 Firewall 部件。

用户提供的认证方案必须可根据在 AuthReq 结构的组件字段中所指示的调用它的 Firewall 组件而修改其行为。组件字段的有效值定义在 authschm.h 中。组件字段当前的有效值是:

表 23. 组件字段的有效值

AuthSchm.h 中的组件符号	Firewall 组件	交互/非交互
AUTHSCHM_UNKNOWN	新的或不能识别的 Firewall 组件	假设它是交互式的
AUTHSCHM_REMADMIN	配置服务器	交互式
AUTHSCHM_FTP	FTP 代理	非交互式
AUTHSCHM_TELNET	Telent 代理	交互式
AUTHSCHM_HTTP	HTTP 代理	交互式
AUTHSCHM_SOCKS_PWD	使用口令认证的 Socks 服务器	非交互式
AUTHSCHM_SOCKS_CRAM	使用 CRAM 认证的 Socks 服务器	交互式
AUTHSCHM_REMIPSEC	远程客户 IPSEC 服务器（当前在 Windows NT 上不可用）	交互式

AuthSchmFn 完成其处理后，必须用在 authschm.h 定义的 GWA 返回码之一返回至调用者。该返回码用来指示用户是否成功认证和在处理期间是否出现错误:

表 24. GWA 返回码

返回码	方法
GWA_OK	处理期间未发生错误且已成功认证用户
GWA_DENY	处理期间未发生错误，但用户认证未成功
GWA_IOFAILURE	在尝试发送提示至用户或从用户处获得响应时发生错误。典型地是在调用返回例行程序出错时返回。
GWA_BUFFERTOOSMALL	AuthSchmFn 函数无法检索来自用户响应，因为它不能分配足够的缓冲区来接收响应。
GWA_NOAUTHFN	错误 - 与认证无关
GWA_FNNOTREG	错误 - 与认证无关
GWA_RSVNAME	错误- 认证请求包含保留的和不能由该认证方案使用的名称。
GWA_BADNETTYPE	错误 - 与认证无关
GWA_BADAPP	错误 - 与认证无关
GWA_BADADDR	错误 - 提供给认证请求的地址无效
GWA_MEMSHORTAGE	错误 - 未分配内存所以不能处理认证请求
GWA_USERDBFAIL	错误 - 不能查询需要的数据库
GWA_REGFAILED	错误 - 与认证无关
GWA_AUTHERROR	错误 - 认证方案特定的错误条件
GWA_INTERNAL	错误 - 认证方案中的多种错误条件

AuthSchmFn 返回至 Firewall 时，如果返回码是 GWA_OK，认为用户已成功认证并对请求的服务器进行了访问。 GWA_DENY 认为是无错误条件，但拒绝用户访问请求的服务器。所有其它返回码认为是错误条件且拒绝用户访问请求的服务器。

编译和链接至源代码： 把源代码编译并链接至 DLL 时，必须使用 `\bin\authsdk` 目录中提供的 gwauth4.lib 把 DLL 链接至 gwauth4.dll，以分解 authschm.h 中定义的入口点名称。同样的，AuthSchmFn 不是从 DLL 输出的，这一点十分重要。IBM VisualAge for C++ 和 Microsoft Visual C++ 的样本制作文件在 `\bin\authsdk` 目录中提供。

安装 DLL： 一旦成功建立了 DLL，把它拷贝到 `ROOTDIR\bin\authschm` 目录中并重启动 Firewall 机器。必需重新启动是为了使 Firewall 加载 DLL 并注册 DLL 的认证方案。

把所有的都结合起来： 第47页的图 1 显示了认证请求处理期间认证方案如何加载，密钥函数如何调用。

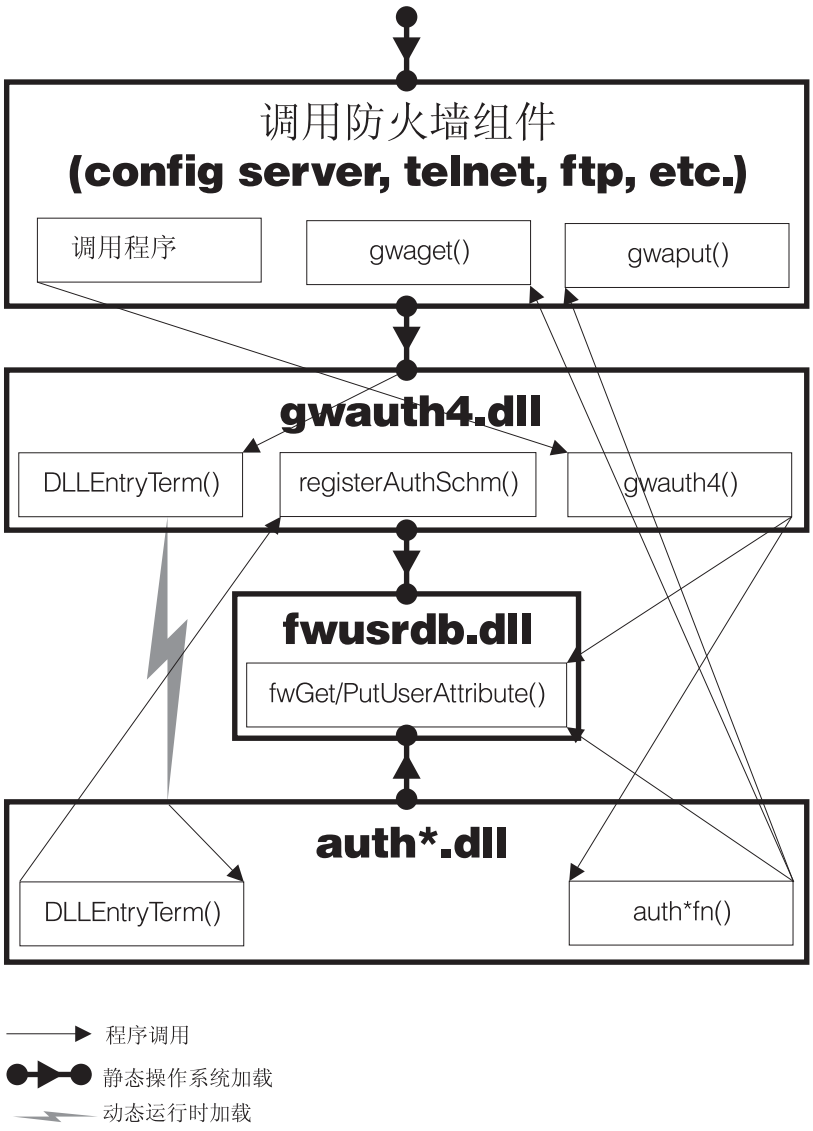

图 1. DLL 初始化和登记

需要使用认证服务器的 Firewall 部件链接至名为 gwauth4 的 Firewall DLL。gwauth4 dll 加载后，调用其 DLLEntryTerm 例行程序，且该例行程序将尝试在运行时间加载 `ROOTDIR\bin\authschm` 中的所有 DLL。 如果未能加载认证方案 DLL，不会认为是 gwauth4 dll 加载的错误。gwauth4 dll 串行化这些加载尝试。

认证方案的 DLLEntryTerm 例行程序运行后，它们负责用 gwauth4.dll 注册认证方案。通过调用 registerAuthSchm 来做到这一点。authschm dll 对每个 DLL 支持的认证方案都需要调用 registerAuthSchm 一次。由 registerAuthSchm 函数传入的 AuthSchmInfo 结构把存储在用户数据库中的认证方案和 AuthSchmFn 函数的入口点关联在一起。登记函数将拷贝传入其中的结构，使 authschm dll 可以在需要时重用/修改该结构。Authentication 方案 DLL 也负责释放 AuthSchmInfo 结构。

registerAuthSchm 函数负责建立表示所有已注册的认证方案的链接列表。gwauth4 的 DLLEntryTerm 例行程序将初始化列表锚为 NULL。然后时 authschm DLL 调用 registerAuthSchm 函数时，它将:

1. 扫描认证方案列表，查找与传入名称相同的输入项。如果存在，从列表中删除并删除所有与其关联的存储器。
2. 建立基于 AuthSchmInfo 结构的 AuthSchmEntry 结构并把它添加到认证方案列表中。
3. 返回调用者注册是否成功的指示（成功: GWA_OK，失败: GWA_REGFAILED）。

gwauth4 的 DLLEntryTerm 完成每个 authschm dll 的运行时间的加载和 authschm DLL 注册其认证方案后，gwauth4 的 DLLEntryTerm 例行程序将返回至调用者。在该点，其它组件可开始调用 gwauth4 函数请求认证服务。

gwauth4.dll 卸出后，将再次调用 DLLEntryTerm 例行程序终止处理。调用该例行程序去终止时，它将删除 AuthSchmList 中的所有 AuthSchmEntry 项和关联的存储器。做了这些后，认证方案就不需要自己去从 Firewall 注销。

认证请求处理: Firewall 服务器需要认证用户时，它调用 gwauth4.dll 中的函数。gwauth4 带来调用组件的信息并查询 Firewall 用户数据库来确定用来处理请求的认证方案的名称。

一旦 gwauth4 确定了认证方案的名称，它扫描已注册的认证方案的列表以寻找相同名称的方案。如果找到了相同名称的已注册方案，它建立 AuthReq 结构来表示当前请求并调用与名称相关的认证方案 DLL 的入口点。

由 gwauth4 调用的 AuthSchmFn 函数处理请求并在需要与最终用户交互时调用 gwaget 和 gwaput 调用返回函数。完成其处理后，它用适当的的返回码返回到对 gwauth4 的控制。

gwauth4 写适当的日志记录把认证请求编成文档并返回产生请求的 Firewall 组件，propagating 从认证方案 DLL 接收到的返回码。

第6章 使用 Make Key File Utility（MKKF）

安全的 SSL 网络连接需要:

- 为 SSL 配置配置服务器
- 创建了用于安全通信的密钥
- 指定了服务器上受托的超级用户
- 存放了密钥文件口令

使用 MKKF 来创建初始服务器密钥、密钥环文件并确认请求。MKKF 同样用来接收初始确认到密钥环中并保存您的密钥文件口令。

创建密钥文件

运行该实用程序时，必须使用 Windows NT 管理员帐户注册。

1. 到 ROOTDIR\config 目录中并启动密钥实用程序，通过输入:

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

   MKKF Key Manager
   Copyright IBM Corp. 1996
   All Rights Reserved
   ```

2. 创建新的密钥环文件。

   ```
   Key Ring Menu
   Currently Selected Key Ring: (none)

   N - Create New Key Ring File
   O - Open Key Ring File
   X - Exit

   Enter a command: n
   ```

   如上所示，输入 'n'，创建一新的密钥文件。

   将提示需要密钥文件的文件名。可以使用任何文件名，但必须以 .kyr 结尾。缺省的，防火墙寻找一名为 fwkey.kyr 的文件。

   输入密钥环文件的名称，或按 ENTER 接受 **fwkey.kyr** 的系统默认值。

   MKKF 将创建新的密钥文件并显示密钥环菜单。注意密钥文件将列示为当前选中的密钥环。

3. 创建新的密钥并确认请求。

   ```
   Key Ring Menu
   Currently Selected Key Ring: fwkey.kyr

   N - Create New Key Ring File
   O - Open Key Ring File
   S - Save Key Ring File
   A - Save Key Ring as Another File
   P - Set Password for Key Ring File
   C - Create Stash File for Key Ring File
   R - Receive a Certificate into a Key Ring File
   W - Work with Keys and Certificates
   ```

```
X - Exit

Enter a command: w
```

输入 'w'，如上所示的那样，到密钥菜单中。

```
Key Menu
Currently Selected Key Ring: fwkey.kyr
Selected Key Entry: (none)

L - List/Select a key to work with
C - Create a New Key and Certificate Request
I - Import a key from an Armored key file
X - Exit this menu

Enter a command: c
```

如前所示，输入 'c'，创建一新的密钥。

在密钥文件可存储密钥前，密钥文件必须有口令保护。MKKF 将提示输入口令用来保护密钥文件。在输入时，口令将不显示。 MKKF 会询问口令是否应该到期。如上所述，输入 'n':

```
Enter password to use for the key file:
password
Enter the password again for verification: password
Should the password expire?
Enter Y for yes or N for no:
n
Password successfully set.
Press ENTER to continue
```

MKKF 提示将创建的密钥类型。

```
Choose Certificate Type Menu
S - PEM Certificate Request Format (Private Enhanced Message)
P - PKCS10 Certificate Request Format
C - Cancel

Enter a command: s
```

如前所示，输入 's'，创建 PEM 证明请求格式。 MKKF 将生成一空的证明:

```
Compose Secure Server Certificate Menu

Current Certificate Information
Key Name: (none)
Key Size: 0
Server Name: (none)
Organization: (none)
Organization Unit: (none)
City/Locality: (none)
State/Province: (none)
Postal Code: (none)
Country: (none)

M - Modify the Certificate Fields
R - Ready To Create Key and Certificate Request
C - Cancel

Enter a command: m
```

输入 'm' 以修改空的证明。将提示输入新证明的信息:

- 输入要使用的名称。该名称可以是任何字符串并只能用于 MKKF 实用程序:

```
Enter a name to use for the key entry:

Firewall Key
```

- 输入密钥的大小。IBM Firewall 只带有可输出的 MKKF 版本。最大的密钥大小为 1024。

```
1:   508
2:   512
3:   768
4:   896
5:   1024
Enter the number corresponding to the key size you want:

2
```

- 输入防火墙的全限定 TCP/IP 主机名（例如， jupiter.raleigh.ibm.com）：

```
Enter the server's fully qualified TCP/IP domain name or press
Enter by itself to leave the field blank

jupiter.raleigh.ibm.com
```

- 输入组织名称与证明相关联。（例如，公司名称）：

```
Enter Organization Name for the certificate
or press ENTER by itself to leave the field blank.

AAA Inc.
```

- 输入组织单元名称。（例如，部门名称）：

```
Enter Organizational Unit Name for the certificate
or press ENTER by itself to leave the field blank.

Network Security Products
```

- 输入将使用证明的城市:

```
Enter Locality/City Name for the certificate
or press ENTER by itself to leave the field blank.

RTP
```

- 输入州或省。

  注: 与证明规范相对应，该字段必须是三个字符的最小值，因此两字母的州名缩写无效。

```
Enter State/Province Name for the certificate
or press ENTER by itself to leave the field blank.
State/Province must be at least three characters long.

N.C.
```

- 输入邮政编码与证明相关联。（这与邮递区号是一回事）：

```
Enter Postal Code for the certificate
or press ENTER by itself to leave the field blank.

27709
```

- 输入两字母的国家代码:

```
Enter Country Code for the certificate
or press ENTER by itself to leave the field blank.
Country code must be exactly two characters long.

US
```

在 MKKF 收到所有的信息后，将显示证明:

```
Compose Secure Server Certificate Menu

Current Certificate Information
Key Name: Firewall Key
Key size: 512
Server Name: jupiter.raleigh.ibm.com
Organization: AAA Inc.
Organizational Unit: Network Security Products
City/Locality: RTP
State/Province N.C.
Postal Code: 27709
Country: US

M - Modify the Certificate Fields
R - Ready To Create Key and Certificate Request
C - Cancel

Enter a command: r
```

如果在证明信息中有任何错误，可输入 'm' 校正。如果信息正确，输入 'r' 创建新的密钥和关联密钥文件。

MKKF 将提示用一文件来存储证明。可以使用任何文件名，但经常遵循的约定是使用相同的基名作为密钥文件并添加 .cert 作为扩展名:

```
Enter file to store the certificate request in:
fwkey.cert
Creating Private Key...
Private key was successfully created.
Creating certificate request...
certificate request was successfully created
Adding new key to key file.
The new key and certificate request were created successfully.
Press ENTER to continue
```

4. 使新创建的密钥成为系统默认值。

   在密钥和证明创建后，将显示密钥菜单。新创建的密钥将显示为选中的密钥输入项:

```
Key Menu
Currently Selected Key Ring: fwkey.kyr
Selected Key Entry: Firewall Key

L - List/Select a Key To Work With
S - Show Information about Selected Key
```

```
D - Delete Selected key
C - Create a New Key and Certificate Request
I - Import a Key From an Armored Key File
E - Export Selected Key To an Armored Key File
F - Make Selected Key the Default Key for this Key Ring
U - Unmark Selected Key's Trusted Root Status
R - Create A Certificate Request for Selected Key
X - Exit This Menu

Enter a command: f
```

必须使新创建的密钥成为密钥文件中的缺省密钥。如先前的那样输入 'f'。将提示确认操作:

```
Key Menu
Currently selected key: Firewall Key
Are you sure you want to make this key the default?
Enter Y for yes or N for No:
y
Key was made the default key.
Press ENTER to continue
```

在密钥标记为系统默认值后，显示了密钥菜单:

```
Key menu
Currently Selected Key Ring: fwkey.kyr
Selected Key Entry: Firewall Key

L - List/Select a Key To Work With
S - Show Information about Selected Key
D - Delete Selected key
C - Create a New Key and Certificate Request
I - Import a Key From an Armored Key File
E - Export Selected Key To an Armored Key File
F - Make Selected Key the Default Key for this Key Ring
U - Unmark Selected Key's Trusted Root Status
R - Create A Certificate Request for Selected Key
X - Exit This Menu

Enter a command: x
```

输入 'x' 退出密钥菜单。

5. 接收证明到密钥环文件中。

   将显示密钥环菜单:

```
Key Ring Menu
Currently Selected Key Ring: fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
C - Create Stash File for Key Ring File
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: r
```

注: 因为防火墙没有使用 SSL 用于认证目的，所以证明没有必要用证明权限来标记。

```
Enter file name or press ENTER for Cert.txt.
fwkey.cert
This is a self-signed certificate. Add it to the key file?
Enter Y for yes or N for no:
y
Certificate added to key ring.
Press ENTER to continue
```

6. 创建密钥文件的存贮文件。

   在证明添加到密钥环中后，显示密钥环菜单:

```
Key Ring Menu
Currently Selected Key Ring: fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
C - Create Stash File for Key Ring File
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: c
```

   需要创建密钥文件的存贮文件。如先前那样输入 'c'。MKKF 将使用相同的基名作为密钥文件并将 .sth 作为扩展名:

```
Stashed password file saved to fwkey.sth
Press ENTER to continue
```

   在存贮文件创建后，显示密钥环菜单。

```
Key Ring Menu
Currently Selected Key Ring: fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
C - Create Stash File for Key Ring File
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: x
```

   密钥文件现在可以使用。如前所示，输入 'x' 退出 MKKF 并输入 'y' ，保存对密钥文件的更改如下:

```
Key ring file has been changed. Save?
Enter Y for yes or N for no:
y
Key ring saved to fwkey.kyr
Press ENTER to continue
#
```

7. 更新配置文件。

   在创建密钥文件后，必须在配置服务器参数文件中使用fwcfgsrv命令指定密钥文件名称。

如果使用配置服务器的 SSL 加密，将需要使用fwcfgsrv命令来设置 encryption=ssl 选项 。

使用 fwcfgsrv 命令后，关闭并重新启动服务器服务。

第7章 故障检测与测试

本章告诉您当设置和配置 IBM Firewall 时，如何检测所遇到的一些常见问题。

若有问题，首先，用调试优先级创建一个防火墙日志，以增加发送到日志的信息。参阅 第5页的『日志文件管理』 以获取更多的信息。

安装和设置

筛选程序支持失败

问题说明

接收这些错误信息。

```
Filter support verification failed. Socket creation call failed.
A file or directory in the path name does not exist.
```

产生此问题的原因在于安装防火墙之后未重引导。

建议的操作

重新引导防火墙，并重试该过程。

路由选择问题

IBM Firewall 在标题为*测试 IP 路由选择*的**安全性策略**对话框中提供了一项功能，该功能可用于调试路由选择问题。启用该复选框，激活“连接”配置，并启用“连接规则记录”。 然后检查防火墙日志 以查看所有穿越防火墙的包的详细信息。

需要执行这些测试，则首先使用 IP 地址，然后使用主机名。若通信量路由正确地使用了地址但未使用名称，详见 第59页的『DNS 问题』。

无法从防火墙远程侦测主机

问题说明

网络接口配置不正确。

建议的操作

参阅操作系统文档。

问题说明

连接到非安全网络的配置不正确。

建议的操作

与您的 Internet 服务供应商联系，以求帮助。

问题说明

若安全网络被隔离在路由器后面，则防火墙必须拥有一个连到该路由器的静态路径。使用 `netstat -rn`，以验证静态路径选择:

```
netstat -rn
```

对于“协议簇 2”，输出应该如下列所示:

```
Destination  Gateway          Flags     ....
default      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
```

图 2. netstat -rn 的输出的范例.

nrr.nrr.nrr.nrr

为系统默认路由，代表到 internet 的路由器。系统默认路由为静态路由（Flag=UG）。

nnn.nnn.nnn

代表非安全域。这是一个接口路由（Flag=U）。

nnn.nnn.nnn.nnn

代表非安全接口。

sss.sss.sss

代表安全域。这是一个接口路由（Flag=U）。

sss.sss.sss.sss

代表安全接口。

ss1.ss1.ss1

代表网络安全方的子域，srr.srr.srr.srr 代表到那个子域的路由器。这是一个静态路由（Flag=UG）。

127.0.0.1

是回送或本地主机。 这是一个接口路由（Flag=U）。

每个接口都应该有一个接口路由，并且系统默认路由应该指向防火墙非安全方上的路由器。

建议的操作

添加静态的路由至路由器。与路由器管理员联系。使用 `route add` 命令。

问题说明

安全接口上的子网掩码或正在尝试联系的主机是不正确的。

建议的操作

使用客户程序的配置实用程序，以校正掩码设置。

无法从安全主机远程侦测非安全主机（或反之）

问题说明

每个与防火墙邻近的路由器必须包含一个静态路由，该静态路由将防火墙指定为防火墙之上到目标网络的网关。

建议的操作

与路由器管理员联系。

问题说明

若安全网络使用了未经注册并在非安全网络上无法路由的地址，其中也包括如在 RFC，1597 中所指定的专用地址，则包将不回送至发送人。

建议的操作

使用一个带有经注册地址的客户程序。

DNS 问题

防火墙 DNS 通过查询安全名称服务器来分辨名称。由安全名称服务器分辨安全网络中的所有名称。它将非安全名称的请求转发到防火墙名称服务器。由防火墙名称服务器通过查询非安全名称服务器来分辨请求。

DNS 问题可能影响其它防火墙操作的区域。如果问题与 DNS 不明显有关，最好也检查一下 DNS。

这里有一些例子，按步骤地指导您通过使用 nslookup 实用程序分离该问题。在这些例子中，我们将使用下列值:

www.ibm.com

代表非安全网络上一个任意的主机名

nns.nns.nns.nns

代表非安全名称服务器的地址

sns.sns.sns.sns

代表安全名称服务器的地址

host.secure.company.com

代表安全网络内部任意的主机名称

127.0.0.1

代表防火墙的回送地址。

这些值可从配置客户的**域名服务器**对话框获得。在练习过程中，您将需要使用这些值。

注: nslookup 命令要求在主机名后面添上附加点，用以防止将安全域名加到 nslookup 后面。

未配置 DNS

问题说明

未配置防火墙的 DNS 设施。

建议的操作

完成**域名服务器**对话框。

DNS 查询失败或超时

问题说明

防火墙通信量控制不允许 DNS 包流动。

建议的操作

转至**安全性策略**对话框，选中*允许 DNS 查询*复选框并重新激活通信量控制。

nslookup www.ibm.com. nns.nns.nns.nns 失败

问题说明

非安全名称服务器未使用所指示的地址，或其配置不正确。

建议的操作

与您的 DNS 服务供应商联系，以便获得一个有效的名称服务器地址。

nslookup www.ibm.com. 127.0.0.1 失败

问题说明

Microsoft DNS 服务器可能不运行。转至服务控制管理程序以确定它是否运行。

建议的操作

使用服务控制管理程序来启动 DNS。

nslookup host.secure.company.com. sns.sns.sns.sns 失败

问题说明

安全名称服务器已关闭。

建议的操作

重新启动名称服务器。

nslookup www.ibm.com. sns.sns.sns.sns 失败

问题说明

未正确配置安全名称服务器，所以不能与 IBM Firewall 交互。

建议的操作

参考 *IBM eNetwork Firewall 用户指南*，以获得配置需求。

配置客户程序

服务器不响应

问题说明

配置客户机和配置服务器使用的是不同的语言。

建议的操作

在配置客户注册面板上，选择防火墙已安装的语言。

问题说明

SSL 加密的配置可能不正确。

建议的操作

确定已在客户程序的注册面板中选定了 SSL。使用服务控制管理程序，停止并重新启动防火墙配置服务器。

问题说明

可能禁用了防火墙配置服务器。

建议的操作

保证防火墙配置服务器正在运行。

问题说明

防火墙配置可能正在监控一个非标准端口。

建议的操作

检查 c:\winnt\system32\drivers\etc\services 并保证它包含行 ibmfwrcs 1014/tcp。 若要使用在不同端口上的服务器，则相应地编辑 ibmfwrcs 1014/tcp，并保证指定了客户程序的注册面板中的新端口。 使用服务控制管理程序，停止并重新启动配置服务器。

问题说明

防火墙的通信量控制可能不允许其与配置服务器通讯。这仅影响正在远程主机上运行的配置客户程序。

建议的操作

为正在运行配置客户程序的机器与防火墙之间编码一个连接。配置客户程序应该是连接的源，而防火墙是目的地。重新生成并激活所做的更改。请参阅 *IBM eNetwork Firewall 用户指南*以获取更多的信息。

问题说明

可能未将配置服务器配置为允许从远程主机注册。

建议的操作

使用 fwcfgsrv 命令来验证 localonly 参数已设置为 no。

无法注册提到配置服务器

问题说明

每个在防火墙上得到认证的用户名可能配置为使用任何认证方式。使用 Deny all 来禁止用户使用特定的服务。

建议的操作

检查正在使用的用户名的“安全管理”和“非安全管理”字段。这些字段只能被管理员使用，防火墙用户不可用。

通信量控制

对连接所做的更改不生效

问题说明

任何对“通信量控制”组件的更改都直到它们激活才生效。 包括系统管理下的**安全性策略**对话框。

建议的操作

使用**连接激活**对话框，以重新生成并激活配置。

代理服务器

不发送数据

问题说明

防火墙的代理服务器直到安装好机器并重新启动之后才启动。

建议的操作

重启动机器。

问题说明

防火墙的“通信量控制”必须配置为允许包流入、流出代理过程，并非直接通过防火墙。

建议的操作

按照 *IBM eNetwork Firewall 用户指南*中的描述配置每个代理连接。

可能的话，特别用 FTP 通信量来使用预先定义的服务。

无法连接到期望的主机

问题说明

若数据正在流入、流出代理，但是无法与主机联系，则客户程序可能不能正确分辨主机名。

建议的操作

确保**安全性策略**对话框启用了*允许 DNS 查询*，且已激活了连接配置。请参阅 第59页的『DNS 问题』 获取更多的信息。

问题说明

每个在防火墙上由防火墙服务认证的用户名可配置为使用任何认证方法。使用 `Deny all` 来禁止用户使用特定的代理。

建议的操作

检查在配置客户程序上的**用户**对话框中的用户帐户认证设置。

认证服务

NT 管理员帐户不能被认证

问题说明

NT 管理员帐户的防火墙属性使用 `fwdfadm` 存储在防火墙用户数据库中。

建议的操作

验证 `fwdfadm` 有为您尝试使用的服务器设置的正确的认证方法。

防火墙代理用户不能被认证

问题说明

如果防火墙代理用户未在防火墙用户数据库中定义，使用 `fwdfuser` 名称来定义用户属性。

建议的操作

验证 `fwdfuser` 的认证方法为用户尝试访问的服务器正确定义。

网络地址转换

NAT 连接不工作

问题说明

设置并激活 NAT 但连接不工作。

建议的操作

路由表有问题或是 NAT 配置有问题。

如何为 NAT 包建立路由?

问题说明

没有为 NAT 包建立路由。

建议的操作

用目的 NAT 地址和防火墙的网关在防火墙的前的路由器上添加静态路由。

有什么调试工具可用于帮助使用 NAT?

问题说明

有什么调试工具可用于帮助使用 NAT?

建议的操作

NAT 记录，它允许您跟踪动态注册地址的管理。

日志设施

日志设施的更改在服务器上不生效

问题说明

删除或更改日志设施时，GUI 上可看到变化，但在服务器上不生效。

建议的操作

重启动系统。

报告实用程序

访问文件时出错:

问题说明

以上出错可以通过使用下列任何命令之后来查看:

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

建议的操作

提供 .ddl、.dat 或 .dml 文件的正确全限定文件名。

调入数据至数据库时发生错误。

问题说明

来自db2 -vf fwimport.dat>import.out 命令的 import.out 文件中有指示一个导入失败或只有部分成功的信息。

建议的操作

按相应的导入语句检查 .msg 文件来查看要注意的问题。将提供问题的的更多细节。寻找相应的 .tbl 文件中的有关记录来查看输入数据并确定是什么错误。例如，是不是数据库中的目标列太长? 数据类型对于目标列类型是否适当的? 如果输入数据看上去不太对，可能需要找出原始正确记录来确保 fwlogtbl 是否正确生成 .tbl 文件。

如果不能解决该问题，保存 import.out 文件、.msg 文件、关联的 .tbl 文件和原始日志文件，并与 IBM 服务机构联系。

附录A. 信息

本附录包含 IBM Firewall AIX 版、 IBM Firewall NT 版的信息，以及这两种防火墙的公共信息。它提供了关于 IBM Firewall 信息的下列信息:

- 信息如何格式化
- 信息的严重性级别
- 信息及其解释

如果看到信息及其解释，但需要更详细的信息，请参考第57页的『第7章 故障检测与测试』。

信息标记

ICA 最先的 3 个固定字节。

xxxx 范围为 0000 - 9999 的数。

a 严重性指示符。信息通过严重性级别分类。

- i - 信息
- w - 警告
- e - 错误
- s - 严重

0000 - 9999 中的数进一步分为下列类别:

- 0000 - 0999 入侵警报
- 1000 - 1999 过滤器
- 2000 - 2999 代理
- 3000 - 3999 Socks
- 4000 - 4999 寻呼机
- 5000 - 8999 可用的
- 9000 - 9999 一般/其他

信息

ICA0001 **报警 - 认证失败*计数值*次。**

解释: 已满足认证失败的阈值条件。

ICA0002 **报警 - 用户*用户名*认证失败*计数值*次。**

解释: 已满足检测特定日志信息的阈值条件。

ICA0003 **报警 - 对主机*主机 IP 地址*认证失败*计数值*次。**

解释: 已满足来自任何特定主机的认证失败的阈值条件。

ICA0004 **报警 - 用*计数值*个日志项标记*信息标识符*。**

解释: 已满足检测特定日志信息的阈值条件。

ICA0005 **日志监视器 - 内存不足。**

解释: 进程耗尽了内存。

ICA0006 **日志监视器 - 访问服务文件失败: *errno***

解释: 未能在 /etc/services 中找到的项。

ICA0007　　日志监视器 - 创建套接字失败: *errno*

解释: 不能打开套接字 - 见错误信息。

ICA0008　　日志监视器 - bind() 失败: *errno*

解释: 不能 bind 套接字 - 见错误信息。

ICA0009　　不能打开阈值定义文件: *errno*

解释: 访问阈值定义文件出现问题 - 见错误信息。

ICA0010　　日志监视器 - 致命的读取错误: *errno*

解释: 从套接字读取出现问题 - 见错误信息。

ICA0011　　不能得到阈值定义文件的状态: *errno*

解释: 访问阈值定义文件出现问题 - 见错误信息。

ICA0012　　日志监视器精灵程序关闭。

解释: 精灵程序正异常结束或接收到终止信号。上一个日志信息将提供细节。

ICA0013　　日志监视器捕捉到终止信号。

解释: 精灵程序接收终止信号并关闭。

ICA0014　　启动日志监视器精灵程序。

解释: 已启动精灵程序。

ICA0015　　不能为日志监视器创建精灵程序: *errno*

解释: 精灵程序创建失败 - 见错误信息。

ICA0016　　不能打开*进程标识符文件* - 可能已激活精灵程序。

解释: 精灵程序不能打开进程标识符文件。

ICA0017　　不能把进程标识符（*进程标识符*） 写入*文件*。

解释: 精灵程序不能把进程标识符写入文件。

ICA0018　　日志监视器 - 无数据可读。

解释: 接收的信息包不带有数据 - 废弃的。

ICA0019　　日志监视器 - 接收到的包没有足够的数据。废弃标记。

解释: 接收的信息包不带有足够的数据 - 废弃的。

ICA0020　　日志监视器 - 错误格式的 ICA 标记。

解释: 接收的信息包带有错误格式化的数据 - 废弃的。

ICA0021　　日志监视器 - 错误格式的认证数据。

解释: 接收的信息包带有错误格式化的数据 - 废弃的。

ICA0022　　阈值定义文件（*无效项*）中存在无效语法。

解释: 阈值文件中指出的项语法出错。

ICA0023　　不能打开 fwmail.conf 文件。

解释: 打开 fwmail.conf 文件失败或文件为空

ICA0024　　不能连接至 SMTP 服务器。

解释: SMTP 服务器忙或拒绝连接

ICA0025　　报警信息 email 失败。

解释: 不能将日志监视器报警信息 email 至指定地址。

ICA0051　　保存在日志文件中的 Days，*日志文件名称*，必须是不带正负号的短整数值。

解释: 保存在日志文件中的天数必须是有效整数。

ICA0052　　保存在档案中的天数，*日志文件名称*，必须是不带正负号的短整数值。

解释: 保存在档案中的天数必须是有效整数。

ICA0053　　logmgmt.cfg 中不允许日志文件*日志文件名称*的多个输入项。

解释: logmgmt.cfg 中不允许日志文件的多个输入项。

ICA0054 不能打开 *$ Variables :* 文件。

解释: 不能打开 logmgmt.cfg 文件。

ICA0055 logmgmt.cfg 文件中无有效的输入项。

解释: logmgmt.cfg 文件中无有效的输入项。

ICA0056 日志信息*"$ Variables :"*无效

解释: 日志信息无效

ICA1001 无法用进程标识符创建文件

解释: 过滤器日志精灵程序在写文件 fwlogd.pid 时遇到错误。

用户回答: 在目录 /etc/security 所在处检查文件系统。可能为超出空间的情况。

ICA1002 不能与 cfgfilt 程序进行通信

解释: 由于未创建 fwlogd.pid 文件，不可能进行 fwlogd 精灵程序和 cfgfilt 应用程序（过滤器控制需要的）间的通信。

用户回答: 在目录 /etc/security 所在处检查文件系统。可能为超出空间的情况。

ICA1003 继续初始化记录精灵程序

解释: fwlogd 精灵程序将继续启动进程。

ICA1004 过滤器日志精灵程序 *fwlogd* (级别*版本.发行版*)在*日期时间*初始化。

解释: 已启动 IP 信息包日志精灵程序。如果启用了信息包日志，精灵程序 fwlogd 将把需要的记录写入 local4 的 syslog 文件。

ICA1005 由于缓冲区的上溢，抑制了 *filter_rule_no* 包信息的记录

解释: fwlogd 精灵程序过滤器日志缓冲区已上溢。不能记录指定过滤器规则的信息包。

用户回答: 检查日志。防火墙可能受到了拒绝的服务的袭击或是记录了不需要的信息。例如，广播信息应该有一个日志控制设置为否（l=n）的拒绝规则来防止填充日志。

ICA1006 致命 fwlogd 错误 - *失败函数*: *错误信息*

解释: fwlogd 服务器在指定函数中失败，精灵程序终止。

用户回答: 改正指定的系统问题并重新启动 fwlogd。

ICA1007 无法创建子进程: *errno*

解释: 在过滤器日志精灵程序启动期间，遇到了指出的系统错误。

用户回答: 基于显示的错误，执行正确的操作。

ICA1008 从 setpgrp 例行程序返回时出错: *errno*

解释: 在过滤器日志精灵程序启动期间，遇到了指出的系统错误。

ICA1009 无法创建次子进程: *errno*

解释: 在过滤器日志精灵程序启动期间，遇到了指出的系统错误。

ICA1010 该精灵程序必须由超级用户权限运行

解释: 过滤器日志精灵程序必须在管理员权限下启动。

用户回答: 由管理员授权重新启动。

ICA1011 sysconfig 要求查询内核扩展 *load_path* 失败: *errno*

解释: 在过滤器日志精灵程序启动期间，遇到了指出的系统错误。

ICA1012 未装入的 AIX 内核扩展 *netinet* 不能继续执行

解释: netinet 设备驱动程序不包含过滤器支持。

用户回答: 安装 Firewall 代码。有可能，已安装了代码但还未执行*重引导*。

ICA1013 套接字创建呼叫失败: *errno*

解释: 在过滤器日志精灵程序启动期间，遇到了指出的系统错误。

ICA1014 AIX netinet 设备驱动程序不在所需要的级别

解释: netinet 设备驱动程序和 fwlogd 精灵程序不是同一级别。

用户回答: 解决冲突，在安装新的 Firewall 级别后可能需要重启动。

ICA1015 在 ioctl() 调用时出错（SIOCGFWLOG）: *errno*

解释: 在过滤器日志精灵程序启动期间，遇到了指出的系统错误。

ICA1016 不能得到当前延迟的日志队列

解释: 其它的信息与立即领先的日志信息相关联。

ICA1017 从 SIOCGFWLOG ioctl() 调用返回时出错

解释: 在过滤器日志精灵程序启动期间，遇到了指出的系统错误。

ICA1018 致命 fwlogd 错误 - *失败函数*: *系统错误信息*

解释: fwlogd 服务器在指定函数中失败，精灵程序终止。

用户回答: 改正指定的系统问题并重新启动 fwlogd。

ICA1019 退出时出现意想不到的错误，rc 为 *internal_fw_return_code*

解释: 在过滤器日志精灵程序启动期间，遇到了指出的系统错误。

ICA1020 致命 fwlogd 错误 - *失败函数*: 返回码 = 0x*函数返回码*

解释: fwlogd 服务器在指定函数中失败，精灵程序终止。

用户回答: 改正指定的系统问题并重新启动 fwlogd。

ICA1021 打开 */dev/ipsp_poif* 时出错: *errno*

解释: 还未安装指示的设备驱动程序。

用户回答: 如果已安装了 Firewall 代码，检查 /tmp/rc/net.out 文件以获取可能的错误信息。

ICA1022 过滤器支持验证失败

解释: 由于在该信息前记录了一项错误，所以不能验证过滤器支持。

ICA1023 ioctl() 调用（SIOCGFWLVL）时出错: *errno*

解释: 在过滤器日志精灵程序启动期间，遇到了指出的系统错误。

用户回答: 执行下列步骤之一:

- 对于 AIX 版: 验证已安装的 Firewall netinet 设备驱动程序和安装后已重启动的机器的正确级别。
- 对于 OS/390 版: 验证已安装和已用 **IPCONFIG FIREWALL** 配置语句启动的 TCP/IP 的正确级别。

ICA1024 写文件 */etc/security/fwlogd.pid* 时出错: *errno*

解释: 由于指出的系统错误号，fwlogd 无法写指定文件。

用户回答: 校正指出的问题并重新启动过滤器日志精灵程序。

ICA1032 在 *日期*的*时间*时更新过滤器规则。

解释: 已更新 IP 信息包过滤规则。

ICA1033 过滤器支持(级别*版本*.*发行版*)在*日期*的*时间*时进行初始化。

解释: 已初始化 Firewall 过滤器支持。

ICA1034 过滤器支持在*日期*的*时间*时释放

解释: IP 信息包过滤现在使用缺省过滤器规则而不使用定义在 /etc/security/fwfilters.cfg 中的规则。

ICA1035 包所记录的状态在*日期*的*时间*时设置为*启用/禁用*

解释: 信息包状态已改变。信息用时间戳记指示当前状态。

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*

解释: 指示经处理的 IP 信息包的运行记录和与其匹配的相应过滤器规则。要写该记录。匹配过滤器规则必须把日

志控制设置为是。如果与该规则匹配的 IP 信息包是一个片断，对于标题显示 ports/icmp type/code 信息而对于其它信息包显示为 0。

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*

解释: 更新过滤器规则后，激活的规则写入日志。该日志信息说明激活规则之一。

ICA1038 **使用会话套接字端口**: *port_no* **和主套接字端口**: *port_no*, **启动会话密钥机制**

解释: 使用在 /etc/services 中定义的指定 UDP 端口数启动加密隧道。

ICA1039 **策略（重新）定义为**:

解释: 政策高速缓存使用文件 /etc/security/fwpolicy (重)定义。下列行显示新的政策高速缓存。

ICA1040 **>策略语句**: *tunnel_origin tunnel_end tunnel_ID encrypt_flag/authenticate_flag*

解释: 行记录从 /etc/security/fwpolicy 文件读取。

ICA1041 **删除了隧道**: *tunnel_ID* **的上下文规格说明。**

解释: 对于列出的 ID，隧道上下文再也不可执行。

ICA1042 **定义下列隧道上下文规格说明为**:

解释: 已定义隧道上下文规范，如以下日志记录所列。

ICA1043 **>tunnel_ID**: *号码*、**src_addr**: *IP 地址*、**dst_addr**: *IP 地址*, **加密**: *算法*

解释: 信息列示激活隧道上下文的特定属性。

ICA1044 **主机计数器警告**: **超出 IP**（*IP 地址*）

解释: 过多安全主机尝试与 Firewall 机器连接。

系统反应: 传递连接

ICA1045 **TCP 超过上限**: **拒绝** *IP 地址*(*端口*)->*IP 地址*(*端口*)

解释: 有太多 TCP 会话通过防火墙机器

系统反应: 拒绝连接

ICA1046 **UDP 超过上限**: **拒绝** *IP 地址*(*端口*)->*IP 地址*(*端口*)

解释: 有太多 UDP 会话通过防火墙机器

系统反应: 拒绝连接

ICA1047 **宽限期警告**: **传递过多 TCP 会话,跳过***IP 地址*(*端口*)->*IP 地址*(*端口*)

解释: 有太多 TCP 会话通过防火墙机器

系统反应: 传递连接

ICA1048 **宽限期警告**: **传递过多 UDP 会话,跳过***IP 地址*(*端口*)->*IP 地址*(*端口*)

解释: 有太多 UDP 会话通过防火墙机器

ICA1049 **无效 ipsec 包**: **源**: *IP 地址* **目的**: *IP 地址* **协议**: *协议* **spi**: *安全性参数索引*

解释: ipsec 包不能由接收防火墙解包。

用户回答: 保证已正确输出且在每个防火墙上激活了隧道定义。

ICA1050 **删除了隧道**: *tunnel_ID* **的规范。**

解释: 对于列出的 ID，隧道规范再也不可执行。

ICA1051 **定义下列隧道规范为**:

解释: 已定义隧道规范，如以下日志记录所列。

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*

解释: 信息列示激活隧道的特定属性。

ICA1200　　由于以上错误终止日志精灵程序

解释: 由于这条信息以前记录错误，fwlogd 精灵程序终止。

系统反应: IP 过滤器日志不激活。

用户回答: 校正指出的错误并重新启动 fwlogd。

ICA1260　　由于收到*终止*信号，过滤器记录精灵程序在*日期*的*时间*终止

解释: fwlogd 精灵程序接收指示的终止信号并停止。

ICA1305　　“未知的”

解释: 为 syslog 格式化 IP 信息包时，找到一带有未知协议规格说明的记录。协议 IP, ICMP, TCP, UDP 和 IPSP 是可识别的协议。注意 IBM 对于通过隧道传递的加密信息包指定为 IPSP。

ICA1400　　致命 fwtimernat 错误 - *失败函数*: *系统错误信息*

解释: fwtimernat 服务器在指出的函数中失败。fwtimernat 服务器终止。

用户回答: 改正指出的系统问题然后重新启动 fwtimernat。

ICA1401　　致命 fwtimernat 错误 - *失败函数*: 返回码 = 0x*函数返回码*

解释: fwtimernat 服务器在指出的函数中失败。fwtimernat 服务器终止。

用户回答: 改正指出的系统问题然后重新启动 fwtimernat。

ICA1402　　致命 fwtimernat 错误 - *失败函数*: *错误信息*

解释: fwtimernat 服务器在指出的函数中失败。fwtimernat 服务器终止。

用户回答: 改正指出的系统问题然后重新启动 fwtimernat。

ICA2000　　建立了从 *IP 地址*（非安全位置）至 *IP 地址*的新的 FTP 会话。

解释: 从非安全站点启动新的 ftp 会话。

ICA2001　　对于来自*网络 ftp*: *IP 地址*的用户*名称*认证失败。

解释: 一个无帐户的用户试图从网络上使用 ftp 代理。

用户回答: 向防火墙管理员咨询以设置一个代理帐户。

ICA2002　　来自*网络*:*主机名*，使用*认证方式*的用户*名称*认证失败。

解释: 防火墙无法认证指示的使用指定认证方式的用户名。

用户回答: 请向 Firewall 管理员咨询。

ICA2003　　没有为*用户名*配置外壳。

解释: 标识的用户尝试登录代理且无注册外壳已经定义。

用户回答: 向 Firewall 管理员咨询以改正这个用户登录概要文件。

ICA2004　　接收到 0x *十六进制值*的未知审查事件。

解释: 由模块 tcpip_audit.c 接收到未知审查请求。

ICA2005　　写客户机时出错: *errno*。

解释: 无法与客户机通信；见记录的系统信息。

ICA2006　　ptelnetd: auditproc: *errno*。

解释: 指出的错误由 telnet 审查进程返回。系统文件的潜在崩溃。

ICA2007　　ptelnetd: 惊恐状态=*值*。

解释: 检测未知错误。系统文件的潜在崩溃。

ICA2008　　非防火墙用户名*名称*从: *IP 地址*进行远程登录。

解释: 一个无防火墙帐户的用户试图使用 telnet 代理。

系统反应: 假设使用了类属认证。

ICA2009　　/bin/login: *errno*.

解释: 系统登录期间的致命错误。见指出的系统错误信息。

ICA2010 从 *IP 地址*(非安全的)连接至 *IP 地址* 。

解释: 成功通过非安全接口连接指出的 IP 地址。

ICA2011 从 *IP 地址*(安全的)连接至 *IP 地址* 。

解释: 成功通过安全接口连接指示的 IP 地址。

ICA2012 从 *IP 地址*（安全位置）新建 FTP 会话至 *IP 地址*

解释: 启动新的 ftp 会话。

ICA2013 从 *IP 地址*新建 Telnet 会话 至 *IP 地址*。

解释: 建立了新的 telnet 会话。

ICA2014 不支持选项 -*值*。

解释: 不支持指出标志，见前面的信息。

ICA2015 不支持选项 -*值*。

解释: 不支持指出标志，见前面的信息。

ICA2016 远程用户标识符为 *"名称"*。

解释: ftp 连接请求指示的用户。

ICA2017 调试 - *in line*.

ICA2018 找不到用户*名称*的 SNK 密钥。

解释: 找不到指出的用户标识符的 SecureNetKey 值。

用户回答: 向 Firewall 管理员咨询以解决可能的登录配置问题。

ICA2019 未正确读取用户*名称*的 SNK 密钥。

解释: 指出的用户标识符的 SecureNetKey 值作为八进制数位不可读。

用户回答: 向 Firewall 管理员咨询以解决可能的登录配置问题。

ICA2020 /usr/bin/fwuserau 或 /usr/bin/fwuserpt 不存在。

解释: 使用用户提供的认证方式的认证异常终止。

系统反应: 认证异常终止。

用户回答: 确保 /usr/bin/fwuserau and /usr/bin/fwuserpt 存在且所有者为管理员。如果可执行的不存在，用户应该使用与防火墙的操作系统兼容的编译器建立一可执行的并命名为 /usr/bin/fwuserau or /usr/bin/fwuserpt。

ICA2021 尝试用用户标识符*名称*连接至远程主机*名称*。

解释: 尝试建立新的 ftp 连接。

ICA2022 尝试连接至远程主机*名称*。

解释: 尝试建立新的 ftp 连接。

ICA2023 用法: ptelnetd [-n] [-s]。

解释: 启动 ptelnet 精灵程序时指定未知标志。

用户回答: 仅使用标志 -n 和/或 -s。

ICA2024 用户*名称*使用来自*网络*: *主机名*的*方式*认证成功。

解释: FW 使用指定的认证方式认证指示的用户名。

ICA2025 用户*名称*使用来自*网络*: *主机名*的*方式*来登录。

解释: ftp 用户登录。

ICA2026 用户*名称*在*当前时间*的 *n* 秒后超时。

解释: 对于指定的用户连接尝试超时。潜在的网络路由选择问题或远程主机不可用。

ICA2027 *时间*时来自*远程主机*的连接。

解释: 网络 ftp 连接建立至 Firewall 。

ICA2028 拒绝从 *IP 地址*至 *IP 地址* 的 FTP 连接尝试。 该机器不支持来自非安全位置的 FTP。

解释: 通常指出跨越非安全接口而建立至 Firewall 的 ftp 连接的尝试。

系统反应: 拒绝连接。

ICA2029　　系统错误，在*in*第*line*行中 errno =-。

解释: 系统调用在执行一个系统调用时遇到问题。

系统反应: 系统执行停机。

用户回答: 获取该日志，弄清 errno 的意思尝试解决问题。如果不能解决，与 IBM 服务商联系。

ICA2030　　在*in* 第*line*行中函数调用返回码 = -。

解释: 函数调用遇到问题。

系统反应: 错误返回

用户回答: 记录一下，弄清返回码的意思尝试解决问题。如果不能解决，与 IBM 服务商联系。

ICA2031　　sdi 函数调用 creadcfg() rc = -。

解释: 函数调用遇到问题。

系统反应: 错误返回

用户回答: 咨询 sdi 参考以获取说明。

ICA2032　　丢失连接。

解释: 丢失 ftp 连接。

用户回答: 重建会话。

ICA2033　　sdi 函数调用 sd_init rc = -。

解释: 函数调用遇到问题。

系统反应: 错误返回

用户回答: 咨询 sdi 参考以获取说明。

ICA2034　　sdi 函数调用 sd_check rc = -。

解释: 函数调用遇到问题。

系统反应: 错误返回

用户回答: 咨询 sdi 参考以获取说明。

ICA2035　　setsockopt(): *errno*。

解释: setsocketopt 调用的系统错误。

ICA2036　　为用户*用户标识符*(*源 IP 地址*:*目的 IP 地址*)启动 Telnet 会话*会话标识符*。

解释: 信息在每个 Telnet 会话启动时生成。当防火墙对于用户标识符，源 ip 和目的 ip 都知道后，开始一个会话。会话 id 是由防火墙生成的唯一标识。

ICA2037　　不允许用户 fwdfuser 或 fwdpuser 登录。

解释: fwdfuser 和 fwdpuser 的保留用户不应该使用。

系统反应: 拒绝登录。

用户回答: 管理员应该审查是谁在使用该用户。

ICA2038　　ttloop: 同级进程已死: *errno*。

解释: 清空网络输出缓冲区时发生错误。出现同级进程已死亡。

ICA2039　　ttloop; 读取: *errno*。

解释: 清空网络输出缓冲区时发生错误。

ICA2040　　不允许把用户 ID fwdfuser 的认证设置为口令、无或 snk 认证。

解释: fwdfuser 是保留用户 ID 且不应该使用口令或 n none 作为认证方式。

系统反应: 拒绝登录。

用户回答: 管理员应该更改用户 ID fwdfuser 的认证方式。

ICA2041　　为*用户标识符*(*源 IP 地址*:*目的 IP 地址*)启动 FTP 会话*会话标识符*。

解释: 信息在每个 FTP 会话启动时生成。当防火墙对于用户标识符，源 ip 和目的 ip 都知道后，开始一个会话。会话 id 是由防火墙生成的唯一标识。

ICA2042　　req_rsp_code 错误设置为 FW_AUTH_REQ。

解释: fw_tn_authenticate 不允许设置 req_rsp_code 为 FW_AUTH_REQ。

系统反应: 认证异常终止。

用户回答: 更改 fw_tn_authenticate，再次执行库 fwuser.o，且把其放入 Firewall。

ICA2043　　不能得到*用户名*的口令。

解释: 该用户的认证类型是'口令'且找不到口令。

用户回答: 请向 Firewall 管理员咨询。

ICA2044　　为 -t 指定了不正确的时间（*值*）。

解释: 显示的时间值包含 0 至 9 数字范围以外的值或超过最大允许值。

ICA2045　　防火墙不支持选项 -T 。

解释: 不支持指出的选项。

ICA2046　　防火墙不支持选项 -K。

解释: 不支持指出的选项。

ICA2047　　防火墙不支持选项 -s。

解释: 不支持指出的选项。

ICA2048　　防火墙不支持选项 -u。

解释: 不支持指出的选项。

ICA2049　　忽略未知标志 -*值*。

解释: 指定了指出的标志且不可识别。

ICA2050　　未知 parm *值*。

解释: 指定为一个选项的指示值不可识别。

ICA2051　　adapt_addr 在地址转换中出错。

解释: 显示的 IP 地址无效。

用户回答: 文件 /etc/security/fwsecadpt.cfg 的可能毁损。删除该文件，重新配置您的安全的接口然后重新初始化过滤器。

ICA2052　　afopen 未能打开 /etc/security/login.cfg: *errno*。

解释: 无法认证用户；指出文件上打开错误。

ICA2053　　不能打开安全接口文件。

解释: 还未配置安全接口。

用户回答: 如果要定义安全接口，使用 Firewall 命令/smit 面板来定义安全接口。

ICA2054　　enduserdb rc=*值*，*errno*。

解释: 接收到的指出系统错误代码正尝试检索用户登录概要文件信息。

用户回答: 向 Firewall 管理员咨询以验证登录帐户。

ICA2055　　getpeername()(*调用名称*): *errno*。

解释: ftp 精灵程序试图得到套接字名时系统出错。

ICA2056　　getsockname() (*调用名称*): *errno*。

解释: ftp 精灵程序试图得到端口名时系统出错。

ICA2057　　对于*用户标识符*的 getuser 非安全外壳 rc=*值*，*errno*。

解释: 接收到的指出系统错误代码正尝试检索来自 Firewall 非安全方连接的外壳名称。

用户回答: 向 Firewall 管理员咨询以为用户登录概要文件建立一外壳。

ICA2058　　对于*用户标识符*的 getuser 安全外壳 rc=*值*，*errno*。

解释: 接收到的指出系统错误代码正尝试检索来自 Firewall 安全方连接的外壳名称。

用户回答: 向 Firewall 管理员咨询以查询用户登录概要文件的外壳。

ICA2059　　ioctl(): *errno*。

解释: 对于 SIOCSPGRP 的 ioctl() 调用系统错误。

ICA2060　　ptelnetd: **ftok 共享内存失败。**

解释: 无法分配共享内存段。

用户回答: 与 Firewall 管理员联系，解决内存问题。

ICA2061 ptelnetd: shmat 共享内存失败。

解释: 无法分配共享内存段。

用户回答: 与 Firewall 管理员联系，解决内存问题。

ICA2062 ptelnetd: shmget 共享内存失败。

解释: 无法分配共享内存段。

用户回答: 与 Firewall 管理员联系，解决内存问题。

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

解释: 指出错误信息从系统调用 'setsockopt'返回。

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

解释: 指出错误信息从系统调用 'setsockopt'返回。

ICA2065 setuser rc=*value*, *errno*。

解释: 由于指出的原因在系统调用中接收到错误的返回码。

ICA2066 signal(): *errno*。

解释: ftp 精灵程序试图建立信号处理程序时系统出错。

ICA2067 致命的 pftpd 初始化错误 - bind(): *errno*

解释: pftpd 服务器初始化失败，精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 pftpd。该错误最可能的原因是另一个 ftp 精灵程序已在标准 ftp 端口（21）侦听。

ICA2068 致命的 pftpd 初始化错误 - listen(): *errno*

解释: pftpd 服务器初始化失败，精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 pftpd。

ICA2069 致命的 pftpd 错误 - main accept(): *errno*

解释: pftpd 服务器主例程失败，精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 pftpd。

ICA2070 致命的 pftpd 初始化错误 - socket(): *errno*

解释: pftpd 服务器初始化失败，精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 pftpd。

ICA2071 拒绝连接，连接达到最大数。

解释: pftpd 服务器不能创建另一个 FTP 会话，因为已存在会话的最大数。

系统反应: 拒绝连接。

用户回答: 等待现有的连接终止，然后再次尝试请求。

ICA2072 ftp 配置文件（*文件名*）不可用。

解释: ftp 精灵程序尝试打开指定的 ftp 配置文件但它不存在或可能不能打开。

系统反应: ftp 精灵程序进程处理使用缺省配置

用户回答: 无，除非文件存在，在这种情况下应该创建它或移至信息中指定的位置。

ICA2073 ftp 语言表无法获得存储器。

解释: 无法获得需要用来表示 FTP 配置文件中 REPLYLANGUAGE 语句的存储器。

系统反应: 处理继续。

用户回答: 增加区域大小或减少配置文件中的项。

ICA2074 ftp 配置语句: *配置语句* 的处理完成

解释: ftp 已处理了指出的配置语句。

系统反应: 处理继续。

用户回答: 无

ICA2075 *用户标识符*(*源 IP 地址*:*目的 IP 地址*)的 FTP, *操作文件名*, *numbytes*个字节。字节。 sid: *会话标识符*。

解释: 为打开的 FTP 会话上传送的每个文件生成信息。sid 是由防火墙在会话启动时生成的唯一标识。

ICA2076 为*用户标识符*(*源 IP 地址*:*目的 IP 地址*)结束 FTP 会话*会话标识符*, *持续时间* 秒, *numbytes* 个字节。

解释: 信息在每个 FTP 精灵程序会话结束时生成。sid 是由防火墙在会话启动时生成的唯一标识。

ICA2077 为*用户标识符*(*源 IP 地址*:*目的 IP 地址*)结束 FTP 会话*会话标识符*, *numbytes*个字节。

解释: 信息在每个 Telnet 会话结束时生成。sid 是由防火墙在会话启动时生成的唯一标识。

ICA2078 断开的代理用户*用户* - 空闲时间为*时间*分钟。

解释: 用户会话已超过最大允许空闲时间。

ICA2079 注意 - 从*IP 地址*至 *IP 地址* 的连接是未授权的。

解释: 通常指一个跨越非安全接口而建立至 Firewall 连接的尝试。

系统反应: 拒绝连接。

ICA2080 在 ftp 配置文件如第*行*行:*配置语句*第*列*列附近出现语法错误 (*原因*)。

解释: 给定行的 ftp 配置语句出错。提供了错误的原因和检测到错误的位置。

系统反应: 忽略语句。

用户回答: 改正 ftp 配置文件中的语句。

ICA2081 ftp 配置语句提供的信息目录是无用的。

解释: 打开由 REPLYLANGUAGE ftp 配置语句提供的信息目录的尝试失败。无客户机信息目录可用。

系统反应: 客户机信息目录强制为 C 目录下的英语。

用户回答: 保证在每个与 ftp 配置 REPLYLANGUAGE 语句中的语言目录关联的目录中有目录文件。也要检查 NLSPATH 环境变量正确设置为既允许来自 LANG 环境变量（%L）的子目录替代也允许目录名称（%N）替代。

ICA2082 无法设置 ftp LANG 环境变量为*子目录*, 原因: *原因*

解释: 当 FTP 精灵程序尝试改变 LANG 环境变量的设置为指定的子目录时，发生一系统错误（由原因提供）。

系统反应: 处理继续。恢复可能生成其它信息。

用户回答: 使用提供的原因来确定这是系统错误还是程序设计错误。

ICA2083 无法打开目录 *子目录*的 ftp 客户信息目录，原因: *原因*。

解释: ftp 精灵程序不能打开给定子目录中的信息目录。给出的原因是从 catopen() 返回的错误号。

系统反应: 处理继续。恢复可能生成其它信息。

用户回答: 保证在与提供的语言目录关联的目录中有目录。检查 NLSPATH 环境变量正确设置为既允许子目录（%L）替代也允许目录名称（%N）替代。

ICA2084 把 ftp 客户信息目录强制为使用 C 子目录的英语。

解释: 由于前面列出的错误，ftp 精灵程序强制客户信息目录为使用 C 子目录的英语。

系统反应: 如果能强制语言为 C 信息目录，则进程继续。如果不能则程序退出。

用户回答: 更正来自以前信息的错误。如果程序也存在，在 C 子目录中创建信息目录并正确设置 NLSPATH 环境变量。

ICA2085 pid *进程标识符*(*源 IP 地址*)的 Telnet 会话结束。

解释: 信息在每个 Telnet 会话结束时生成。

ICA2086 错误配置的用户文件: 用户*用户*无密钥 (*密钥*)。

解释: ftpd 在用户文件中找到请求的用户，但找不到密钥 - 错误配置的用户文件。

用户回答: 使用 Firewall 命令/smit 面板来更正该问题。

ICA2087 **ftpd 在用户配置文件中找不到指定的用户** *用户*。

解释: 指定的用户名还未配置或 user.cfg 文件已损坏。

用户回答: 使用 Firewall 命令/smit 面板来更正该问题。

ICA2088 **ftpd 不能打开用户配置文件。**

解释: ftpd 调用 fopen 失败因为它不能打开用户配置文件。

用户回答: 确保用户配置文件（缺省值为 user.cfg）可用; 使用 Firewall 命令/smit 面板

ICA2089 **用户文件的权限类型（***权限类型***）与表中的任何项不匹配（结构 tab2 authtab[]）。**

解释: 指定用户的权限类型（由 user.cfg 返回）与任何支持类型不匹配（如 deny, none, snk, sdi, password 等）

用户回答: 检查 user.cfg 文件的完整性或配置; 使用 Firewall 命令/smit 面板来更正该问题。

ICA2090 **对于***客户 ip***的用户'***用户名***'认证失败，因为 user.cfg 文件中 KEY=DENY。**

解释: 认证失败是由于 user.cfg 文件规范由 Firewall 管理员设置。

用户回答: 请向 Firewall 管理员咨询。

ICA2091 **不允许用户'***用户名***' ftp 至非安全端口（***防火墙 ip***）。**

解释: 用户通过非安全端口（nsp） ftp 进入防火墙服务器 - 所有 nsp 用户必须将其 'fwnsftp' 密钥正确配置成一个有效的认证类型（在文件 user.cfg 中）。

用户回答: 检查 user.cfg 文件的完整性或配置; 使用 Firewall 命令/smit 面板来更正该问题。

ICA2092 **内部错误: nt_gwauth() 失败。**

解释: nt_gwauth() 正常返回三值之一（AUTHENTICATED,NOT_AUTHENTICATED 或 DENY），在这种情况下，nt_gwauth 返回一些无效的整数。

ICA2093 **不允许用户'***用户名***' ftp 至安全端口（***端口号***）。**

解释: 用户通过安全端口（sp） ftp 进入防火墙服务器 - 所有 sp 用户必须将其 'fwnsftp' 密钥正确配置为有效的认证类型（在 user.cfg 文件中）。

用户回答: 检查 user.cfg 文件的完整性或配置; 使用 Firewall 命令/smit 面板来更正该问题。

ICA2094 **登录失败: 在: "USER <***用户名***>"之后，格式应为: "PASS <口令>"; 接收到***无效 cmd***。**

解释: 认证失败是因为 ftp 客户未发送所需的格式（符合 RFC959 的 PASS '口令'）

用户回答: 输入用户<用户名>"; 输入正确的口令。请向 Firewall 管理员咨询。

ICA2095 **登录失败: （通过方式***auth 方式***）失败认证***客户 ip***（客户位置）的用户'***用户名***。**

解释: 认证失败是由于无效的输入（由客户对于指定的认证类型） - 如用户输入无效口令，snk 密钥等。

用户回答: 请向 Firewall 管理员咨询。

ICA2096 **认证: （通过方式***auth 方式***）成功认证***客户 ip***（客户位置）的用户'***用户名***。**

解释: 认证成功。

ICA2097 **httpd --> 启动 HTTP 代理服务器版本** *HTTP 代理版本*。

解释: 启动用于 WWW 访问 的 HTTP 代理。

ICA2098 **httpd --> 关闭 HTTP 代理服务器。**

解释: 关闭用于 WWW 访问 的 HTTP 代理。

ICA2099 **httpd --> 状态: 客户<***IP 地址***>的<***HTTP 状态码***>, 请求<"***HTTP GET 请求***"><***字节数***>字节。**

解释: 通过代理的客户 HTTP 请求一些文件的状态。要获取有关 "状态" 代码值的详细信息，参阅 internet 各站点（包括 ds.internic.net）提供的 HTTP 1.0（RFC 1945） 或 HTTP 1.1（RFC 2068）文档（或接替的 RFC）。

ICA2100　　套接字地址等于 0。

解释: 在本地请求中发现无效目的地址。

ICA2101　　插座地址系列错误: *sin_family_type*。

解释: 在本地请求中发现无效地址系列类型。

ICA2102　　初始化 odm 时出错: *odmerrno*。

解释: ODM（对象数据管理器）发生 odm_initialize() 错误。

ICA2103　　设置 odm 缺省路径时出错: *odmerrno*。

解释: ODM（对象数据管理器）发生 odm_set_path() 错误。对象类，OCSvhost。

ICA2104　　对 odm 数据库加锁时: *odmerrno*。

解释: ODM（对象数据管理器）发生 odm_lock() 错误。

ICA2105　　打开 odm 对象*Customized_Attribute* **时出错**: *odmerrno*。

解释: ODM（对象数据管理器）发生 odm_open_class() 错误。

ICA2106　　搜索 odm 对象 *OCS_virtual_host* **时出错**: *odmerrno*。

解释: ODM（对象数据管理器）发生 odm_get_first() 错误。对象类，OCSvhost。

ICA2107　　关闭 odm 对象*OCS_virtual_host***时出错**: *odmerrno*。

解释: ODM（对象数据管理器）发生 odm_close_class() 错误。对象类，OCSvhost。

ICA2108　　对 odm 数据库解锁时出错: *odmerrno*。

解释: ODM（对象数据管理器）发生 odm_unlock() 错误。

ICA2109　　终止 odm: *odmerrno***时出错。**

解释: ODM（对象数据管理器）发生 odm_terminate() 错误。

ICA2110　　通过名称获得服务器时出错: *errno*。

解释: 发生 getservbyname() 错误。主机登录监视器服务器 lm 未在 /etc/services 文件中正确指定。

ICA2111　　byname() 错误: *errno*。

解释: 发生 gethostbyname() 错误。主机名称未在 /etc/hosts 中正确指定。

ICA2112　　无效协议名称: *protocol_name*。

解释: 不支持 ODM 对象类中指定的协议名称 OCSvhost。

ICA2113　　打开至 LM 的套接字时出错: *errno*。

解释: socket() 错误发生在登录监视器所在的主机中。

ICA2114　　联接本地地址时出错: *errno*。

解释: 为该 OCS 节点使用本地地址的 bind() 错误。

ICA2115　　连接至 LM 的套接字时出错: *errno*。

解释: connect() 错误发生在登录监视器驻留的主机中。

ICA2116　　协议类型错误: *protocol_type*。

解释: 用来与主机登录监视器通信的虚拟终端协议无效。

ICA2117　　LM 信息 Malloc 时出错。

解释: 为可变长度登录监视器信息动态分配空间时发生 malloc() 错误。

ICA2118　　发送 msg 至 LM 时出错: *errno*。

解释: 当发送登录监视器请求以打开正确的主机设备时发生 send() 错误。

ICA2119　　接收来自 LM 的 msg 时出错: *errno*。

解释: 登录监视器返回确认的发生 recv() 错误。

ICA2120　　来自 LM 的状态出错: *状态*。

解释: 来自登录监视器的确认指示主机设备未成功打开。

ICA2121 打开 OCS 管理设备时出错: *errno*。

解释: OCS 管理设备未成功打开。

ICA2122 未能转换 IP 地址至 TBM ID: *errno*。

解释: 发生 ioctl() OCS_GET_TBMID 错误。ioctl 命令 OCS_GET_TBMID 在 OCS 管理设备上失败。

ICA2123 连接由 rlogin 确定的 TBM 时出错: *errno*。

解释: 发生 ioctl() OCS_IS_TBM_CONNECTED 错误。ioctl 命令 OCS_IS_TBM_CONNECTED 在 OCS 管理设备上失败。

ICA2124 未连接任何主机节点: *errno*。

解释: 从可能的主机节点的列表中，无主机节点连接至该 OCS 节点。

ICA2125 获取 ODM(对象数据管理器): *Customized_Attribute*列表时出错:*odmerrno*。

解释: ODM 对象类发生 odm_get_list() 错误，CuAt（定制的属性）。

ICA2126 无 OCS 主机节点名称与: *hostnode_to_connect*关联。

解释: 找到 CuAt（定制的属性）项，但没有 hostnode/ocsnode 匹配。

ICA2127 在主机数组上 Malloc 错误。

解释: 为可能的主机名数组动态分配空间时发生 malloc() 错误。

ICA2128 *客户 ip*（客户位置）的用户（未知）在认证之前尝试命令 '*无效命令*'。

解释: 用户在输入认证的用户名和口令之前为了尝试操作 - 在任何进一步处理可能继续之前用户首先必须认证。

用户回答: 请用 USER 和 PASS 登录。

ICA2129 gethostbyname (*调用名称*): *errno*

解释: ftpd 尝试获得与主机名相应的主机信息时发生系统错误。

ICA2130 *客户 ip* (客户位置)的用户(*用户名*)在认证之前尝试命令 '*无效命令*'。

解释: 指定的用户尝试无效命令。

用户回答: 仅允许命令 USER，QUOTE SITE 和 QUIT，除非指定 "引用位置目的地 "。

ICA2131 对于*客户 ip*的用户'*用户名*'认证失败，因为 user.cfg 文件中存在错误。

解释: 认证失败是由于由 Firewall 管理员设置的 user.cfg 文件轨范（检查上一个日志）。

用户回答: 请向 Firewall 管理员咨询。

ICA2132 *客户 ip* (客户位置)的用户'(*用户名*)'尝试无效命令 '*无效命令*'。

解释: 用户尝试无效命令。该点唯一有效的命令是 SITE，USER 和 QUIT。

ICA2133 出错: *实例*: 第*行*，*函数*调用失败，*WSAGetLastError*

解释: 常规的错误信息；检查日志

ICA2134 注意: ftpd: connect() （*实例* 中）不能到达 *IP*，*WSAGetLastError*。

解释: Connect() 找不到请求的地址，检查 WSAGetLastError 结果。

用户回答: 双重检查地址 - 可能是 DNS 或网络错误

ICA2135 完成数据传送: 接收到*字节*个字节 (从*源 IP*)；发送了*字节*个字节(至*目的 IP*)。

解释: 该信息反映特殊 ftp 会话期间的单个数据传送。然而，请注意数据传送可能未成功完成（检查日志以寻求失败的 recv 或 send 调用）。

ICA2136 错误: 在*实例*中 **CreateThread()** 失败: *errno*。

解释: ftpd 不能创建线程

ICA2137 建立数据连接; 服务器为: *源 ip* 客户机为: *目的 ip*。

解释: 数据连接成功。

ICA2138 内存不足: **pftpd**: 函数（*实例*）中 **malloc** *字节*返回 **NULL**。

解释: 无法分配足够内存 - malloc 返回 NULL。

ICA2139 **LogonUser()** 失败: *原因*。

解释: Windows NT （SAM） API LogonUser（用于口令认证） 失败，是由于指定的原因。

用户回答: 与 Firewall 管理员联系。

ICA2140 **httpd --> HTTP** 代理认证*结果*用户 **<***用户***>, on <***用户 ip***>,** 通过*网络* **... RC:<***原因***>**。

解释: HTTP 代理尝试用户认证。成功或失败都在这里报告指定的原因。

用户回答: 与 Firewall 管理员联系。

ICA2141 终止从 *IP 地址*至 *IP 地址*的 **FTP** 会话。

解释: 终止至防火墙的 ftp 会话。

ICA2142 **fw_tn_authenticate** 成功认证*用户标识符*。

ICA2143 **fw_tn_authenticate** 对*用户标识符*的认证失败。

解释: fw_tn_authenticate 不能认证指定的用户 ID。

系统反应: 拒绝登录。

用户回答: 如果 fw_tn_authenticate 有任何记录设施，则管理员应该查看日志文件来确定原因。

ICA2144 **fw_tn_authenticate** 未返回成功。

解释: fw_tn_authenticate 返回的值不是 0。函数 fw_tn_authenticate 可能丢失了。

系统反应: 拒绝登录。

用户回答: 仔细查看 fw_tn_authenticate 是否返回一个非零值，如果是这样就更正它。如果发生这种情况，再次执行库 fwuser.o，且把其放入 Firewall。

ICA2145 在文件*文件名*的行*行号*，系统返回的返回码 *rc*。

解释: 系统调用失败。库 fwuser.o 可能异常终止。

系统反应: 认证异常终止。

用户回答: 确保出现 /usr/lib/fwuser.o。如果是这样，与 IBM 代表联系。

ICA2146 **IBM** 提供的 **fwuser.o** 还未替换。

解释: 您正在使用 IBM 提供的 fwuser.o，因为不能用您自己的 fwuser.o 来替换。

系统反应: 认证异常终止。

用户回答: 如果已定义了可使用用户提供的认证的任何用户，应该编写并编译自己的认证。IBM 提供的 fwuser.o 拒绝对所有非 AIX 和非 Firewall 用户的访问。

ICA2147 **fwtelnet**: 用户*用户标识符*从*源 IP addr*（安全端）至*目的 IP addr*启动透明 **telnet** 会话。

解释: 目的地在每个透明代理会话的（fwtelnet）生成信息。当防火墙对于用户标识符，源 ip 和目的 ip 都知道后，开始一个会话。只允许从安全方启动的会话。

系统反应: 允许透明 telnet。

ICA2148 注意 - 不允许用户*用户标识符*从*源 IP addr*（非安全端）至*目的 IP addr*进行未授权连接会话。

解释: 通常指一个跨越非安全接口而建立至 Firewall 连接的尝试。

系统反应: 拒绝连接。

用户回答: 应该使用透明代理从安全方远程登录。

ICA2149 **fwtelnet**: 从*源 IP addr*至*目的 IP addr*启动透明 **telnet** 会话时发生 **LOGIN_ADAPTER_ERROR** 错误。

解释: 调用 q_check_secure(0) 时发生 LOGIN_ADAPTER_ERROR。

系统反应: 拒绝连接。

用户回答: 检查安全适配器。

ICA2150 **Pftpd 出错 -** *失败函数*: **返回码 = 0x***函数返回码*

解释: pftpd 服务器在指出函数中检测出一个错误。 精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 pftpd。

ICA2151 **拒绝登录。**

解释: 对尝试登录但不允许的用户显示这条信息。

ICA2152 **fwlogin**: 写入*设备*失败。

解释: 不能写入设备。

ICA2153 **fwlogin**: 读取*设备*失败。

解释: 不能读取设备。

ICA2154 由于*原因*, 在*端口名*中出错。

解释: 这个 Firewall 遇到一个问题。

ICA2155 **Pftpd 出错 -** *失败函数*: *系统错误信息*

解释: pftpd 服务器在指出函数中检测出一个错误。精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 pftpd。

ICA2156 **注意 -- 不允许用户***用户标识符*尝试从 **NONSECURE** 的端*源 IP*至*目的 IP addr* 使用透明 **ftp**。

解释: 通常指一个跨越非安全接口而建立至 Firewall 连接的尝试。

系统反应: 拒绝连接。

用户回答: 应该使用透明代理从安全方 ftp。

ICA2157 不允许用户*用户标识符*从 *IP addr*至*目的 IP addr*使用透明代理。

解释: 通常指在未配置透明代理时建立至 Firewall 连接的尝试。

系统反应: 拒绝连接。

用户回答: 设置 fwtpproxy ftp = on

ICA2158 选项 *值* 未正确指定。

解释: 没有正确指定指出的标志。

ICA2159 没有指定 **-t** 选项的超时值。

解释: 必须对 -t 选项提供超时值。

ICA2160 来自*网络*: *主机名*的用户*用户 ID*的口令已更改。

解释: FTP 用户已成功在口令数据库中更改其口令。

系统反应: 无

用户回答: 无

ICA2161 用户*用户 ID*尝试从*网络*: *主机名*使用期满口令来登录。

解释: FTP 用户尝试使用期满口令来建立至 Firewall 的连接。

系统反应: FTP 登录验证失败且用户返回至 FTP 命令外壳。

用户回答: 用户必须尝试通过 FTP USER 命令或通过重新建立 FTP 连接并以 “old_password/new_password/new_password” 的形式传递口令字符串再次验证。

ICA2162 *网络*的用户*用户 ID*:*主机名*未能更改口令。

解释: 一个 FTP 用户试图更改其口令但未能执行口令验证例行程序。失败的可能原因包括: - 指定了不正确的 ″旧″ 口令, - 仅指定了一个 ″新″ 口令, - 两个 ″新″ 口令不匹配或 - 用来分隔口令的定界符不是 ″/″。

系统反应: FTP 登录验证失败且用户返回至 FTP 命令外壳。

用户回答: 尝试用 FTP 服务器验证正确地输入了口令来重新验证。如果问题仍存在, 请联系服务代表。

ICA2163 safemaild 已启动。

解释: 启动 safemaild。

ICA2164 safemaild 已停止。

解释: 停止 safemaild。

ICA2165 中断 telnet 会话。

解释: Telnet 会话结束，但它不能从管道检索会话信息。会话可能在启动期间由客户机中断，这样会话就未完全初始化。

ICA2166 不能检索用户*用户标识符*的属性*属性*。返回码 = *返回码*。

解释: 认证服务不能为指定的用户检索来自用户数据库的指定属性。系统操作: 用户认证失败。

用户回答: 与系统管理员联系以更正用户数据库记录。

ICA2167 使用来自*网络类型*的*客户地址*的*认证方案*来为*服务器*的*用户标识符*认证失败

解释: 指定用户未能使用指定认证方式为指定的服务认证。用户请求来自指示的地址和网络类型的服务器。系统操作: 用户认证失败。

用户回答: 请与系统管理员联系。

ICA2168 由于存储器不足，为*服务器*的*用户标识符*认证失败。

解释: 对于服务不能认证用户 ID，因为在认证处理期间分配内存失败。系统操作: 用户认证失败。

用户回答: 请与系统管理员联系。

ICA2169 使用来自*网络*: *主机名*的*方式*，为*服务器*成功认证用户*名称*。

解释: FW 使用指定的认证方案为请求的服务器认证指出的用户名。

ICA2170 为*服务器*的*用户标识符*认证失败。*认证方式*未在 Firewall 注册。

解释: 对于服务不能认证用户 ID。请求的认证方式未在 Firewall 注册。系统操作: 用户认证失败。

用户回答: 请与系统管理员联系。

ICA2171 由于口令到期，帐户*用户名*已加锁。

解释: 口令到期且还未更改。该帐户已锁定。

系统反应: 帐户被锁定且 Firewall 口令认证失败。UserRes

ICA2172 帐户*用户名*已加锁。

解释: 该帐户已锁定。

系统反应: 帐户被锁定。Firewall 口令认证将失败。

用户回答: 向 Firewall 管理员咨询以解锁帐户。

ICA2173 用户尝试使用保留的用户名*用户标识符*登录。

解释: 防火墙为使用保留由用户提供的 ID。

系统反应: 拒绝登录。

用户回答: 管理员应该审查是谁在使用该用户名。

ICA2174 由于内部的处理错误，使用来自*网络类型*的*客户地址*的*认证方案*来为*服务器*的*用户标识符*认证失败。

解释: 指定用户未能使用指定认证方式为指定的服务认证。用户请求来自指示的地址和网络类型的服务器。因为内部处理错误，认证请求失败。系统操作: 用户认证失败。

用户回答: 请与系统管理员联系。

ICA2175 用户*用户名*的 Windows NT LogonUser 调用失败。上一次错误为*上一次错误*。

解释: Windows NT LogonUser API 调用未能认证指定的用户名。Windows NT 在 LogonUser 失败后报告上一个错误。系统操作: 用户认证失败。

用户回答: 请与系统管理员联系。

ICA2176 使用来自*网络*的*组件*为*用户名*定义了未知认证方案*认证方案*。

解释: 使用来自指定网络的指定防火墙组件时，为指定用户定义指定认证方案，但是认证方案当前未在防火墙上注册。系统操作: 用户认证请求失败。

用户回答: 请与系统管理员联系。

ICA2177 从*套接字同级名称*接收到的 SafeMail 连接 0x *会话*。

解释: SafeMail 从列出的同级名称接收到入站连接。指出的连接 ID 数已为跟踪的目的而赋值指定。 (调试级别)

系统反应: 分派一个线程处理这个连接。

ICA2178 SafeMail 会话 0x *会话 ID* 已从*发送人的 IP 地址*建立至*收件人的 IP 地址*。

解释: SafeMail 已与收件人邮件服务器建立联系并准备传送邮件。 (信息级别)

系统反应: 数据传送准备开始。

ICA2179 SafeMail 已从*发送服务器的地址*至*接收服务器的地址*为连接 0x *会话 ID* 发送*信息大小*字节。

解释: SafeMail 已成功在两个列出的邮件服务器间发送一条信息。该会话以前在 ICA2166 信息中标识。这条信息包含指示的字节数。 (信息级别)

ICA2180 SafeMail 终止来自*发送人的地址*的会话 0x*会话 ID*。

解释: SafeMail 拒绝传送在指出的会话中发送的邮件。 (信息级别)

系统反应: 会话已终止。

用户回答: 增加日志优先级级别以包含更详细的诊断信息。

ICA2181 SafeMail 由于原因码*原因码*终止会话 0x *会话 ID*。

解释: SafeMail 的主处理器终止指示的会话，因为检测出了主要的错误条件。原因码包括: \01 - 无法定位收件人邮件服务器 \02 - 发送人试图在两个非安全服务器间路由邮件 \03 - 收件人邮件服务器拒绝连接，可能是因为已关机 \04 - 收件人邮件服务器拒绝接受邮件 \05 - 一个或多个连接超时; 发送或接收邮件服务器可能关闭 \06 - recv() 返回 0 字节; 发送或接收邮件服务器可能关闭 \07 - recv() 返回负值; \08 - 接受到太多错误 \09 - select() 返回负值; 发送或接收邮件服务可能关闭。这条消息注册在调试级别上。

系统反应: 连接已终止。

ICA2182 SafeMail 由于无效 *SMTP 命令*命令而拒绝会话 0x *会话 ID*, 原因码*原因码*。

解释: SafeMail 的命令验证子例程检测到无效或危险的命令。这些原因码随每个 SMTP 命令不同而不同。参阅 IBM Firewall 支持 web 页面以获取当前值。 (调试级别)

系统反应: 连接已终止。

用户回答: 更正发送邮件客户机或发送邮件服务器，以发送安全有效的信息。

ICA2183 httpd --> HTTP 代理配置文件（*文件名*）不可用。

解释: HTTP 代理精灵程序尝试打开指定的配置文件但它不存在或不能打开。

系统反应: HTTP 代理不启动

用户回答: 通过 GUI 或 fwhttp 命令配置代理然后重新启动代理.

ICA2184 signal() 出错,带有信号*信号 No.*。 safemaild 退出。

解释: safemaild 精灵程序试图建立信号处理程序时系统出错。

ICA2185 不能打开套接字。 safemaild 退出

解释: 打开套接字时失败。

ICA2186 不能把套接字联接至端口。 safemaild 退出

解释: 当联接套接字至端口时失败。

ICA2187 不能接受新的连接。safemaild 再次尝试

解释: 不能接收新的连接。

ICA2188 为 -I 指定了不正确的时间（*值*）。

解释: 显示的时间值包含 0 至 9 数字范围以外的值或超过最大允许值。

ICA2189 **没有指定 -l 选项的超时值。**

解释: 必须为 -l 选项提供超时值。

ICA2200 （*服务器*: *功能*） **WinSocket 初始化出错**: *WSAGetLastError*

解释: 当初始化 WinSocket 时发生错误。

用户回答: 更正由 WSAGetLastError 指出的系统问题并重新启动指出的服务器（第一个参数）。

ICA2201 **(***服务器*: *调用函数***)** *失败函数***在行***行号***失败**: *WSAGetLastError*

解释: 指定的连网组件已失败。

用户回答: 更正由 WSAGetLastError 指出的系统问题并重新启动指出的服务器（第一个参数）。

ICA2202 **(***服务器*: *调用函数***) 在***WSAGetLastError***秒后***超时***超时**:

解释: 指出的功能在指出的时间空闲后超时。

用户回答: 重连接至指出的服务器并在指出的超时之前响应

ICA2203 **(***服务器*: *调用函数***) 内存出错**; *失败函数* **在行***行号***返回***返回值*: *WSAGetLastError*

解释: 发生内存错误，通常是内存不足；检查 WSAGetLastError

用户回答: 释放磁盘空间 - 向系统管理员咨询

ICA2204 **(***服务器*: *调用函数***)** *文件名***出错: 拒绝存取或创建失败。**

解释: 当试图存取或创建指定的或与文件参数关联的文件时，指示的服务器遇到错误。

用户回答: 确保指示的文件名存在并有正确的许可权。

ICA2205 （*服务器*: *调用函数*）**需要文件***文件名***但找不到。**

解释: 指定的文件不存在。失败最可能的原因是删除了 Firewall 的缺省配置。从当前备份中恢复文件。

用户回答: 验证配置文件不存在。配置程序期望该文件存在。如果备份版本不可用，请与维修人员联系。

ICA2206 **(***服务器*: *调用函数***) 破坏了配置文件***文件名***。**

解释: 指出的配置文件为不可用格式。内容被破坏了。破坏最可能的原因是手工编辑了文件并添加了无效数据。

用户回答: 配置文件需要重新正确创建。首先 cat 文件（或建立可查看副本）然后擦除原始文件。通过适当的防火墙配置命令重新配置文件，必要时，参考原来的文件。

ICA2207 **(***服务器*: *调用函数***) 配置文件***文件名***为空。**

解释: 找不到指示的配置文件或找到了文件，但文件为空。找不到文件的最可能的原因是未执行对指出的服务的配置。

用户回答: 验证配置文件的状态。如果文件存在，配置命令期望该文件包含数据。请查阅手册获取附加信息。

ICA2208 *服务器***会话***会话标识符***对于来自非安全的适配器(***源 IP 地址*: *目的 IP 地址***)的***用户标识符***开始。**

解释: 信息在每个指出的会话开始时生成。

ICA2209 *服务器***会话***会话标识符***对于来自非安全的适配器(***源 IP 地址*: *目的 IP 地址***)的***用户标识符***结束**; **字节***总字节***。**

解释: 信息在每个指出的会话结束时生成。字节总数表示在会话期间传送的字节数。不支持字节总数的服务器（例如: ptelnetd） 将指出 0。

ICA2210 **(***服务器***) 用户***用户标识符***试图使用到期口令从***源 IP 地址***(非安全的)登录。**

解释: 指出的用户尝试使用指出的到期口令来建立从非安全适配器上指出的源 IP 至 Firewall 的连接。

用户回答: 给出的口令按每个口令规则集时到期。与系统管理员联系。

ICA2211 **(***服务器***) 用户***用户标识符***试图使用到期口令从***源 IP 地址***(安全的)登录。**

解释: 指出的用户尝试使用指出的到期口令来建立从安全适配器上指出的源 IP 至 Firewall 的连接。

用户回答: 给出的口令按每个口令规则集时到期。与系统管理员联系。

ICA2212 **(***服务器***) 来自***源 IP 地址***(安全的)的用户***名称***的认证成功。**

解释: FW 认证了安全适配器上来自指出的源 IP 的指出的用户名。

ICA2213 **(***服务器***) 来自***源 IP 地址***(非安全的)的用户***名称***的认证成功。**

解释: FW 认证了非安全适配器上来自指出源 IP 的指出的用户名。

ICA2214 **(***服务器***) 来自***源 IP 地址***(非安全的)的用户***名称*** 的认证失败。**

解释: 为来自非安全适配器上所指源 IP 的指出的示用户名的 FW 认证失败。

用户回答: 最可能的原因是错误输入了用户名或口令; 用户名和口令是区分大小写的 (请检查 Caps Lock)。

ICA2215 **(***服务器***) 来自***源 IP 地址***(安全的)的用户***名称*** 的认证失败。**

解释: 为来自安全适配器上所指源 IP 的指示用户名的 FW 认证失败。

用户回答: 最可能的原因是错误输入了用户名或口令; 用户名和口令是区分大小写的 (请检查 Caps Lock)。

ICA2216 **(***服务器***) 来自***源 IP 地址***(非安全的)用户***名称***未从匹配的(验证)口令。**

解释: 请求或需要更改口令而且来自安全适配器上指出源 IP 的所指的用户输入了不匹配的口令。用户认证数据未更改。

用户回答: 更改口令需要输入口令两次, 第二次是为了验证; 最为可能的原因是错误输入了验证口令。

ICA2217 **(***服务器***) 来自***源 IP 地址***(安全的)用户***名称***未从匹配的 (验证) 口令。**

解释: 请求或需要更改口令而且来自安全适配器上指示源 IP 的指示用户输入了不匹配的口令。用户认证数据未更改。

用户回答: 更改口令需要输入口令两次, 第二次是为了验证; 最为可能的原因是错误输入了验证口令。

ICA2218 ***服务器*****会话***会话标识符*****对于来自安全的适配器(***源 IP 地址***: ***目的 IP 地址***)的***会话标识符*****开始; 。**

解释: 信息在每个指出的会话开始时生成。

ICA2219 ***服务器*****会话***会话标识符*****对于来自安全的适配器(***源 IP 地址***: ***目的 IP 地址***)的***用户标识符*****结束; 字节***总字节***。**

解释: 信息在每个指出的会话结束时生成。字节总数表示在会话期间传送的字节数。不支持字节总数的服务器 (例如: ptelnetd) 将指出 0。

ICA2220 **(***服务器***) 用户***用户标识符***从***源 IP 地址***(安全端)至***目的 IP 地址***启动透明代理会话。**

解释: 在每个透明代理会话的开始生成信息。当防火墙对于用户标识符, 源 ip 和目的 ip 都知道后, 开始一个会话。只允许从安全方启动的会话。

系统反应: 允许透明代理。

ICA2221 **(***服务器***) 警告: 控制线路同级端上的 IP (***控制 IP***) 不等于数据线路同级端上的 IP (***数据 IP 地址***)。**

解释: 为了安全性目的 (例如: 防止黑客) 确保控制连接套接字连接的同级的 IP 地址与数据连接套接字连接的同级的 IP 相同。这在使用 Net Dispatcher 或目的地使用了多个适配器的情况下可能不同

系统反应: 检查是否目的 FTP 服务器正使用多个适配器或正使用 Net Dispatcher。确保过滤器仅允许有效的 IP 地址通过端口 20 和端口 21。

ICA2222 **(***服务器***) 警告! 协议违规。接收到 Non-RFC 遵从命令 ***无效字符串***; 期望的***协议字符串***。**

解释: 指出的服务器接收到未预料到的字符串, 它不遵从关联的 RFC; 可能是黑客。

系统反应: 使用遵从指出的服务的 RFC 的客户

ICA3001 ***报警***: 实用户是 *ident 用户名,* 而不是***套接字连接用户名***

解释: 可能安全性破坏尝试; 用户名未认证。

ICA3006 *客户*的*计数值*个字节，*服务器*的*计数值*个字节。

解释: 信息指出的在 sockd 精灵程序和其相关的客户机与服务器之间传送的字节数。

ICA3007 拒绝一个连接，因为超过最大连接数。

解释: socks 服务器配置成仅接受特定客户会话的最大数。在已达到阈值和附加连接请求时，生成这条信息。

系统反应: 关闭了新的连接尝试。

用户回答: 最大并行连接数由 socks5.conf 中的 SOCKS5_MAXCHILD 确定。增加该设置值并刷新服务器。请参阅 IBM Firewall 参考大全以获取细节。 start unused

ICA3010 连接 -- 从*用户*(*real_user*)@*src_addr*连接到 *dst_addr* (*目的端口*)

解释: 建立连接。

ICA3011 连接 -- 从*用户*(*real_user*)@*src_addr*连接到 *dst_addr* (*应用程序*)

解释: 至外界成功的套接字连接。

ICA3012 拒绝连接 -- 从*用户*(*real_user*)@*src_addr*连接到 *dst_addr* (*应用程序*)

解释: 远程主机拒绝连接。

ICA3013 select（） *errno*

解释: 系统错误。

ICA3014 终止 -- 从*用户*(*real_user*)@*src_addr*连接到 *dst_addr* (*目的主机*)。(*客户*的*计数值*字节，*服务器*的*计数值*字节)

解释: 连接终止。

ICA3015 终止 -- 从*用户*(*real_user*)@*src_addr*连接到 *dst_addr* (*目的主机*)。(*客户*的*计数值*字节，*服务器*的*计数值*字节)

解释: 至服务器的连接终止。

ICA3016 ***不能找到适当的接口来与*目的主机*通信

解释: 文件 /etc/sockd.route 不包含指定目的主机的路由选择信息。

ICA3017 不能执行 pid *sockd 进程* 的外壳命令

解释: Sockd 精灵程序无法执行 /bin/sh 命令。

用户回答: 验证 /bin/sh 外壳在系统上可用。

ICA3018 拒绝 -- 从*用户*（*real_user*）@*src_addr*连接到 *dst_addr*

解释: 远程主机拒绝连接。

ICA3019 主机 *socks_src_name* 的 GetDst() 中存在的错误: *errno*

解释: 解析请求的连接的目的地址出错。

ICA3022 第*行号*行存在无效的 ?= 字段

解释: 在 /etc/sockd.conf 文件中发现无效项。

ICA3023 第*行号*行存在无效比较

解释: 在 /etc/sockd.conf 文件中发现无效项。

ICA3024 第*行号*行存在无效项

解释: 在 /etc/sockd.route 文件中发现无效项。

ICA3025 第*行号*行存在无效 permit/deny 字段

解释: 在 /etc/sockd.conf 文件中发现无效项。

ICA3026 第*行号*行存在无效端口数

解释: 在 /etc/sockd.conf 文件中发现无效项。

ICA3027 对于*"cmd"* 外壳命令失败 (*exec 状态*)

解释: 未能显示外壳命令。

用户回答: 验证外壳处理在系统上可用。

ICA3030 **无法打开配置文件（*/etc/sockd.conf*）**

解释: 打开指出的文件的请求失败。

ICA3031 **无法打开路由选择文件 （*/etc/sockd.route*）: *errno***

解释: 打开指出的文件的请求失败。

用户回答: 请向 Firewall 管理员咨询。在 Firewall 安装期间提供一个缺省文件。

ICA3032 **无法打开用户文件 （*用户名文件*）: *errno***

解释: 找不到在允许规则中为 *=userlist 指定的文件名。

ICA3033 **由 Validate() 产生意外结果**

解释: 指定了用户名的 Identd 验证，Identd 以未预料到的结果响应。

ICA3035 **不能连接至*客户主机*的 identd**

解释: 指定用户名的 Identd 验证，Identd 不响应。

ICA3039 **出错 -- 外壳命令 *"cmd"* 包含非字母数字字符。**

解释: 无效外壳命令；见日志信息。

ICA3040 **出错 -- shell_cmd fork() *errno***

解释: Sockd 精灵程序无法经由 'fork()' 切换到子进程

ICA3041 **出错 -- 无法获得客户机地址。**

解释: 'getpeername()' 调用返回的错误。

用户回答: 检查路由和 DNS 配置。

ICA3042 **出错 -- 主机*客户地址*中未定义的命令 (0x*hex-command-received*)。**

解释: 从客户应用程序接收到的无效命令。

用户回答: 客户和 Firewall 支持级别上可能的客户配置问题或不匹配。

ICA3043 **出错 -- 来自主机*客户地址*的版本 (0x*hex-version-number*) 错误。**

解释: Firewall 支持 socks 版本 4.2。

用户回答: 客户和 Firewall 支持级别上可能的客户配置问题或不匹配。

ICA3044 **失败 -- 从 *user*(*real_user*)@*src_addr* 至 *dst_addr*(*application*) 的连接。 错误代码: *命令导致失败 errno*。**

解释: 连接请求失败。

ICA3045 **失败 -- 从 *user*(*real_user*)@*src_addr* 至 *dst_addr* 的联接。出错: 连接至错误的主机 *dst_name* (*dst_port (application)*)。**

解释: 联接请求失败。

ICA3046 **失败 -- 从 *user*(*real_user*)@*src_addr* 至 *dst_addr* 的联接。错误代码: *命令导致失败 errno*。**

解释: 联接请求失败。

ICA3047 **超时 -- 从 *user*(*real_user*)@*src_addr* 至 *dst_addr* 的联接。**

解释: 连接超时。

ICA3048 **外壳命令太长: *命令*...**

解释: /etc/sockd.conf 文件中要执行的命令太长。

ICA3049 **超时 -- 从 *user*(*real_user*)@*src_addr* 至 *dst_addr* (*application*) 的连接。**

解释: 连接超时。

ICA3050 ***匹配的 sockd.conf 过滤器规则***

解释: /etc/sockd.conf 文件中匹配 socks 连接的过滤器规则。

ICA3051 **AIX sockd_route() 不能找到*远程地址*的接口。**

解释: 不能找到接口路径信息。

ICA3052 **把 userid 设置为 ″nobody″ 时出错。**

解释: 不能把子 sockd 进程的 userid 设置为 ″nobody″ 。

ICA3053 **popen（AIX 路由脚本）出错**: *系统错误信息*

解释: 运行脚本以找到路由选择信息失败。

ICA3054 **AIX sockd_route() 中存在严重的内存分配故障。**

解释: 内存分配在尝试集中路由信息时失败。

ICA3055 **对*输入行*的第一个空格进行语法分析时出现严重错误 AIX sockd_route()**

解释: 错误语法分析系统路由信息。

ICA3056 ***输入行*中对第二个空格的语法分析的致命错误 AIX sockd_route()**

解释: 错误语法分析系统路由信息。

ICA3057 **在 AIX sockd_route() 读取路径脚本输出时发生致命错误**: *系统错误信息*

解释: 错误读取脚本输出。

ICA3058 **popen（AIX adapter script）出错**: *系统错误信息*

解释: 未能运行脚本来找到接口信息。

ICA3101 **发送数据时 Sockd 出错 - select()**: *系统错误信息*

解释: 发送数据时发生(SOCKS422)错误。

ICA3102 **发送数据时 Sockd 出错 - write()**: *系统错误信息*

解释: 发送数据时发生(SOCKS422)错误。

ICA3103 **接收数据时 Sockd 出错 - select()**: *系统错误信息*

解释: 接收数据时发生(SOCKS422)错误。

ICA3104 **接收数据时 Sockd 出错 - read()**: *系统错误信息*

解释: 接收数据时发生(SOCKS422)错误。

ICA3105 **不能创建进程标识符文件*文件名*。**

解释: 未能创建/写入（SOCKS422）进程标识符文件。

ICA3106 **Sockd 未能创建子进程**: *系统错误信息*

解释: （SOCKS422）创建子进程来处理 SOCKS 请求的尝试失败。

ICA3107 **设置入站套接字 SO_LINGER 选项失败**: *系统错误信息*

解释: (SOCKS422)不关键

ICA3108 **设置出站套接字 SO_LINGER 选项失败**: *系统错误信息*

解释: (SOCKS422)不关键

ICA3109 **文件*文件名*中第*行号*行存在无效项。**

解释: (SOCKS422) 错误的配置项语法。

ICA3110 **文件*文件名*中第*行号*行存在非法接口字段。**

解释: (SOCKS422) 错误的配置项语法。

ICA3111 **文件*文件名*中第*行号*行存在非法目的 IP。**

解释: (SOCKS422) 错误的配置项语法。

ICA3112 **文件*文件名*中第*行号*行存在非法目的屏蔽。**

解释: (SOCKS422) 错误的配置项语法。

ICA3113 **对文件*文件名*中第*行数*行进行语法分析。**

解释: (SOCKS422) 错误的配置项语法。

ICA3114 **文件*文件名*中找不到有效行。**

解释: （SOCKS422） 配置文件为空，或语法不正确。

用户回答: 更正指出的配置文件。

ICA3115 文件*文件名*中第*行号*行存在无效 'permit/deny' 字段。

解释: (SOCKS422) 错误的配置项语法。

ICA3116 文件*文件名*中第*行号*行存在无效的 '?=' 字段。

解释: (SOCKS422) 错误的配置项语法。

ICA3117 文件*文件名*中第*行号*行存在非法的源 IP。

解释: (SOCKS422) 错误的配置项语法。

ICA3118 文件*文件名*中第*行号*行存在非法的源掩码。

解释: (SOCKS422) 错误的配置项语法。

ICA3119 文件*文件名*中第*行号*行存在无效比较。

解释: (SOCKS422) 错误的配置项语法。

ICA3120 文件*文件名*中第*行号*行存在无效的端口号。

解释: (SOCKS422) 错误的配置项语法。

ICA3121 接收到 SIGUSR1 - 转储 socks 配置。

解释: （SOCKS422）遵循该信息，将活动的配置转储至日志文件的信号。

ICA3122 Sockd 不能创建精灵程序: *系统错误信息*

解释: （SOCKS422）创建以初始化 sockd 精灵程序失败。

用户回答: 改正指出的系统问题并重新启动 sockd。

ICA3123 Sockd 服务器正在启动。

解释: （SOCKS422）Sockd 已成功初始化，正等待连接。

ICA3124 sockd 初始化严重出错 - bind(): *系统错误信息*

解释: (SOCKS422) Sockd 服务器初始化失败，精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 sockd。

ICA3125 sockd 初始化严重出错 - listen(): *系统错误信息*

解释: (SOCKS422) Sockd 服务器初始化失败，精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 sockd。

ICA3126 sockd 严重出错 - main accept(): *系统错误信息*

解释: （SOCKS422） Sockd 服务器主例程失败，精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 sockd。

ICA3127 Sockd 服务器接收到终止信号。

解释: root(或 nobody)终止进程，精灵程序终止。

用户回答: 如果管理员希望这样，则重新启动 sockd （输入 ″sockd″）。

ICA3128 sockd 初始化严重出错 - socket(): *系统错误信息*

解释: Sockd 服务器初始化失败，精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 sockd。

ICA3129 sockd 初始化严重出错 - *失败函数*: *系统错误信息*

解释: Sockd 服务器在指出的函数中初始化失败，精灵程序终止。

用户回答: 改正指出的系统问题并重新启动 sockd。

ICA3130 Sockd 出错 - *失败函数*: *系统错误信息*

解释: sockd 服务器在指定函数中检测出一个错误。精灵程序继续，但连接可能被拒绝或终止。

用户回答: 如果问题仍存在，则停止 sockd，改正指定的系统问题并重新启动 sockd。

ICA3131 读取*文件名*时出错。将使用原先已高速缓存的数据。

解释: 不能读该文件或该文件存在错误数据。使用上一个信息来说明问题。 Sockd 将继续与来自该文件以前版本的高速缓存数据一起操作。

用户回答: 改正指定文件中的错误。

ICA3132　　未知标志*值*。

解释:　不能识别指定的标志，精灵程序终止。

用户回答:　改正语法并重新启动 sockd。

ICA3133　　未知参数*值*。

解释:　不能识别指出的参数，精灵程序终止。

用户回答:　改正语法并重新启动 sockd。

ICA3134　　*选项 1* 和*选项 2* 发生冲突。

解释:　特定选项不能同时被指定，精灵程序终止。

用户回答:　改正语法并重新启动 sockd。

ICA3135　　Sockd 出错 - *失败函数*: 返回码 = 0x*function return code*

解释:　sockd 服务器在指定函数中检测出一个错误。精灵程序终止。

用户回答:　改正指出的系统问题并重新启动 sockd。

ICA3700　　WinSocket 初始化错误: *WinSocket 错误*

解释:　当初始化 WinSocket 时发生错误。

用户回答:　改正指出的系统问题并重新启动 sockd。

ICA4000　　*程序* - 警告: 接收到 *signal* 信号，终止操作...

解释:　因收到信号而终止。

ICA4001　　STOP（停止）*程序*作为 PID *processId*

解释:　打印精灵程序完成结束。资料信息。

ICA4002　　临时 ID

解释:　资料信息。

ICA4003　　子进程 *processId* 存在问题。

解释:　无法创建子进程。

ICA4004　　严重错误。终止了信号 *signal* 中的 fwpagerd。

解释:　信号处理程序。

ICA4005　　没有 fwpagerd 精灵程序在运行，*程序*没有找到。

解释:　因精灵程序未激活而无法发送页面。

ICA4006　　没有与进程 id *processId* 一起运行的 fwpagerd 精灵程序。

解释:　找不到精灵进程的进程 Id。

ICA4007　　START（启动）*程序*作为 PID *processId*

解释:　打印开始信息。资料信息。

ICA4008　　不能为 SIGPIPE 设置 sigignore。

解释:　当设置忽略中断管道信号时失败。

ICA4009　　不能为 SIGCHILD 设置 sigset。

解释:　当设置捕捉死亡子信号时失败。

ICA4010　　不能设置终止进程。

解释:　设置捕捉终止进程的信号失败。

ICA4011　　不能打开套接字。

解释:　当打开套接字时失败。

ICA4012　　不能为 SIGTERM 设置 sigset。

解释:　当设置以捕捉 SIGTERM 和 SIGINT 信号时失败。

ICA4013　　不能设置套接字重用选项。

解释:　当设置套接字再使用选项时失败。

ICA4014　　不能设置套接字 linger 选项。

解释:　当设置套接字 linger 选项时失败。

ICA4015 不能把套接字联接至端口。

解释: 当联接套接字至端口时失败。

ICA4016 不能在套接字上设置侦听。

解释: 当设置到套接字上的侦听时失败。

ICA4017 服务 *servName* 使用 TCP 套接字 *socket*。

解释: 资料信息。

ICA4018 函数调用 select() 失败。

解释: 内部函数调用失败。

ICA4019 new_work() 严重错误。

解释: 来自 new_work 例行程序的内部严重错误。

ICA4020 出错（*程序*）：不能写入流套接字: *socket*

解释: 可能系统错误。

用户回答: 检查套接字用法。

ICA4021 接收响应时存在问题。

解释: 从调制解调器接收响应时存在问题。

用户回答: 检查调制解调器连接和初始化字符串。

ICA4022 请求成功。

解释: 资料信息。

ICA4023 请求失败。

解释: 请求发送页面失败。

ICA4024 出错（*程序*）：优先级超出范围 （*minpri* - *maxpri* ）。

解释: 错误的优先级范围。

用户回答: 改正优先级范围。有效的值从 -1 到 5。

ICA4025 出错（*程序*）：当使用 -n 选项时，地址必须以 ID@carrier 的形式出现。

解释: 错误的命令使用语法。

用户回答: 正确的命令使用语法。

ICA4026 出错（*程序*）：未知主机*主机名*

解释: 不能分辨主机名。

用户回答: 检查主机名。

ICA4027 出错（*程序*）：不能打开流套接字: *errno*

解释: 不能创建新的套接字。

ICA4028 出错（*程序*）：不能设置套接字选项: *errno*

解释: 不能设置套接字持续选项。

ICA4029 出错（*程序*）：不能连接至*主机*: *errno*

解释: 不能连接到主机。

用户回答: 检查串行口配置和设备驱动程序文件的存在。

ICA4030 出错（*程序*）：不能写入流套接字: *errno*

解释: 不能写到流套接字。

ICA4031 接收响应时存在问题。信息的条件未知。

解释: 从调制解调器接收响应时存在问题。

ICA4032 信息成功发送至队列。

解释: 资料信息。 已发送信息到队列。

ICA4033 信息发送失败。无信息发送。

解释: 无法发送信息到寻呼机队列。

ICA4034 *日期*失败(ID *ID* 优先级*优先级*秒数*周期*重试次数*重试次数*) [*fromEntry*] *个人姓名*: *信息*。

解释: 当寻呼发送失败时，显示该信息。

ICA4035 不能重新排列从 *程序*发至个人的信息 *mesg*。

解释: 不能发送到寻呼队列。

ICA4036 成功的 **(ID** *ID* 优先级*优先级*秒数*周期*重试次数*重试次数*) [*fromEntry*] *个人姓名*: *信息*。

解释: 当寻呼发送成功时，显示该信息。资料信息。

ICA4037 转储至 *dumpFile* **(ID** *ID* 优先级*优先级* 秒数*周期*重试次数*重试次数*) [*fromEntry*] *个人姓名*: *信息*。

解释: 转储不能立即发送的页面到文件中以便以后再试。

ICA4038 不能写入转储文件*dumpFile*。

解释: 不能写入转储文件。

用户回答: 检查文件系统许可权。

ICA4039 **IpcKey**: **0x***IpcKey*

解释: 资料信息。

ICA4040 超过了 *retryTime* 分钟的重试时间。

解释: 在指定分钟后初始化调制解调器失败。

用户回答: 检查初始化字符串。

ICA4041 发现数字寻呼机中有字母数字信息。

解释: 数字寻呼机不能包含字母数字数据。

用户回答: 正确使用 smitty/SMIT 菜单。

ICA4042 个人不能接收寻呼。

解释: 寻呼机未打开。

用户回答: 检查是否打开寻呼机。

ICA4043 通信公司 *carrier* 不存在。

解释: 不存在指定的通信公司。

用户回答: 正确使用 smitty/SMIT 菜单。

ICA4044 通信公司 *carrier* 没有 **DTMF** 电话号码。

解释: 指定的通信公司没有 DTMF 电话号码。

用户回答: 正确使用 smitty/SMIT 菜单。

ICA4045 寻呼机号 *pagerNumber* 超出了通信公司的最大长度 *carrLen* 。

解释: 寻呼机号码对于通信公司的最大值来讲太长。

用户回答: 使用另一个比通信公司最大值较短的寻呼机号。

ICA4046 寻呼机号 *pagerNumber* 超出了 *defaultCarrLen* 的缺省长度。

解释: 当缺省长度太短时出现该信息。

用户回答: 正确使用 smitty/SMIT 菜单。增加缺省长度。

ICA4047 调制解调器文件*调制解调器文件名*中第*行号*行存在问题。

解释: 调制解调器定义文件包含一个无效的字符。

用户回答: 正确使用 smitty/SMIT 菜单。

ICA4048 不能打开设备 **/dev/***deviceName* 上的调制解调器。

解释: 不能打开指定设备上的调制解调器。

用户回答: 检查或重新配置串行口。检查设备。

ICA4049 打开 **/dev/***deviceName* 上的调制解调器。

解释: 资料信息。 调制解调器在串行口上已成功检测。

ICA4050 不能设置调制解调器特性。

解释: 当尝试去设置调制解调器特性时失败。

用户回答: 检查调制解调器初始化字符串。

ICA4051 在 *numInitTries* 次重试后不能初始化调制解调器。

解释: 调制解调器不能初始化。

用户回答: 检查调制解调器初始化字符串和串行口配置。

ICA4052 不能拨打寻呼机号码*pagerNumber*

解释: 不能拨寻呼机号。

用户回答: 检查寻呼机号的有效性。

ICA4053　　不能挂起调制解调器。

解释: 不能挂起调制解调器。

用户回答: 检查调制解调器初始化字符串和使用的挂起命令。

ICA4054　　不能拨打信息*message*

解释: 不能拨信息。

ICA4055　　调制解调器文件*文件名*中第*行号*行存在问题。

解释: 无效的调制解调器定义文件。

用户回答: 正确使用 smitty/SMIT 菜单。

ICA4056　　不能拨打通信公司 *carrier* 的 DTMF 号码 (*DTMFnumb*)。

解释: DTMF 号码可能被更改或对该通信公司已不正确。

用户回答: 正确使用 smitty/SMIT 菜单。

ICA4057　　不能发送块。

解释: 当尝试去发送块时失败。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4058　　对已发送的块无响应。

解释: 发送块后不能从通信公司接收响应。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4059　　不能接收对信息传递的响应。

解释: 信息传递后不能从通信公司接收响应。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4060　　不能发送寻呼机 id。

解释: 不能发送寻呼机 id。

用户回答: 使用 smitty/SMIT 菜单来检查寻呼机号和通信公司参数。

ICA4061　　不能发送自动方式请求的结束 <CR>。

解释: 不能发送自动方式请求的结束 <CR>。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4062　　不能发送自动方式请求。

解释: 不能发送自动方式请求信号。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4063　　*numTries* 次重试后，不能接收来自通信公司 *carrier* 的继续向前信息。

解释: 此刻通信公司可能忙。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数并稍后再试。

ICA4064　　在通信公司 *carrier* 提示期间通信出错。

解释: 通信错误可能由于很多原因发生。稍后请再试一次。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数并稍后再试。

ICA4065　　不能接收对注册的响应。

解释: 调制解调器不能接收对注册的响应。

用户回答: 检查调制解调器初始化字符串和通信公司参数。

ICA4066　　通信公司 *carrier* 没有对试图注册的举动作出响应。

解释: 通信公司没有响应注册尝试。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数并稍后再试。

ICA4067　　通信公司 *carrier* 发回 *receiveDataString*。

解释: 通信公司发送回一些错误信息或忙信息。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数并稍后再试。

ICA4068 通信公司 *carrier* 在注册期间强迫断开。

解释: 通信公司在注册中强迫断开。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4069 通过 *ConnectRetryMax* 次循环重试致使信息转储至通信公司*carrier*。

解释: 如果通信公司正忙，程序转储寻呼并稍后再试。

ICA4070 因为 *maxTotalTries* 次会话连接尝试失败，所以跳过至通信公司 *carrier* 的信息。

解释: 在一系列尝试后不能联系通信公司。

用户回答: 检查通信公司参数并稍后再试一次。

ICA4071 出错（*程序*）：不能为通信公司重试分配内存：*errno*。

解释: 可能的系统或内存分配错误。

ICA4072 出错（*程序*）：不能添加至通信公司重试列表：*errno*。

解释: 通信公司可能不存在。

用户回答: 检查通信公司的有效性并再试一次。

ICA4073 *retryCount* 次重试后，至使用 *phoneNumber* 的通信公司 *carrier* 的数据连接失败。

解释: 数据连接失败。

用户回答: 使用 smitty/SMIT 菜单来检查调制解调器连接和通信公司参数。

ICA4074 *numTries* 次重试后，没有接收到来自通信公司 *carrier* 的 ID 提示。

解释: 通信公司带 ID 或确认提示符的响应失败。

用户回答: 确认通信公司使用 TeleAlphanumeric 协议。

ICA4075 用通信公司 *carrier* 注册时，通信出错。

解释: 通信错误可能由于很多原因发生。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4076 超过了通信公司 *carrier* 的最多注册次数。

解释: 通信公司在指定尝试次数内响应失败。

用户回答: 检查通信公司参数并稍后再试一次。

ICA4077 没有接收到来自通信公司 *carrier* 的继续向前信息。

解释: 通信公司无法以继续向前提示符为响应。

用户回答: 检查通信公司参数并稍后再试一次。

ICA4078 不能创建块。

解释: 通信公司不能为传输创建块。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4079 通信公司 *carrier* 没有对信息传递作出响应。

解释: 通信公司传递信息有困难。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4080 通信公司 *carrier* 在信息传递期间强迫断开。

解释: 通信公司在信息传递中强迫断开。

用户回答: 检查通信公司参数和调制解调器初始化字符串。

ICA4081 通信公司 *carrier* 拒绝接收信息或寻呼机 ID。

解释: 通信公司拒绝接收寻呼机信息或寻呼机 id。

用户回答: 检查寻呼机 id 的有效性、寻呼机的激活状态和通信公司参数。

ICA4082 在信息传递至通信公司 *carrier* 时，通信出错。

解释: 通信错误可能由于很多原因发生。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4083 *maxTries* 次重试后仍没有接收到来自通信公司 *carrier* 的确认信息。

解释: 如果通信公司正忙或不能建立连接时则出现该信息。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数，并在几分钟后再试。

ICA4084 不能发送 <EOT>。

解释: 调制解调器不能发送 <EOT>。

用户回答: 检查调制解调器连接和初始化字符串。

ICA4085 不能接收对 <EOT> 的响应。

解释: 调制解调器不能接收至 <EOT> 的响应。

用户回答: 检查调制解调器连接和初始化字符串。

ICA4086 通信公司 *carrier* 没有对 <EOT> 作出响应。

解释: 通信公司不能对被发送的数据作出响应。

用户回答: 检查通信公司的有效性和调制解调器连接。

ICA4087 通信公司 *carrier* 以因内容出错数据无法接收作为响应。

解释: 通信公司不能对被发送的数据作出响应。

用户回答: 使用 smitty/SMIT 菜单来检查通信公司参数。

ICA4088 不能打开缺省文件 *defaultPathname*。

解释: 调制解调器缺省文件可能不存在或有不正确的许可权。

用户回答: 检查文件的存在和许可权。

ICA4089 缺省文件 *defaultPathname* 不完整。

解释: 调制解调器缺省文件有遗漏数据。

用户回答: 正确使用 smitty/SMIT 菜单。

ICA4090 缺省文件 *defaultPathname* 中第 *lineNumber* 行存在无效的外部行号。

解释: 通信公司数据库文件有一个无效的外部行号。

用户回答: 清除通信公司数据库文件。

ICA4091 缺省文件 *defaultFile* 中第 *lineNumber* 行存在无效的波特率值。

解释: 通信公司数据库文件有一个无效的波特率。

用户回答: 清除通信公司数据库文件。

ICA4092 缺省文件 *defaultFile* 中第 *lineNumber* 行存在无效的数据位值。

解释: 通信公司数据库文件有一个无效的数据位值。

用户回答: 清除通信公司数据库文件。

ICA4093 缺省文件 *defaultFile* 中第 *lineNumber* 行存在无效的奇偶性值。

解释: 通信公司数据库文件有一个无效的奇偶性值。

用户回答: 清除通信公司数据库文件。

ICA4094 缺省文件 *defaultFile* 中第 *lineNumber* 行存在无效的停止位值。

解释: 通信公司数据库文件有一个无效的停止位值。

用户回答: 清除通信公司数据库文件。

ICA4095 缺省文件 *defaultFile* 中第 *lineNumber* 行存在不确定的标记 *tag id* 。

解释: 通信公司数据库文件有一个无效的标记。

用户回答: 清除通信公司数据库文件。

ICA4096 参数的数目不正确。

解释: 资料信息。

ICA4097 出错（*程序*）：不能创建通信公司列表。内存问题。

解释: 可能的系统或内存问题。

ICA4098 出错（*程序*）：寻呼通信公司文件 *carrierFile* 时出错。

解释: 通信公司数据库文件有一些无效数据。

用户回答: 检查通信公司数据库文件的无效标记。

ICA4099 出错（*程序*）：不能获得 IPC 令牌 *errno*。

ICA4100 出错（*程序*）：不能创建重试列表。可能是内存问题。

解释: 可能系统错误或内存问题。

ICA4101 出错（*通信公司*）：不能创建队列，**page_q_err**: *pageQErr*。

ICA4102 出错（*程序*）：不能设置对 **SIGTERM/SIGINT** 信号的捕捉: *errno*。

解释: 可能系统错误。

ICA4103 出错（*程序*）：不能设置通信公司 *carrier* 的调制解调器特性。

解释: 不能设置调制解调器。

用户回答: 检查串行口配置和初始化字符串。

ICA4104 通信公司 *carrier* 的标记 *tag* 丢失。

解释: 丢失调制解调器信息。一个标记可能是波特率、外部行等等。

用户回答: 检查调制解调器配置文件的无效字符。

ICA4105 通信公司 *carrier* 必须至少拥有一个电话号码。

解释: 通信公司必须包含电话号码。

用户回答: 使用 smitty/SMIT 菜单来添加电话号码。

ICA4106 不能打开文件 *CarrierFileName*。

解释: 通信公司数据库文件必须存在。

用户回答: 如果不存在，通过使用 smitty/SMIT 菜单来创建一个。

ICA4107 第 *lineNumber* 行太长。

解释: 通信公司数据库文件中的行太长。

用户回答: 检查通信公司数据库文件的无效行。

ICA4108 第 *lineNumber* 行存在未知标记。

解释: 通信公司数据库文件存在未知标记。

用户回答: 检查通信公司数据库文件的无效标记。

ICA4109 第 *lineNumber* 行存在未知序列。

解释: 通信公司数据库文件存在未知序列。

用户回答: 检查通信公司数据库文件的无效序列。

ICA4110 通信公司 *carrier* 无效并跳过它。

解释: 不能为寻呼目的使用通信公司。

用户回答: 检查通信公司的有效性。

ICA4111 不能添加通信公司至列表。

解释: 不能添加通信公司到列表。

用户回答: 检查通信公司的有效性和电话号码。

ICA4112 第 *lineNumber* 行中通信公司名丢失或太长.

解释: 通信公司名称丢失。

用户回答: 使用 smitty/SMIT 菜单来添加通信公司。

ICA4113 不能分配新的寻呼通信公司: *carrier*。

解释: 不能分配通信公司到列表。

用户回答: 检查通信公司的有效性和电话号码。

ICA4114 第 *lineNumber* 行的值太长。

解释: 通信公司数据库文件中遇到的行太长。

用户回答: 清除通信公司数据库文件中的长行。

ICA4115 忽略第 *lineNumber* 行中的重复标记 *tag*。

解释: 遇到重复的标记。

用户回答: 从通信公司数据库文件删除重复的标记。

ICA4116 第 *lineNumber* 行中值不存在。

解释: 遇到空白字段。

用户回答: 使用 smitty/SMIT 菜单在空白字段中添加值。

ICA4117 第 *lineNumber* 行中的值必须是 Y、Yes、 N 或 No 。

解释: 该字段需要 Y、 Yes、 N 或 No。

用户回答: 使用 smitty/SMIT 菜单来添加或更改有效的数据。

ICA4118 第 *lineNumber* 行中的值必须大于零。

解释: 该字段必须是正数。

用户回答: 使用 smitty/SMIT 菜单更改值为正数值。

ICA4119 第 *lineNumber* 行中的值无效。

解释: 在指定行上遇到无效值。

用户回答: 使用 smitty/SMIT 菜单来更改值。

ICA4120 通信公司 *name* 无效并跳过它。

解释: 遇到无效通信公司。

用户回答: 使用 smitty/SMIT 菜单来添加有效的通信公司。

ICA4121 不能添加通信公司至列表。

解释: 不能添加通信公司到寻呼列表。

用户回答: 检查通信公司的有效性。

ICA4122 忽略第 *lineNumber* 行中的重复标记 *tag*。

解释: 在通信公司节中遇到重复标记。

用户回答: 清除包含重复值的通信公司节。

ICA4123 出错（*程序*）: 不能获得 IPC 令牌: *errNo*

解释: 程序不能获得 IPC 令牌。

ICA4124 出错（*程序*）: 读队列时出现错误 *pageqErr* 。

解释: 程序不能读队列。

ICA4125 *count* 个队列项。

解释: 资料信息。

ICA4126 删除带有 ID *id* 的信息。

解释: 资料信息。

ICA4127 ID *id* 不在队列中。

解释: 资料信息。

ICA4128 出错（*程序*）: 试图删除 ID *id* 时出现错误 *pageqErr* 。

解释: 尝试去删除队列的 ID 。

ICA4129 密钥是: *entryKey* 的内容为 @ *ptr*: *ptr*。

解释: 仅为资料信息。

ICA4130 调制解调器特性:

解释: 调制解调器初始化信息。

ICA4131 名称: *modemName*

解释: 调制解调器初始化信息。

ICA4132 Init（初始化）: *initString*

解释: 调制解调器初始化信息。

ICA4133 命令方式: *command*

解释: 调制解调器初始化信息。

ICA4134 命令终止符: 0x*terminator*

解释: 调制解调器初始化信息。

ICA4135 拨号: *dial*

解释: 调制解调器初始化信息。

ICA4136 **拨号暂停**: *pause*

解释: 调制解调器初始化信息。

ICA4137 **拨 #**: *diallb*

解释: 调制解调器初始化信息。

ICA4138 **拨 ***: *dialstar*

解释: 调制解调器初始化信息。

ICA4139 **挂起**: *hangup*

解释: 调制解调器初始化信息。

ICA4140 **有效的命令响应**: *validCommandresp*

解释: 调制解调器初始化信息。

ICA4141 **有效连接**: *validConnect*

解释: 调制解调器初始化信息。

ICA4142 **回显**: *echo*

解释: 调制解调器初始化信息。

ICA4143 **调制解调器调试记录**: **PUTS(***id* **) txd->** *outStr*

解释: 调制解调器信号交换信息。

ICA4144 **调制解调器调试记录**: **PUTC(***id***) txd->** *outStr*

解释: 调制解调器信号交换信息。

ICA4145 **调制解调器调试记录**: **GET rxd->** *记录标识符*

解释: 调制解调器信号交换信息。

ICA4146 **调制解调器调试记录**: **INPUT(***记录标识符*

解释: 调制解调器信号交换信息。

ICA4147 **调制解调器调试记录**: **) rxd->**

解释: 调制解调器信号交换信息。

ICA4148 **调制解调器调试记录**: **WAITFOR(***记录标识符*

解释: 调制解调器信号交换信息。

ICA4149 **不能分解子信号。**

解释: 分解 SIGCHLD 信号。

ICA4150 **不能合并子信号。**

解释: 合并 SIGCHLD 信号。

ICA4151 **热启动文件** *filePathname* **不存在。**

解释: 资料信息。

ICA4152 **不能打开热启动文件** *filePathname* **。**

解释: 资料信息。

ICA4153 **热启动文件** *filePathname* **中的行太长。**

解释: 热启动文件包含一些无效字符。

ICA4154 **热启动文件** *filePathname* **含有无用的数据。**

解释: 资料信息。

ICA4155 **热启动文件** *filePathname* **为空。**

解释: 资料信息。

ICA4156 **热启动文件** *filePathname* **第** *lineNumber* **行存在错误的被访地址** *address*, **忽略它。**

解释: 热启动文件包含一些无效字符。资料信息。

ICA4157 **热启动文件** *filePathname* **第** *lineNumber* **行存在错误格式，忽略它。**

解释: 热启动文件包含一些无效字符。资料信息。

ICA4158 热启动文件 *filePathname* 第 *lineNumber* 行没有信息，忽略它。

解释: 热启动文件没有信息。资料信息。

ICA4159 热启动文件 *filePathname* 第 *lineNumber* 行序列出错，忽略它。

解释: 热启动文件包含一些无效字符。资料信息。

ICA4160 完成文件 *filePathname* 中 *count* 条信息的热启动。

解释: 资料信息。

ICA4161 出错（*程序*）：出现太多的连续子错误。

解释: 一行有太多子进程错误。当通信公司或调制解调器定义文件有一些无效字符时会发生这种情况。

用户回答: 使用 smitty/SMI 菜单来检查通信公司数据库文件和调制解调器定义文件。

ICA4162 子进程不能执行*程序*: *errno*。

解释: 可能系统错误。

ICA4163 出错（*errno*）：子进程不能创建子进程: *程序名*。

解释: 可能系统错误。

ICA4164 不能创建寻呼通信公司列表。

解释: 内部程序错误。

ICA4165 寻呼通信公司文件 *carrierFile* 出错。

解释: 通信公司数据库包含一些无效数据。

用户回答: 通过使用 smitty/SMI 菜单来检查通信公司数据库文件。

ICA4166 资料信息。 IPC 密钥是: 0x*IpcKey*。

解释: 资料信息。

ICA4167 不能创建队列 **page_q_err**: *pageQerr*。

解释: 当尝试去创建队列时失败。

ICA4168 在 *time* 时创建寻呼热启动文件。

解释: 资料信息。

ICA4169 来自 *objfrom* *信息*的优先级 **-p** *priority* *numPager*

解释: 资料信息。

ICA4170 来自 *from* *信息*的优先级 **-p** *priority* *alpaPager@carrier*

解释: 资料信息。

ICA4171 来自 *from* *信息*的优先级 **-p** *priority* **-n** *numPager* *@carrier*

解释: 资料信息。

ICA4172 寻呼机热启动文件终止。

解释: 资料信息。 表示报文结束。

ICA4173 不能写入热启动文件 *warmstrtFile*。

解释: 热启动文件可能不存在。

ICA4174 来自 *user@host* 的 *time* **STATUS-REQUEST**

解释: 显示状态请求信息。

ICA4175 来自 *user@host* 的 *time* **SUMMARY-REQUEST**

解释: 显示摘要请求信息。

ICA4176 *count* 个队列项。

解释: 计算寻呼机队列的队列输入项数。

ICA4177 **Oldest** 项: 在 *time* 时接收到 **ID** *id* 。

解释: 显示队列中最早的输入项。

ICA4178 扩展失败后重新连接内存。

解释: 可能系统错误。

ICA4179 扩展不能对齐后重新连接内存。

解释: 可能系统错误。

ICA4180 在 **page_q_print()** 中不能关闭 **PAGE_Q** 信号: *errno*。

解释: 可能系统错误。

ICA4181 在 **page_q_print()** 中不能打开 **PAGE_Q** 信号: *errno*。

解释: 可能系统错误。

ICA4182 链接 *headLink* **->** 信息 **ID**: *id*。

解释: 资料信息。

ICA4183 优先级: *priority*。

解释: 资料信息。

ICA4184 个人: *name*。

解释: 资料信息。

ICA4185 通信公司: *carrier*。

解释: 资料信息。

ICA4186 信息（**Mesg**）: *message*。

解释: 资料信息。

ICA4187 不能得到共享 **RAM** : *errno*。

解释: 可能系统错误。

ICA4188 不能得到附加的共享 **RAM** : *errno*。

解释: 可能系统错误。

ICA4189 不能得到 **PAGE_Q** 信号。

解释: 可能系统错误。

ICA4190 在 **page_q_create()** 中不能初始化 **PAGE_Q** 信号: *errno*。

解释: 可能系统错误。

ICA4191 在 **page_q_create()** 中不能设置 **PAGE_Q** 信号: *errno*。

解释: 可能系统错误。

ICA4192 在 **page_q_empty()** 中不能关闭 **PAGE_Q** 信号: *errno*。

解释: 可能系统错误。

ICA4193 在 **page_q_empty()** 中不能打开 **PAGE_Q** 信号: *errno*。

解释: 可能系统错误。

ICA4194 在 **page_q_enq(***name***,***message***)** 中不能关闭 **PAGE_Q** 信号: *errno*。

解释: 可能系统错误。

ICA4195 在 **page_q_enq()** 中不能打开 **PAGE_Q** 信号: *errno*。

解释: 可能系统错误。

ICA4196 **page_q_enq()**: **ID(***id***)** 优先级**(***priority***)** 个人**(***name***)** 信息**(***message***)**。

解释: 资料信息。

ICA4197 在 **page_q_head()** 中不能关闭 **PAGE_Q** 信号: *errno*。

解释: 可能系统错误。

ICA4198 在 **page_q_head()** 中不能打开 **PAGE_Q** 信号: *errno*。

解释: 可能系统错误。

ICA4199 **在 page_q_first() 中不能关闭 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4200 **在 page_q_first() 中不能打开 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4201 **在 page_q_next() 中不能关闭 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4202 **在 page_q_next() 中不能打开 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4203 **在 page_q_tail() 中不能关闭 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4204 **在 page_q_tail() 中不能打开 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4205 **在 page_q_del() 中不能关闭 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4206 **在 page_q_del() 中不能打开 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4207 **page_q_del(*ID*)。**

解释: 调试信息。

ICA4208 **在 page_q_deq() 中不能关闭 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4209 **在 page_q_deq() 中不能打开 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4210 **page_q_del(): ID(*id*) 优先级(*priority*) 个人(*name*) 信息(*message*)。**

解释: 资料信息。

ICA4211 **在 page_q_walk() 中不能关闭 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4212 **在 page_q_walk() 中不能打开 PAGE_Q 信号: *errno*。**

解释: 可能系统错误。

ICA4213 **PAGE_Q 满。**

解释: 寻呼队列已满。

用户回答: 过一会儿发送寻呼。

ICA4300 **挂起。**

解释: 挂起呼叫。

ICA4301 **初始化调制解调器。**

解释: 用初始字符串初始化调制解调器。

ICA4302 **拨号 .....**

解释: 拨电话号码。

ICA4303 **等待连接。**

解释: 等待调制解调器连接。

ICA4304 **CONNECTED** *速度*

解释: 以指示的速度连接(波特率)。

ICA4305 **CONNECTED!!!!!!!**

解释: 已连接到寻呼服务供应商

ICA4306　　请求自动方式的提示。

解释: 自动的方式请求提示符。 等待 ″ID=″

ICA4307　　提示 OK.....

解释: 从供应商获得 ″ID=″ 。

ICA4308　　发送自动方式请求。

解释: 发送 ID 和 SST 到寻呼服务供应商

ICA4309　　发送自动方式请求 .....OK!

解释: 获得 [p; 回答。意味通信成功

ICA4310　　发送出信息

解释: 发送出信息块

ICA4311　　等待结果

解释: 等待确认

ICA4312　　接收到 Ack 。寻呼成功。

ICA4313　　接收到 Nak ， 再次发送块。尝试 *NakTries* 次 。

解释: 接收到 Nak 。寻呼供应商要求再发送。

ICA4314　　事务处理出错。 再次发送块。尝试 *RsTries* 次。

解释: 事务处理出错。 再发送块。

ICA4315　　通信公司终止连接。

解释: 寻呼供应商终止对话。向供应商查询该问题。

ICA4350　　fwpage [carrier=″...″] [modem=″...″] [ID=″...″] [msg=″...″]

解释: fwpage 的用法。检查参数并再试一次。

ICA4351　　*该*文件不存在

解释: 检查文件看是否在正确的目录下。carriers.cfg、modems.cfg 和 pager.cfg 必须在使用该代码前创建。

ICA4352　　*What* 文件遭破坏。

解释: 用户修改了该文件，该文件不在节格式中。所有的属性应该通过 GUI 输入。

ICA4353　　*What* 太长，请缩短它然后再试一次

解释: ’What’ 参数太长。 缩短它并再试一次。

ICA4354　　*What* 出错。

解释: 如果波特率出错，有效的选项是: 600、 1200、2400、 4800、 9600、 14400。 如果数据位(每字节)出错，有效的选项是: 7、8 。如果停止位出错，有效的选项是: 1、2 。如果外部行前缀出错，输入应该仅是数字。如果寻呼方法出错，该版本中仅支持 TAP 。如果寻呼机 ID 出错，检查一下它是否都为数字。如果奇偶性出错，有效的选项是: O(奇数)、E(偶数)、N(无)、S(空格)、M(标记)。如果 COM 端口出错，有效的选项是: COM1、COM2 .... 该版本中的 COM 端口应小于 10 。如果信息字符出错，检查信息看里面是否有特殊字符。

ICA4355　　在 *where* 中设置参数时出错。

解释: 无法在 (where) 中设置参数。 检查参数并再试一次。

ICA4356　　在 *When* 时，COM 端口读错误。

解释: COM 端口读错误。设置调制解调器回显并再试一次。

ICA4357　　在 *Where* 时，COM 端口写错误。

解释: COM 端口写错误。

ICA4358　　设置 *What* 时出错

解释: 设置 ’What’ 指出的错误。 检查日志文件并找出错误。

ICA4359　　在 *Where* 处超过最多可尝试的次数。程序异常终止 .....

解释: 尝试在 60 分钟内 60 次打开 COM 端口。全部失败 如果是这种情况，请检查硬件连接。 尝试在 10分钟内 10 次发送寻呼机信息。全部失败。 如果是这种情况，寻呼供应商可能关闭。

ICA4360 通信公司电话号码中存在未知字符: **pCarrierPhoneNum*

解释: 通信公司电话号码中找到一个不能识别的字符。请检查号码并再试一次。

ICA4361 警告!!! 寻呼提供者的调制解调器通常速度应小于 2400。

解释: 这只是一个警告。寻呼提供者的调制解调器速度通常设置为小于 2400。

ICA4362 无法初始化调制解调器

解释: 更改调制解调器初始化字符串并再试一次。

ICA4363 调制解调器返回时出错。

解释: 调制解调器通信错误

ICA4364 *tries* 次尝试打开 COM 端口时出错。在 1 分钟内重试

解释: 打开 COM 端口错误。可能另一个程序正在使用它。1 分钟后自动重试

ICA4365 *tries* 次尝试发送寻呼失败。在 1 分钟内重试

解释: 发送页面失败。检查记录文件以找出确切的原因。

ICA4366 信息太长，请截断它

解释: 只是一个警告。信息长度太长。截断以适合它。

ICA4367 将最大信息长度重新设置成内部定义值: *msg-length*

解释: 因为用户定义的信息长度大于内部定义(80)，所以复位最大信息长度到缺省值。

ICA4368 执行: *Where* 出错

解释: 如果打开 COM 端口出错，检查配置并再试一次。如果关闭 COM 端口出错，则为系统问题。如果清除 COM 端口出错，则为系统问题。如果发送拨号命令出错，则为拨号命令问题。检查看是否是 Haye 兼容调制解调器。如果发送 ID 请求出错，检查寻呼供应商是否支持 TAP 协议。如果发送自动提示符出错，检查寻呼机服务工作是否正确。如果发送信息出错，检查日志文件以找出失败原因。如果提示符出错,则无法从寻呼机供应商取回提示符。

ICA4369 因事务太多出错。异常终止 ....

解释: 太多事务处理错误，异常终止该尝试。

ICA4370 接收到太多的 Nak，异常终止程序 .....

解释: 从寻呼机供应商接收到太多 Nak，异常终止该尝试。

ICA4371 COM 端口上含函数*函数名*的 *szComPort* 返回 *Error Number*。

解释: 检查参数并再试一次。

ICA4372 调制解调器返回错误信息..... *ReturnMessage*

解释: 信息是: 未连接、 铃响，但未连接、 无通信公司、 无拨号音、 忙、 无回答。

ICA4373 (*function name*) 来自调制解调器或通信公司的未知响应代码: *char1*，*char2*。

解释: 该信息报告了来自调制解调器或通信公司的响应，即 Firewall 的调页功能不能识别。 char1 和 char2 是响应中的最先 2 个字符的 ascii (十六进制)代码。

用户回答: 当查询调制解调器指令或通信公司以确定未知响应意义时，使用该信息。

ICA5005 SKIT 初始化失败。返回码是: *return code*

解释: 安全套接字初始化失败，从显示的 SKIT 返回码。

ICA5014 远程客户隧道服务器侦听端口 *server port #*

解释: 显示为 sslrctd 配置的端口号。

ICA5015 从 *chp0.chp1.chp2.chp3* 接受连接

解释: 显示客户机的 IP 地址。

ICA5017 无法获得安全套接字。函数 **skit_secure_soc_init retcode** 为: *function retcode*

解释: 因为 skit_secure_soc_init() 失败，无法获得安全套接字。

ICA5018 **使用的从属服务器 cipher specs 是 *spec1 spec2 spec3***

解释: 显示密码规范说明。

ICA5019 **不能得到空闲 Homenet IP 池。**

解释: 动态过滤器问题。

ICA5020 **不能打开远程客户程序文件。**

解释: 文件 /etc/security/rcsfile.cfg 不可用。

用户回答: 检查文件存在和内容。

ICA5021 **找不到'*keyword*' 关键字。**

解释: 文件 /etc/security/rcsfile.cfg 无此关键字。

用户回答: 检查并更正 /etc/security/rcsfile.cfg。

ICA5024 ***例行程序名* 中函数 skit_secure_soc_write() 出错。**

解释: skit_secure_soc_write() 在此例行程序中失败。

ICA5025 **ACKClient() 中的函数 skit_secure_soc_write() 出错。**

解释: ACKClient() 例行程序中的函数 skit_secure_soc_write() 失败。

ICA5026 **从*例行程序名*中的客户机接收到无效返回码。**

解释: 从该例行程序的客户接收到未预料到的返回码。

ICA5027 **从*例行程序名*中的客户机接收到错误请求的返回码。**

解释: 该例行程序返回码信息中的请求代码出错。

ICA5028 **无效的登录请求。**

解释: 登录请求信息的格式无效。

ICA5030 **未知远程客户 ID**: *远程客户 ID*

解释: 该用户 ID 对于防火墙机器未知。

用户回答: 更正该远程客户的用户信息。

ICA5031 **RCTLoginPhase 中的函数 skit_secure_soc_write 出错。**

解释: skit_secure_soc_write() 在登录阶段失败。

ICA5035 **无效的退出请求。**

解释: 注销请求信息的格式无效。

ICA5067 **接收到无效信息包。**

解释: 接收到的信息包格式无效。

ICA5078 **获得 SvrReqHandler() 中无法识别的请求**

解释: 接收到不能识别的请求并将其忽略。

ICA5082 **至客户*远程客户 ID*的隧道已断开。**

解释: 带有该 ID 的远程客户的隧道已断开。

ICA5086 **ID: *userid* 未定义。**

解释: 该用户 ID 在防火墙机器上不存在。

ICA5087 **'*userid*' 的认证失败。**

解释: 该用户 ID 认证失败。

ICA5089 **功能 rcFilterClear() 失败。返回码是*返回码*。**

解释: rcFilterClear() 带有该返回码失败。

用户回答: 检查 IPSEC LAN 客户外表。这些产品不能共存。

ICA5090 **函数 rcFilterInit() 失败。返回码是*返回码***

解释: rcFilterInit() 带有该返回码失败。

ICA5091 **函数 TunnelUp() 不能运行可执行文件*命令行*。**

解释: 显示的命令行未能进行 system() 调用。

ICA5092 **不能从 recoverstash 函数调用得到密钥环口令。**

解释: 不能从 stash 文件恢复密钥环口令。

ICA8001 **SYSLOG/udp: 未知服务**

ICA8002 *函数名***函数失败 - ***错误号*****, errno2 = 0x***errno2*

解释: 处理终止，因为 syslogd 不能执行指定函数。errno 信息是附加在错误信息上的。

用户回答: 联系系统程序员。系统程序员: 使用 errno 信息来确定失败原因。

ICA8004 **AF_INET 套接字上检测出错误，\ slogd 将不再监控套接字**

ICA8006 **未知优先级名称 \"***priority***\"**

解释: 在配置文件中找到的优先级名称无效。

用户回答: 联系系统程序员。系统程序员: 检查配置文件。

ICA8007 **未知设施名称 \"***facility***\"**

解释: 在配置文件中找到的设施名称无效。

用户回答: 联系系统程序员。系统程序员: 检查配置文件。

ICA8008 *时间戳记***时来自 SYSLOG@ ***主机名*****的信息 ...**

解释: syslog 精灵程序配置文件包含将 syslog 信息发送到所有注册用户的入口项。该信息将发送到所有注册到系统（syslog 精灵程序正在其上运行的）的用户。

用户回答: 无 SystemProgrammer : 无

ICA8009 **SYSLOGD 在信号***信号* **处退出**

解释: syslog 精灵程序接收到一个信号，使 syslog 精灵程序退出。

用户回答: 无 SystemProgrammer : 无

ICA8010 **SYSLOGD 重新启动**

ICA8012 **SYSLOGD 无法记录到 SMF -** *error_text*

解释: 在将记录写入 SMF 时出错。出错文本信息是附加在错误信息上的。

用户回答: 联系系统程序员。系统程序员: 使用出错文本信息来确定 SMF 写入失败的原因。

ICA8013 **更新进程状态失败，返回码 = 0x***return_code*

解释: 当要为 Firewall 内核进程更新 syslogd 进程时出错。返回码概要叙述了从更新进程状态调用返回的特定错误。

用户回答: 联系系统程序员。系统程序员: 联系维修人员。

ICA8014 **SYSLOGD 调用指定了未知选项 (-***startup_option***)**

解释: 当要启动 syslogd 精灵进程时出错。syslogd 调用不支持指定的选项。

用户回答: 检查启动选项并重新启动 syslogd 精灵程序。系统程序员: 如果问题仍存在，联系维修人员。

ICA8015 **配置文件项 (***config_data***) 无效**

解释: 当要从 SYSLOG 配置文件来分析配置入口项时出错。

用户回答: 检查配置文件入口项并重新启动 syslogd 精灵程序。系统程序员: 如果问题仍存在，联系维修人员。

ICA8016 *文件名***的***函数名***失败 -** *错误号*

解释: 当要执行指定设备的指定功能时出错。 errno 信息是附加在错误信息上的。

用户回答: 验证指定设备存在并重试请求。如果问题仍存在，请与系统程序员联系。系统程序员: 如果问题仍存在，联系维修人员。

ICA8050 *函数* **失败。***error_text*

解释: 在执行信息中显示的功能时遇到错误。有关错误的其它信息由错误文本提供。

用户回答: 更正信息中指定的错误，如果可能，请重试操作。

ICA8051 *函数***失败: 返回码 = 0x***return_code*

解释: 在执行信息中显示的功能时遇到错误。同样也显示来自指定功能的返回码。

用户回答: 更正信息中指定的错误，如果可能，请重试操作。

ICA8052 **FWSTACKD 在为 *stack_name* 激活过滤器记录。**

解释: FWSTACKD 正在尝试激活包过滤器记录。

系统反应: 程序继续。

ICA8053 **FWSTACKD 不能为 *stack_name* 激活过滤器记录。** *error_text*

解释: 未激活包过滤器记录，原因在附随的错误信息中说明。

系统反应: 将不执行过滤器记录。

用户回答: 使用错误信息来更正错误，然后用 **fwfilter cmd=startlog** 重新激活过滤器记录。

ICA8054 **FWSTACKD 在为 *stack_name* 激活 NAT 记录。**

解释: FWSTACKD 正在尝试激活网络地址转换(NAT)记录。

系统反应: 程序继续。

ICA8055 **FWSTACKD 不能为 *stack_name* 激活 NAT 记录。** *error_text*

解释: 未能激活网络地址转换(NAT)记录，原因在附随的错误信息中说明。

系统反应: 将不执行网络地址转换记录。

用户回答: 使用错误信息来更正错误，然后用 **fwnat cmd=startlog** 重新激活网络地址转换记录。

ICA8056 **FWSTACKD 为 *stack_name* 激活 NAT。**

解释: FWSTACKD 正在尝试激活网络地址转换(NAT)。

系统反应: 程序继续。

ICA8057 **FWSTACKD 不能为 *stack_name* 激活 NAT。** *error_text*

解释: 未能激活网络地址转换(NAT)，原因在附随的错误信息中说明。

系统反应: 将不执行网络地址转换。

用户回答: 使用错误信息来更正错误，然后用 **fwnat cmd=update** 重新激活网络地址转换。

ICA8058 **FWSTACKD 为 *stack_name* 重新激活隧道定义。**

解释: FWSTACKD 正在尝试重新激活在系统停止时活动的隧道定义。

系统反应: 程序继续。

ICA8059 **FWSTACKD 不能为 *stack_name* 重新激活隧道定义。** *error_text*

解释: 未激活隧道定义，原因在附随的错误信息中说明。

系统反应: 隧道定义不能激活。

用户回答: 使用错误信息来更正错误，然后用 **fwtunnl cmd=activate** 重新激活隧道定义。

ICA8060 **FWSTACKD 为 *stack_name* 激活过滤器和 Socks 规则。**

解释: FWSTACKD 正在尝试激活包过滤器规则和 Socks 规则的当前设置。

系统反应: 程序继续。

ICA8061 **FWSTACKD 不能为 *stack_name* 激活过滤器和 Socks 规则。** *error_text*

解释: 未激活过滤器规则和 Socks 规则，原因在附随的错误信息中说明。

系统反应: 缺省过滤器规则将有效。将允许本地访问，而否定所有其它访问。

用户回答: 使用错误信息来更正错误，然后用 **fwfilter cmd=update** 重新激活过滤器和 Socks 规则。

ICA8062 **FWSTACKD 为 *stack_name* 激活 RealAudio 支持。**

解释: FWSTACKD 正在尝试激活 RealAudio 支持。

系统反应: 程序继续。

ICA8063 **FWSTACKD 不能为 *stack_name* 激活 RealAudio 支持。** *error_text*

解释: 未激活 RealAudio 支持，原因在附随的错误信息中说明。

系统反应: RealAudio 服务不可用。

用户回答: 使用错误信息来标识错误，然后用 **fwaudio cmd=change** 重新激活 RealAudio。

ICA8064 *函数* **失败。***error_text*

解释: 在执行信息中显示的功能时遇到错误。有关错误的其它信息由错误文本提供。

用户回答: 更正信息中指定的错误，如果可能，请重试操作。

ICA9000 **IBM Firewall 在** *number* **天内评估结束。**

解释: 该软件被标明为评估副本并将禁用自身。

ICA9001 **文件系统完整性检查器警告 -** *警告说明文本*

解释: fwfschk 在文件系统中找到一个差异 - 潜在的威胁。

ICA9002 **上一次信息重复 %1$d 次**

解释: 当等同的信息不以任何介入信息方式记录时，由 AIX syslogd 产生信息。在这里保存信息以便日志监视器能检测条件。该信息必须是任何写 real syslogd 信息的语言。

ICA9003 **在配置服务器上对用户** *name* **认证失败。**

解释: FW 配置服务器无法认证指定的用户。

用户回答: 请向您的 FW 管理员咨询。

ICA9004 **在配置服务器上对用户** *name* **认证成功。**

解释: FW 配置服务器认证了指定的用户。

ICA9005 **启动远程配置服务器。**

解释: 配置服务器已启动。

ICA9006 **关闭远程配置服务器。**

解释: 配置服务器正常终止。

ICA9007 **远程配置服务器无法打开信息目录。**

解释: 远程配置服务器使用的一个或多个信息目录可能丢失。

用户回答: 请向您的 FW 管理员咨询。

ICA9008 **远程配置服务器 getpeername() 失败: 出错** *errno*。

解释: 配置服务器无法得到客户的信息。

用户回答: 请向您的 FW 管理员咨询。

ICA9009 **远程配置服务器 getsockname() 失败: 出错** *errno*。

解释: 配置服务器无法得到它自身的信息。

用户回答: 请向您的 FW 管理员咨询。

ICA9010 **远程配置服务器获取适配器信息失败。**

解释: 配置服务器无法得到适配器信息。

用户回答: 请向您的 FW 管理员咨询。

ICA9011 **配置服务器无法进行远程配置。**

解释: 配置服务器在自身的配置文件中有 local=yes 设置，且客户在远程机器上。

用户回答: 请向您的 FW 管理员咨询。

ICA9012 **远程配置服务器无法读取注册请求。**

解释: 配置服务器在客户注册请求中不能读。

用户回答: 请向您的 FW 管理员咨询。

ICA9013 **远程配置服务器接收到不正确的注册请求。**

解释: 注册请求包含错误信息。

用户回答: 请向您的 FW 管理员咨询。

ICA9014 **远程配置服务器无法创建管道。**

解释: 配置服务器不能为认证创建管道。

用户回答: 请向您的 FW 管理员咨询。

ICA9015 **远程配置服务器无法创建进程。**

解释: 配置服务器不能为认证创建进程。

用户回答: 请向您的 FW 管理员咨询。

ICA9016 启动 EFM 精灵程序。

解释: 在已管理的防火墙上启动 EFM 精灵程序。

ICA9017 关闭 EFM 精灵程序; rc = *value*。

解释: EFM 精灵程序带指定返回码终止。

ICA9018 EFM 精灵程序无法打开信息目录。

解释: EFM 精灵程序使用的一个或多个信息目录可能丢失。

用户回答: 请向您的 FW 管理员咨询。

ICA9020 正在运行的用户 ID 无法交换。

解释: 无法调用系统以切换正在运行的用户 ID。

用户回答: 请向您的 FW 管理员咨询。

ICA9021 该防火墙不支持 *logon* 方式。

解释: 该防火墙不支持该特定模式。

用户回答: 请向您的 FW 管理员咨询。

ICA9022 *user* 以 *logon* 方式在防火墙上注册是不允许的。

解释: 该用户名没有授权使用该特定方式注册。

用户回答: 请向您的 FW 管理员咨询。

ICA9023 无法装入 EFM DLL。

解释: 无法装入 efm dll。

用户回答: 请向您的 FW 管理员咨询。

ICA9024 由 *user* 启动的至防火墙 *machine* 的传送请求。

解释: 启动传送操作。

ICA9025 传送请求结束，返回码为 *returncode* 。

解释: 传送操作已完成。

ICA9026 在 *time* 时，接收到来自防火墙 *machine* 的 *user* 传送请求。

解释: 传送操作在指定时间启动。

ICA9027 把函数 *function* 内的文件 *filename* 添加至传送请求。

解释: 要传送指定的文件。

ICA9028 由 *user* 启动的至防火墙 *machine* 的激活请求。

解释: 启动激活操作。

ICA9029 激活请求结束，返回码为 *returncode* 。

解释: 激活操作已完成。

ICA9030 在 *time* 时，接收到来自防火墙 *machine* 的 *user* 激活请求。

解释: 激活操作在指定时间启动。

ICA9031 关闭激活的函数 *function* ， 返回码为 *returncode* 。

解释: 完成指定函数的激活。

ICA9032 NAT 配置在 *date time* 时更新。

解释: NAT 配置已更新。

ICA9033 NAT 支持(级别 *version.release*) 在 *date time* 时初始化。

解释: 已初始化防火墙 NAT 支持。

ICA9034 NAT 支持在 *date time* 时释放。

解释: 已禁用 NAT 支持。

ICA9035 NAT 不能为安全地址 *Secured IP Address* 分配已注册的地址。

解释: 因为注册的地址池中没有可用的地址，所以不转换安全的地址。

ICA9036 **NAT 把已注册的地址 *Registered IP Address* 释放至地址池。**

解释: 释放注册的地址至已注册 IP 地址池。

ICA9037 **防火墙接口在 *time_and_date* 上自动更新。**

解释: Firewall 初始化程序已调用 **UpdateInterfaces()** 来触发 Firewall 接口文件 fwadpt.cfg 的自动更新。

系统反应: 无

用户回答: 无

ICA9038 **接口地址 *address* 已从 Firewall 配置中删除。**

解释: 列出的点十进制地址在 Firewall config 文件 fwadpt.cfg 中列出，但在 TCP 堆栈中未找到，因此被从 config 文件删除。

系统反应: 无

用户回答: 无

ICA9039 **接口 *address* 已添加至 Firewall 配置。**

解释: 列出的点十进制地址在 TCP 堆栈中找到了，但在 Firewall config 文件 fwadpt.cfg 中未找到，因此被添加至 config 文件。

系统反应: 无

用户回答: 无

ICA9040 **接口 *address* 掩码从 *oldmask* 更新到 *newmask*。**

解释: fwadpt.cfg 文件中的掩码与硬件上安装的不匹配。正确的掩码字段在 fwadpt.cfg 文件中已更新。

系统反应: 无

用户回答: 无

ICA9041 **该机器上没有找到接口。**

解释: 该机器上没有找到适配器接口。

系统反应: 无

用户回答: 无

ICA9042 **NAT 带有工作的多对一地址 *many-to-one address* 激活。**

解释: NAT 已成功初始化且现在是活动的。如果地址是 0，这暗示多对一转换的非活动的。

系统反应: 无

用户回答: 无

ICA9043 **NAT 未能带有返回码 *rc* 初始化。**

解释: NAT 未能初始化且是非活动的。

系统反应: 无 NAT 函数将被调用。

用户回答: 如果用户想要 NAT 的功能，请看返回码并通过调整来更正它。如果问题不能解决，与 IBM 服务商联系。

ICA9044 **释放 NAT。**

解释: NAT 已成功释放且现在是非活动的。

系统反应: 无

用户回答: 无

ICA9045 **NAT 分配地址: 端口*地址*: *端口*给安全地址: *安全地址*: *端口***

解释: NAT 已从地址池为安全的主机分配地址: 端口。

系统反应: 无

用户回答: 无

ICA9046 **NAT 不能为安全地址*安全地址*分配多对一地址。**

解释: NAT 已用完了带有多对一地址的端口。

系统反应: 本地主机的包已卸下。

用户回答: 这暗示有过多的未完成连接。管理员可能想通过更快地消去空闲转换表项，来减少与多对一地址有关的超时。

ICA9047 **NAT 释放地址: 端口*地址*: *端口*从安全地址: *安全地址*: *端口***

解释: NAT 返回指定的地址: 端口对到可用的池。

系统反应: 无

用户回答: 无

ICA9048 **NAT 检测带有协议的分片包**: *协议*地址: **端口***地址*: *端口* **安全地址**: **端口** *安全地址*: *端口*

解释: NAT 已检测到分段 FTP 控制包或分段的 ICMP 出错错误信息。 NAT 将转换分段的 FTP 控制包，然而不检查酬载。如果这是分段的 PORT 命令，则 FTP 数据将因为包含在信息中的 IP 地址未进行转换而失败。如果包是分段的 ICMP 错误信息，则它将被卸下。

系统反应: 请参阅说明。

用户回答: 如果重复发生，请通知 IBM 服务商。

ICA9049 **NAT 检测到从***源地址***至***目的地址***不能转换的错误段。**

解释: NAT 已检测到一个分段的数据报，它比第一个数据报段先到达。

系统反应: NAT 不能正确转换段，且该数据报被卸下。

用户回答: 如果重复发生，请通知 IBM 服务商。

ICA9050 **NAT 未能用协议**: *协议***把包从源地址**: **端口***地址*: *端口***转换至目的地址**: **端口***安全地址*: *端口*, **返回码** *rc*。

解释: NAT 未能转换一个包。

系统反应: 包被卸下。

用户回答: 如果重复发生，请通知 IBM 服务商。

ICA9051 **NAT 检测带有协议到达的分片包**: *协议***从安全地址**: **端口***安全地址*: *端口***到地址**: **端口** *地址*: *端口*

解释: NAT 已经检测到包的到达。

系统反应: 无

用户回答: 无

ICA9052 **NAT 检测带有协议离开的分片包**: *协议***从安全地址**: **端口***安全地址*: *端口***到地址**: **端口** *地址*: *端口*

解释: NAT 已经检测到包的发出。

系统反应: 无

用户回答: 无

ICA9053 **%3$d 中的** *stringValue 文件名*

解释: 调试

系统反应: 无

用户回答: 无

ICA9054 **IP 地址**: *地址***不能同时用作多对一地址和非安全/安全接口地址。**

解释: 它们不等同。

系统反应: 请求的操作不能执行。

用户回答: 选择不同的非安全/安全地址或多对一地址。

ICA9055 **NAT 检测到从***源地址***至***目的地址***能够转换的错误段。**

解释: NAT 检测到一个内部或最后的不按次序到达的数据报段。

系统反应: NAT 能够正确转换段并且不卸下数据报。

用户回答: 无

ICA9060 **致命的配置服务器初始化错误 - socket()**: *系统错误信息*

解释: 配置服务器初始化失败，精灵程序终止。

用户回答: 改正指定的系统问题并重新启动配置服务器。

ICA9061 **致命的配置服务器初始化错误 - listen()**: *系统错误信息*

解释: 配置服务器初始化失败，精灵程序终止。

用户回答: 改正指定的系统问题并重新启动配置服务器。

ICA9062 **致命的配置服务器错误 - main accept()**: *系统错误信息*

解释: 配置服务器主例程失败，精灵程序终止。

用户回答: 改正指定的系统问题并重新启动配置服务器。

ICA9063 **配置服务器出错 -** *失败函数*: **返回码 = 0x***函数返回码*

解释: 配置服务器在指定函数中检测出一个错误。精灵程序终止。

用户回答: 改正指定的系统问题并重新启动配置服务器。

ICA9064　　忽略未知选项 -*值*。

解释: 指定了指示的选项且未标识。

ICA9065　　配置服务器错误 - *失败函数*: *系统错误信息*

解释: 配置服务器在指定函数中检测出一个错误。精灵程序终止。

用户回答: 改正指定的系统问题并重新启动配置服务器。

ICA9066　　内存不足: 配置服务器: 函数 *function_name* 中 malloc(*bytes*) 返回 NULL。

解释: 无法分配足够内存 - malloc 返回 NULL。

ICA9067　　联接失败，地址: *端口*已经在使用。

解释: 提供的端口地址当前正在被使用。

系统反应: 配置服务器终止。

用户回答: 使用不同的端口地址连接至配置服务器，或与您的 Firewall 管理员联系。

ICA9068　　-*值*选项失败或未正确指定。

解释: 指示的选项失败或未正确指定。

系统反应: 配置服务器终止。

用户回答: 更正指示选项的用法并重新启动配置服务器。

ICA9069　　SSL 初始化失败。

解释: SSL 加密环境无法被初始化或与伙伴的信号交换失败。

系统反应: 配置服务器终止。

用户回答: 向 Firewall 管理员咨询以验证 SSL 环境。

附录B. Windows NT 系统配置的加固

加固是通过关闭不必要的精灵程序并禁用未授权的用户标识符来最大化安全性和效率的过程。 加固是 IBM Firewall 软件的安装的一部分并且编辑可能危及安全性的系统资源。

IBM Firewall 配置不需要的并对安全性是一个潜在的威胁的服务，被禁用。删除所有非 TCP/IP 协议。

附录C. 获得 RFC 文档

注释请求是提供新协议并建立 Internet 协议组标准的文档。 所有 RFC 的复印本可从网络信息中心（NIC）获得，也可以单独索取或订阅。您可从下列地址获得这些文档:

Government Systems, Inc.
Attn: Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

您可从下列 URL 访问 RFC:

http//www.cis.ohio-state.edu/hypertext/information/rfc.html。

需要从 NIC 获取联机副本，可通过使用 FTP 连接到 ds.internic.net。您可以通过使用下列格式传送文件:

```
RFC:RFCnnnn.TXT
RFC:RFCnnnn.PS
```

其中:

nnnn 为 RFC 号码

TXT 为文本格式

PS 为 PostScript 格式

RFC 索引的格式为:

```
RFC:RFC-INDEX.TXT
```

注: 许多 RFC 只在文本格式中有效。在请求一个 PostScript 文件之前，首先检查 RFC 索引，确认 RFC 在那种格式中有效。也可以通过发送电子邮件到 mailserv@ds.internic.net，以便从 NIC 邮件服务器请求 RFC 的联机副本。您必须在文字中包含下列命令:

```
SEND RFCnnnn.TXT
或
    SEND RFCnnnn.PS
```

其中:

nnnn 为 RFC 号码

TXT 为文本格式

PS 为 PostScript 格式

例如，需要请求 RFC 812 的文本格式，请在文字中指定:

```
SEND RFC812.TXT
```

需要请求一份 RFC 索引的副本，请在文字中包含下列命令:

```
SEND RFC-INDEX.TXT
```

附录D. IBM eNetwork Firewall Socks5.conf 配置文件格式

配置文件 **socks5.conf** 缺省定位在 IBM Firewall 安装目录中。如果希望的话，可以用文本编辑器编辑该文件。

在第一次调用服务器时读取 **socks5.conf** 配置文件。（不带停止类型 `socks5.config` 而刷新）。该文件包含所有 IBM Firewall 需要用来确定使用哪个接口到达提供地址的信息，无论是直接连接到提供的地址或使用另一个代理服务器，以及在建立代理连接时需要什么需求。

下列部分出现在配置文件中:

- 别名
- 变量
- 模块
- 认证
- 路由选择
- 代理
- 存取控制

在认证，路由选择，代理和存取控制部分中，按次序读取行直到与该部分相匹配: 行的次序非常重要。行要匹配，行中的每个项都要匹配。

指定端口

端口可以使用名称，号码或范围来指定。范围从 [或（ 开始，到 ）或] 结束，这取决于范围是否包括头尾。在范围中，定界符应该是两个端口指示符（名称或号码），由逗号分开。指定端口的方法请参考*port pattern*。

指定主机

经常需要主机地址和网络屏蔽指定哪个主机适用于提供的规则。该指定主机的方法请作为主机模式参考。几个指定主机/屏蔽对的方法:

参数	说明
hostIP/ mask	“与”上掩码的主机地址必须与“与”上掩码的主机 IP 相同。这通常用来把地址的主机部分从网络或子网部分屏蔽。
-	匹配的。允许所有主机。
n1	等于 n1.0.0.0/255.0.0.0。
n1.n2	等于 n1.n2.0.0/255.255.0.0。
n1.n2.n3	等于 n1.n2.n3.0/255.255.255.0。
.domain.name	主机名必须以字符串 *.domain.name* 结束。
a.host.name	主机名必须与 *a.host.name* 完全匹配。

同样也支持旧的主机模式语法，如下所述。然而，推荐使用更新的方法且更容易读。

参数	说明
hostIP/a	匹配的（与″-″相同）。允许所有主机。
hostIP/n	网络匹配。屏蔽地址的主机和子网部分，仅留网络部分。使用的屏蔽取决于主机 IP 地址的级别。
hostIP/s	子网匹配。屏蔽地址的主机部分，仅留子网和网络部分。使用的屏蔽取决于主机 IP 地址的级别。
hostIP/h	主机匹配。等于主机 IP。

指定认证方法

所装运的认证方法是 *ibmcram* 和 *ibmpwd*。也可能添加其它的。

认证方法可以由逗号分开的方法列表来指定。要匹配某一行，选择的认证方法必须由列表中的方法之一来代表。语法作为认证模式参考。缺省定义为认证方法 NULL。其它方法可能通过加载适当的模块来包括。 ″-″ 指示任何可接受的认证方法，包括 NULL。

认证项

认证项指示可以使用的认证类型。格式是:

```
auth/ban   source-address  source-port
auth-methods
```

参数	说明
auth/ban	认证项是否特许（auth 或 ban）。
source-address	有效主机模式。
source-port	有效端口模式。
auth-methods	有效认证模式。

关键字″ban″指示不应该在该主机上尝试认证且对于指定服务器无有效使用。

如果未指定 auth/ban 行，缺省值是任何认证方法都可接受。如果连接的许可权设置为否定（缺省值），将拒绝连接直到认证适用之后。在 SOCKS5 协议中，认证在授权之前发生。必须仅基于主机来决定如何认证主机。

指定命令

命令也可以指定为以逗号定界的列表。该语法作为命令模式参考。命令定义为: 连接，联接，udp，ping 和跟踪路由。其它命令可能通过模块添加。″-″（破折号）指示任何可接受的命令。

加载模块

模块允许客户通过添加新的认证方法，命令，权限检查和内容过滤器来把功能扩展到服务器。格式是: *module stub filename options*

参数	说明
module	加载模块的标识。
stub	存取函数名的依靠模块的名称前缀。
filename	加载模块的文件名。
options	指定模式的配置信息，如果有的话。

模块可能定义其它地方使用的字段，所以最好把模块行放在最前面。例如，认证模块定义在 auth 和 permit 行中使用的认证方法。

路由选择项

在带有多个网络界面的机器上（因此是 IP 地址），希望确保某一网络界面与某一地址一起使用。这是为了通过内部机器使用内部网络界面，外部机器使用外部网络界面来防止“IP 欺骗”（网络外部的机器假装为网络内部的机器）。 SOCKS 服务器也用来确定接收 BIND 请求或发出 SENDTO 请求时网络界面的联接。如果没有项匹配，使用 INADDR_ANY 来联接，且可在任何接口上接收连接。单宿主机不需要有路由选择项: 只有拥有多个网络界面的机器才需要它们。格式是: **route** *dest-address dest-port interface-address*

参数	说明
route	指示路由选择项的关键字。
dest-address	有效主机模式。
dest-port	有效端口模式。
interface-address	网络接口卡的 IP 地址或是网络接口的名称（例如，elnk31）。

变量输入项

日志数量和类型以及资料信息可由配置文件中的某一变量和标志控制。格式是: **set** *variable value*

参数	说明
set	为本地使用设置环境变量项的关键字。
variable	有效环境变量。参考下面的 第118页的『环境变量』 以获取可用变量的列表。
value	指定的值。

环境变量

环境变量	说明
SOCKS5_BINDPORT [port]	配置 IBM Firewall 来使用指定的端口，而不是缺省的端口 1080。
SOCKS5_RECVFROMANYONE	如果启用了 UPD 支持，允许 UPD 客户从未知的发送人接收信息。
SOCKS5_USECLIENTSPORT	配置 IBM Firewall 为仅在可以联接到与客户用来发送信息的相同端口时进行代理。这在服务器把数据流向客户时（在客户发送信息到服务器之前发送信息到客户）对于代理的 UDP 连接是必需的。此用法的例子是实音频的。
SOCKS5_MAXCHILD	最大并行线程数。
SOCKS5_NOREVERSEMAP	禁用 IP 地址至主机名的映射。如果配置文件中指定了别名，将增加日志信息开销的性能。
SOCKS5_NOSERVICENAME	禁用端口号码至服务器名的映射。如果配置文件中指定了别名，将增加日志信息开销的性能。
SOCKS5_NOIDENT	禁用 IDENT 请求，甚至是编译在其中的。这在至客户链接缓慢时非常有用，且它们不使用 IDENTD。这将减少超时周期。
SOCKS5_DEMAND_IDENT	如果没有来自客户的 IDENT 响应，配置 NULL 认证为失败。这对于保证用户名总是与连接请求相关联非常有用。

代理项

代理项说明了 SOCKS 代理服务器的地址。这些行告诉服务器如何与提供的主机联系。如果没有行与主机匹配，就直接与主机联系。格式是: *proxy-type dest-addr dest-port proxy-addr proxy-port*

参数	说明
proxy_type	代理服务器的类型。有效项为: • socks5 • socks4 • no proxy
dest-address	有效主机模式。
dest-port	有效端口模式。
proxy-address	IP 地址或是代理服务器的名称。
proxy-port	SOCKS 套接字接收连接的代理服务器端口。

存取控制项

存取控制部分确定是否允许请求建立连接。有两个类型的行，允许行和否定行。要整个行匹配，行中的每个项都必须匹配。格式是:

```
permit auth cmd src-host dest-host src-port dest-port [userlist]
deny auth cmd src-host dest-host src-port dest-port [userlist]
```

参数	说明
auth	认证方法的列表，由有效认证模式和认证项指定。
cmd	指定与该行匹配命令的有效命令。
scr-host	源主机的有效主机模式。
dest-host	目的主机的有效主机模式。
scr-port	源主机的有效端口模式。
dest-port	目的主机端口的有效端口模式。
userlist	有效用户模式。

过滤器

通过加载模块过滤由过滤器指示来执行。格式是:

```
filter  name auth cmd src-host dest-host src-port dest-port [userlist]
```

参数	说明
name	过滤器模块的标识。
auth	认证方法的列表，由有效认证模式和认证项指定。
cmd	指定与该行匹配命令的有效命令。
scr-host	源主机的有效主机模式。
dest-host	目的主机的有效主机模式。
scr-port	源主机的有效端口模式。
dest-port	目的主机端口的有效端口模式。
userlist	有效用户模式。

文献目录

要进一步了解有关 Internet 上安全性的信息，敬请光临 IBM Firewall 主页，地址为: **http://www.ics.raleigh.ibm.com/firewall**。

IBM 出版物中的信息

在此列出了关于防火墙、Internet 安全性和常规安全性主题的其它的 IBM 信息源。

防火墙主题

该文档可在 IBM Firewall 的 CD-ROM 和 IBM eNetwork Firewall 主页上获取。

- *IBM eNetwork Firewall 用户指南*, GC31-8658
- *IBM eNetwork Firewall 参考大全*, SC31-8659
- *使用 IBM eNetwork Firewall NT 版 3.2 防御黑客 (Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2)*, SG24-5209

Internet 和 World Wide Web 主题(Internet and World Wide Web Topics)

- *Internet 连接服务器指南（A Guide to the Internet Connection Servers ）*, SG24-4805
- *从 WWW 访问 CICS 商业应用程序（Accessing CICS Business Applications from the World Wide Web）*, SG24-4547
- *从 Internet 访问 OS/390 OpenEdition MVS（Accessing OS/390 OpenEdition MVS from the Internet）*, SG24-4721
- *访问 Internet（Accessing the Internet）*, SG24-2597
- *建立 Internet 的基础设施（Building the Infrastructure for the Internet）*, SG24-4824
- *有关 AS/400 和 Internet 的热门主题（Cool Title about the AS/400 and Internet）*, SG24-4815
- *Domino 防御: Lotus Notes 和 Internet 中的安全性（The Domino Defense: Security in Lotus Notes and the Internet）*, SG24-4848
- *在 WWW 上使用 MQSeries 的范例（Examples of Using MQSeries on WWW）*, SG24-4882
- *如何确保 Internet 连接服务器 MVS/ESA 版的安全（How to Secure the Internet Connection Server for MVS/ESA）*, SG24-4803
- *AIX 系统上的 Lotus Domino 服务器发行版 4.5: 安装、定制和管理（Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration）*, SG24-4694
- *Netscape 代理服务器（Netscape Proxy Server）*, SK2T-7444
- *经 Web 运行 CICS 事务处理: 至 VSE/ESA 的 CICS Internet 网关（Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA）*, SG24-4799
- *安全冲浪: 如何创建一个安全的 WWW 连接（Safe Surfing: How to Build a Secure World Wide Web Connection）*, SG24-4564
- *用 PERL 进行 CGI 程序设计自学七日通（Teach Yourself CGI Programming with PERL in a Week）*, SR23-7343
- *使用信息高速公路（Using the Information Super Highway）*, GG24-2499
- *World Wide Web 至 DB2 的访问（World Wide Web Access to DB2）*, SG24-4716

常规安全性主题

- *IP 网络设计基础（The Basics of IP Network Design）*, SG24-2580
- *安全性要素: AIX V4.1 （Elements of Security: AIX V4.1）*, GG24-4433
- *企业范围安全体系结构及解决方案演示指南（Enterprise-Wide Security Architecture and Solutions Presentation Guide）*, SG24-4579
- *HACMP/6000 定制范例（HACMP/6000 Customization Examples）*, SG24-4498
- *IBM 全球网（IGN）安全性策略（IBM Global Network （IGN） Security Policy）*, GC34-2206
- *IBM 安全性体系结构: 确保开放客户机/服务器分布式企业（IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise）*, SC24-8135
- *IBM 系统监视器: 智能代理的结构（IBM Systems Monitor: Anatomy of a Smart Agent）*, SG24-4398

- *开放系统连网的安全性概述（Security Overview of Open Systems Networking）*, GG24-3815
- *系统监视器 AIX 版用户指南（Systems Monitor for AIX User's Guide）*, SC31-8173
- *TCP/IP 教程和技术概述（TCP/IP Tutorial and Technical Overview）*, GG24-3376

业界出版物中的信息

这些工业出版物适用于 sendmail, TCP/IP 和 UNIX:

- Albitz, Paul, and Cricket Liu. *DNS 和 BIND（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 网络管理（TCP/IP Network Administration）* O'Reilly and Associates, Inc. （ISBN: 0-937175-82-X）
- Nemeth, Snyder, et al. *UNIX 系统管理手册（UNIX System Administration Handbook）* Prentice Hall. （ISBN: 0-13-151051-7

以下出版物都涉及到了防火墙和 Internet 上的安全性:

- Ahuja, Vijay. *网络和 Internet 安全性（Network and Internet Security）*. Boston: Academic Press Professional, 1996. （ISBN: 0120455951）
- Ahuja, Vijay. *Internet 上的安全贸易（Secure Commerce on the Internet）*. Boston: Academic Press Professional, 1997. （ISBN: 0120455978）
- Anderson, Bart, et al. *怀特组的 UNIX 通信和 Internet（The Waite Group's UNIX Communications and the Internet）*。 Indianapolis, IN: Sams Pub., 1995. （ISBN: 0672305372）
- Atkins, Derek, et al. *Internet 安全性: 专业人员参考大全（Internet Security: Professional Reference）*. Indianapolis, IN: New Riders Publishing, 1996. （ISBN: 1562055577）
- Chapman, D. Brent, and Elizabeth D. Zwicky. *建立 Internet 防火墙（Building Internet Firewalls）*. Sebastopol, CA: O'Reilly and Associates, 1995. （ISBN: 1565921240）
- Cheswick, Willam R., and Steven M. Bellovin. *防火墙和 Internet 安全性（Firewalls and Internet Security）*. New York: Addison-Wesley, 1994. （ISBN: 0201633574）
- Cooper, Frederic J., et al. *实现 Internet 安全性（Implementing Internet Security）*. Indianapolis, IN: New Riders Publishing, 1995. （ISBN: 1562054716）
- Curry, David. *UNIX 系统安全性: 用户和系统管理员指南（UNIX System Security: Guide for Users and Systems Administrators）*。 Sebastopol, CA: O'Reilly and Associates, 1994. （ISBN: 0201563274）
- Garfinkel, Simson, and Gene Spafford. *UNIX 安全性实用大全（Practical UNIX Security）*. Sebastopol, CA: O'Reilly and Associates, 1991. （ISBN: 0937175722）
- Garfinkel, Simson, and Gene Spafford. *UNIX 和 Internet 安全性实用大全（Practical UNIX and Internet Security）*. Sebastopol, CA: O'Reilly and Associates, 1996. （ISBN: 1565921488）
- Hare, Chris, and Karanjit Siyan. *Internet 防火墙和网络安全性（Internet Firewalls and Network Security）*. Indianapolis, IN: New Riders Publishing, 1996. （ISBN: 1562056328）
- Randall, Neil. *自学 Internet 七日通（Teach Yourself the Internet in a Week）*. Indianapolis, IN: Sams.Net, 1995. （ISBN: 0672307359）
- Stallings, William. *Internet 安全性手册（Internet Security Handbook）*. Foster City, CA: IDG Books, 1995. （ISBN: 0077092546）
- Stevens, W. Richard. *TCP/IP 图解（TCP/IP Illustrated）*. Reading, MA: Addison-Wesley, 1994. （ISBN: 0201634953）

注意事项

本出版物中所提及的 IBM 产品、程序或服务并不意味着 IBM 将在所有有 IBM 业务的国家中提供。任何对 IBM 产品、程序或服务的引用并不说明或暗示只能使用 IBM 产品、程序或服务。任何不触犯 IBM 知识产权且有同等功能的产品、程序或服务都可以用来代替 IBM 产品、程序或服务。在与其它产品结合使用时，除了由 IBM 明确指定的产品之外，其评估和验证均由用户自行负责。

IBM 可能已经申请或正在申请与本文档有关的各项专利权。提供本文档并不表示允许您使用这些专利。您可以用书面方式将特许查询寄往:

IBM Director of Licensing

IBM Corporation

500 Columbus Avenue

Thornwood, NY 10594

USA

为了以下目的: （i）允许在独立创建的程序和其它程序（包括本程序）之间进行信息交换（ii）允许对已经交换的信息进行相互使用，而希望获取本程序有关信息的合法用户请与下列地址联系:

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
USA

依照适当的条款和条件，其中包括在一些情况下需要付费，这些信息或许是可用的。

本文档中说明的特许程序和所有可用的特许资料是由 IBM 按照 IBM 客户协议条款提供的。

本文档不打算供生产使用，对本文档的供给也不作任何形式的担保，因此我们拒绝一切保证，包括可销售性和对一个特定用途的适用性。

本产品包含了由加利福尼亚大学伯克立分院及其赞助商共同开发的软件。

商标

下列术语是 IBM 公司在美国或其它国家或两者的商标:

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

Microsoft、Windows、Windows NT 和 Windows 95 徽标是 Microsoft 公司的商标或注册商标。

UNIX 是 X/Open 有限公司特许专用的在美国和其它国家的注册商标。

Java 和 HotJava 是 Sun 微系统公司的商标。

其它公司、产品和服务名，可能会以双星号（**）标识，是其它公司的商标或服务标志。

词汇表

您可访问位于
http://www.networking.ibm.com/nsg/nsgmain.htm
的 IBM 软件词汇表。

索引

本索引按汉语拼音，数字，英文字母和特殊字符顺序排列。

[Z]

A

D

F

H

I

M

N

P

R

S

T

U

W

读者意见表

IBM eNetwork Firewall Windows NT 版
参考大全
版本 3 发行版 2.1.1

SA31-1911-01

姓名

地址

单位及部门

电话号码

读者意见表

SA31-1911-01

请沿此线
撕下或折起

折起并封口　　请勿使用钉书机　　折起并封口

在此
贴上
邮票

IBM Corporation
Information Development
Department CGMD / Bldg 500
P.O. Box 12195
Research Triangle Park, NC
27709-9990

折起并封口　　请勿使用钉书机　　折起并封口

SA31-1911-01

请沿此线
撕下或折起

Printed in China

SA31-1911-01