IBM eNetwork Firewall Windows NT 版

用户指南

版本 3 发行版 2.1.1

GA31-1909-01

IBM eNetwork Firewall Windows NT 版

用户指南

版本 3 发行版 2.1.1

GA31-1909-01

注

在使用该信息及其所支持的产品之前，请阅读第111页的『附录. 注意事项』中的信息。

第二版（1998 年 6 月）

本版本适用于 IBM eNetwork Firewall Windows NT 版版本 3 发行版 2.1.1（产品号 5765-C16）。本版本取代 GA31-1909-00。

目录

关于本书

本书描述如何配置和管理 Windows NT** 系统上的 IBM eNetwork Firewall，从而可防止不需要或未授权的通信出入您的安全网络。

本书是针对安装、管理和使用 IBM Firewall 的网络或系统安全性管理员的。虽然我们描述如何用客户程序访问防火墙，但这并不是一本有关客户程序的用户指南。要使用如 telnet 或 FTP 等客户程序，请查看有关 TCP/IP 客户程序的用户指南。

在使用本书之前，请使用附在 CD-ROM 包装上的安装指令来安装该产品。

在启动配置客户程序后，联机帮助信息将帮您填写配置客户程序字段以及在一个个对话框间移动。

必备知识

在安装和配置 IBM Firewall 之前，具备一定的 TCP/IP 寻址、掩码和网络管理知识是非常重要的。因为将设置和配置一个可对出入您网络的访问进行控制的防火墙，所以首先您必须理解网络是如何操作的。特别是您需要理解基本的 IP 地址、全限定名和子网掩码。

涉及 netstat、arp、ifconfig、ping、nslookup、DNS、sendmail、路由选择及其他有关 TCP/IP 的一本好书是 *TCP/IP 网络管理(TCP/IP Network Administration)*。请参阅*书目*以获得更多细节。

用于执行 UNIX 管理，同时给出了 TCP/IP 和路由选择、网络硬件、DNS 和 sendmail 等的较好概述的一本非常有用的书籍是 *UNIX 系统管理手册*。请参阅书目以获得更多细节。

本发行版的特性

IBM eNetwork Firewall Windows NT 版提供种类繁多的特性，并包括所有三种体系结构:

1. 应用程序代理
   - FTP
   - HTTP，(包括 Gopher 和 WAIS)
   - Telnet
   - SafeMail

   HTTP、 Telnet 和 FTP 有认证能力。
2. 通过 Socks 协议 版本 5 (一种 Internet 标准) 的电路级网关
3. 过滤 -- 一套全面且健全的标准，可允许或拒绝通信。标准包括 TCP/IP 地址、端口、协议、方向和适配器 (安全/非安全) 等等。

   许多预先定义的服务使设置更快速。

Socks 协议版本 5

除了简单和灵活性，Socks 协议 5 还提供下列优点:

- 易于部署的认证和加密方法
- UDP 关联，是为跨越基于 UDP 的代理电路创建一条虚拟代理电路。
- Socks V5 监视器，显示实时 socks 性能信息

网络地址转换

随着 Internet 的迅速发展，IP 地址的枯竭问题显得非常重要。基于地址重用，网络地址转换（NAT）为 IP 地址枯竭的问题提供了一种解决方案。

NAT 的优点是: 它透明地允许使用专用或非法地址的网络与 Internet 上的主机通信，实际上允许专用网络拥有更大的地址空间。另外，通过使用 NAT，将专用网络中的地址对外部世界隐藏起来，提供了另一层安全性级别。

简单的管理

通过使用可从远程机器管理的 Java** 应用程序，可简便地更新防火墙配置。而且，还可为不同的管理员指定不同级别的权限以进一步控制对防火墙的访问。这种单一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

安装了防火墙，则禁用非 TCP/IP 协议、多余的系统服务以及自非管理员帐户的本地登录。

强大的认证

支持所有受欢迎的基于令牌的认证机制，如所提供的 SecurID、SecureNet Key 等等。

报告实用程序

一旦将系统日志导出到某一数据库引擎中，报告实用程序就允许您对其运行 SQL 查询。

报警、监视和记录

全面而详细的记录包括所有与 TCP/IP 地址、用户标识符、TOD、文件名、端口号等有关的防火墙活动。日志监视器包括监视可疑活动并在超出阈值时警告您。

隔离多个网络

通过在防火墙中使用多个网络界面卡 (NIC)，您可隔离多个子网。

国家语言支持

所提供的国家语言支持是英语、日语、韩语、法语、简体中文、繁体中文、意大利语、西班牙语和巴西葡萄牙语。

输入 IP 地址

当配置防火墙时，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，带所有 4 个八位位组:

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

这里每个 nnn 是 000-255 范围内的一组三位数字。

如何呼叫 IBM 服务

IBM 支持中心为您提供问题的诊断与解决方面的电话辅助。您可在任何时间致电 IBM 支持中心; 在八小时工作时间内您将收到回电（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，请联系当地的 IBM 代理或 IBM 授权供应商。

第1章 介绍 IBM Firewall

IBM eNetwork Firewall 是一种用于 AIX 和 Windows NT** 的网络安全程序。 简单而言，防火墙是在一个或一个以上安全的内部专用网络和另一个（非安全的）网络或 Internet 之间的封琐线。其目的是防止无意或未授权的通信进出安全网络。防火墙有三项功能:

- 实施 Internet 安全性策略
- 让自己网络中的用户使用来自外部网络授权的资源而不泄露自己网络的数据和其它资源
- 将未授权的用户阻拦于网络之外

防火墙概念

Internet 的任意连通性带来了许多安全性风险。必需保护自身的专用数据，同时还要保护专用网络内部的机器免受外部的滥用。为实现这个保护目标，首先，要限制专用网络连接到 Internet 的站点数。只用一个网关将专用网络连接到 Internet 的配置无疑使您拥有了对进出 Internet 通信量的控制。我们称这种网关为防火墙。

要了解防火墙是如何工作的，请参考这个例子。想象有一栋大楼，想要限制对它的访问并控制进入的人员。该大楼的一个大厅是其唯一的入口点。在这个大厅内，由前台服务员接待进入的来宾，保安人员会对他们进行监视，且通过摄像机拍下他们的一举一动，并用胸卡阅读器来认证他们的身份。

这对于控制进入一个专用大楼非常有效。只是如果一个不速之客成功地通过了大厅，那么以后他对大楼所做的一切破坏我们都将束手无策。但是，如果监视了这个人的行踪，就可能侦察出任何可疑行为。

当定义防火墙策略时，可能认为它足以阻止任何目前对组织所构成的危险，而为其余那些潜在的危险敞开大门。但是，由于新的攻击方法层出不穷，则需要预料如何去阻止这些攻击，正如在大楼案例里，您必须监视任何防御已泄露的信号。一般来说，亡羊补牢所造成的损失和花费比防御在先要大得多。

IBM Firewall 工具

IBM Firewall 是用来实现不同防火墙体系结构的工具箱。一旦选定了体系结构和安全性策略，就应选择必需的 IBM Firewall 工具。 IBM Firewall 配置客户程序为管理提供了友好的图形用户界面。IBM Firewall 提供了所有重要事件的综合记录，例如管理更改和对安全性进行破坏的尝试。

因为 IBM Firewall 本质上是一个 IP 网关，它将世界分隔成两个或更多网络: 一个或多个非安全网络和安全网络。例如 Internet 就是非安全网络。安全网络通常为公司的 IP 网络。IBM Firewall 提供的一些工具为:

- 专家过滤器
- 代理服务器
- Socks 服务器
- 特定的服务，如域名服务（DNS）和 SafeMail

专家过滤器

专家过滤器是在会话层检查包的工具，它以多个标准为根据（如一天的时间、IP 地址和子网）。 过滤器与 IP 网关功能一起使用，所以要求机器必需有两个以上网络接口，每个接口都位于一个单独的 IP 网络或子网中。一组接口说明为非安全的，其它都为安全的。过滤器在这两组接口之间起的作用如第2页的图 1 中所示。

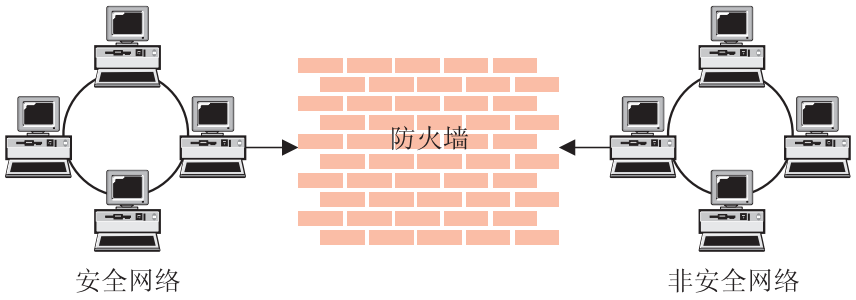

图 1. 使用专家过滤的防火墙

专家过滤器的目标

专家过滤为防火墙提供了基本保护机制。过滤器允许根据 IP 会话的细节来决定防火墙上通过哪些通信，故保护了安全网络免于受到外部的威胁，例如扫描安全服务器或 IP 地址欺骗。将过滤器设施看作构成其它工具的基础。

代理服务器

代理服务器与过滤有所不同，过滤仅观察通过的包，而代理服务器是防火墙的一部分并以用户身份执行特定的 TCP/IP 功能的应用程序。用户与使用一种 TCP/IP 应用程序 (Telnet 或 FTP)的代理服务器联系。代理服务器以用户的身份与远程主机联系，因此，当对外部用户隐藏起网络时，能够控制访问。 第2页的图 2 描述了一个代理 Telnet 服务器从外部用户截取请求。

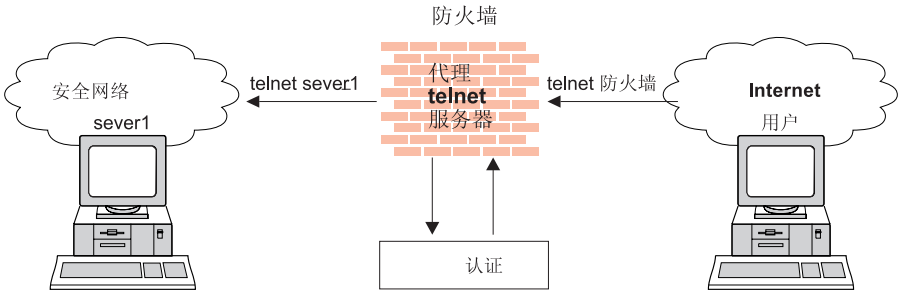

图 2. 使用代理服务器的防火墙

可用的代理服务有 FTP、HTTP、WAIS、GOPHER、HTTPS 和 SafeMail。

IBM Firewall 代理服务器能够使用多种认证方法来认证用户。用户能够访问 Internet 上有用的信息，而无须以泄露内部网络的安全性为代价。

代理服务器的作用

当通过一个代理服务器来连接时，TCP/IP 连接在防火墙上断开，故泄露安全网络的潜在危机减少了。可能要求用户使用众多认证方法中的一种来作自我认证。

代理服务器的一项主要优点是地址隐藏。所有出栈代理连接都使用防火墙地址。另一项代理服务器的主要优点是安全性。 IBM 专家已经开发了这些代理服务器，以保护客户机上可能存在的安全性问题。

代理服务器的一个主要优点是在客户机上不需要特殊版本的客户程序。所以，一旦安装了防火墙，则不用任何附加的软件安装，Firewall 中每个用户都对非安全网络有访问权。

Socks 服务器

Socks 是一种电路层网关标准，它不需要更常规的代理服务器系统开销就能提供地址隐藏。

Socks 服务器与代理服务器相似，会话都在防火墙中断。不同之处是 socks 能支持所有应用程序，而无需为每个应用程序要求一个唯一代理。明显地，socks 客户使用 IBM Firewall 主机上的 Windows NT socks 服务来启动会话，然后验证源地址和用户 ID 是否被允许建立向前连接入非安全网络，再创建第二个会话。第3页的图 3描述了一个带有 socks 服务器的防火墙。

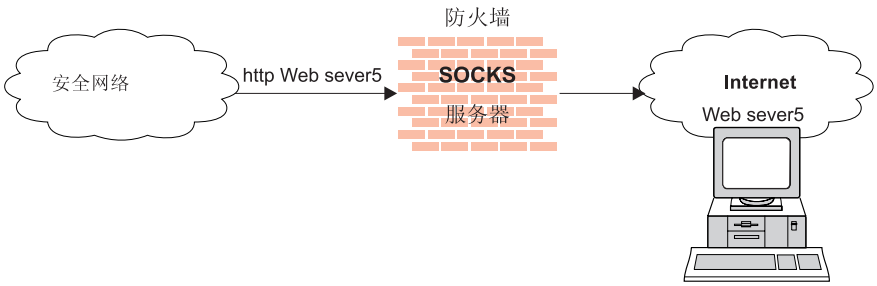

图 3. 使用 Socks 服务器的防火墙

Socks 化的客户程序(使用 Socks 的客户程序) 在许多应用程序中可用，如 Netscape Navigator**、Microsoft** Internet Explorer，或通过 TCP/IP 软件(如 Aventail** AutoSocks**)。

Socks 服务器的作用

对于出站会话（从安全客户到非安全服务器），socks 服务器与代理服务器有相同的作用，就是将会话在防火墙处断开，并提供了用户必须证实他们的身份才能通过的一道安全门。 其一大优势是简化了用户的工作，但并不增加太多额外的管理性工作。

域名服务

访问安全网络的域名记录对于入侵者来说是非常有帮助的，因为这将为他们提供了一个要进行攻击的主机列表。一个遭破坏的域名服务服务器也能够为入侵者提供访问的路径。从外部网络角度来看，防火墙上的命名服务器仅知道自己本身，而从不会给出

内部 IP 网络的信息。从内部网络的角度来看，该名称服务器知道 Internet 网络，并且通过它的名称来访问 Internet 上的所有机器是非常有用的。

DNS 服务器的作用

在防火墙上运行 DNS 服务器有双重优点，其一是能防止名称解析请求流经防火墙，其二将安全网络的主机对非安全世界隐藏起来。

SafeMail

邮件是一个访问 Internet 最主要的原因之一。 SafeMail 是设计为隐藏内部网络域名的 IBM 邮件网关。 SafeMail 功能不在网关上存储邮件或在 root 用户 ID 下运行。在外出邮件中用防火墙网关公用域名替代专用域名，这样邮件看上去就象是从防火墙地址来的，而不是用户地址。 SafeMail 支持简单邮件传送协议（Simple Mail Transfer Protocol（SMTP）） 和多用途 Internet 邮件扩展（Multipurpose Internet Mail Extensions（MIME））。

使用网络安全性审计器

网络安全性审计器扫描网络中的安全性漏洞或配置错误。网络安全性审计器可扫描您的服务器和防火墙中的一系列问题和弱点，例如开放端口和其它曝光，并且编制一个列表以便改正。网络安全性审计器可用作关键主机的定期扫描器或一次性信息收集工具。网络安全性审计器的管理是通过易用命令行界面来完成的。有了网络安全性审计器，您可在防火墙上保持警戒性。

网络安全性审计器的功能包括:

- 扫描 TCP 和 UDP 端口
- 识别非标准端口上的服务器
- 报告危险服务、已知弱点、过时的服务器版本，以及违反了定制的站点策略的服务器或服务。
- 生成 HTML 格式的报告以方便浏览

第2章 规划

在配置 IBM 防火墙以前，先使用校验表和规划工作单以帮助您了解网络配置。

规划校验表

1. 定义您的目标。想要:
   - 访问 Internet（telnet，匿名 FTP 等）吗?
   - 划分内部网络的各部分吗?
   - 为网络提供*外部*访问吗?
2. 评估 IP 子网层次上的网络的拓扑结构。
   - 一个安全和一个非安全接口是一个正确的配置吗?
   - 您的地址能支持规则中的子网掩码吗?
3. 决定如何使用 DNS。 请参阅第27页的『第6章 处理域名服务』。
4. 决定如何使用 safemail。请参阅第35页的『第7章 SafeMail』。
5. 如果要使用 Socks，则要确保安装了 Socks 化的客户程序，例如 Netscape Navigator 或 Microsoft Navigator。对于有关使用 socks 的信息，请参阅第63页的『第11章 配置 Socks 服务器』
6. 需要何种类型的认证?
   - 如果要使用 Security Dynamics** ACE/Server** 认证客户，在防火墙主机上安装 ACE/Server 客户程序代码。我们建议您在安全网络内的某些其它主机上安装 ACE/Server 服务器代码。

     对于安装和使用 Security Dynamics ACE/Server 和 SecurID** 卡的有关信息，请参阅由 Security Dynamics Technologies 公司提供的信息。
   - 如果要使用 AssureNet Pathways** SecureNet Key** 卡，请单独购买 IBM Firewall 卡。
   - 如果要使用自身的认证方式，请参阅在 *IBM eNetwork Firewall 参考*大全中“提供自身的认证方式”一章。
   - 必须配置实现用于认证目的的搜索可信 Windows NT 域，使用 TCP 替代 NETBIOS 的 Windows 客户机代码。NETBIOS 将被禁用。可信 Windows NT 服务器必须有 TCP/IP 主机名和地址，并有在它们和防火墙之间的 TCP/IP 连接。防火墙管理员需要在防火墙和可信 NT 服务器间创建连接以允许通信量在这两者间流动。

     使用下列预先定义的服务来设置该连接:

     a. 域控制器认证 - 允许用户认证的域控制器的使用

     b. NetBT 名称服务广播 - 允许 TCP/IP 上的 NetBIOS 名称服务广播

     使用 NT 配置实用程序，以定义信任关系。
7. 如果使用过滤，一开始使用简单的过滤器规则，并使它们非常有限制性。熟悉所需服务所使用的端口和协议。
8. 决定存档日志文件的方式。存档是在 Windows NT 调度程序服务中的预定作业的一个理想候选。请参阅第97页的『第15章 管理日志和档案文件』。

网络配置规划工作单

填写以下信息作为规划您的 IBM Firewall 配置的一部分。

防火墙主机名 _____

安全网络接口（连接至内部安全网络）

IP 地址 _____ 子网掩码 _____

IP 地址 _____ 子网掩码 _____

IP 地址 _____ 子网掩码 _____

IP 地址 _____ 子网掩码 _____

非安全网络接口（连接至非受托非安全网络）

IP 地址 _____ 子网掩码 _____

IP 地址 _____ 子网掩码 _____

IP 地址 _____ 子网掩码 _____

IP 地址 _____ 子网掩码 _____

路由器名称 _____

路由器地址 _____

安全域名 _____

安全域名服务器（DNS）的 IP 地址 _____

非安全域名服务器（DNS）的 IP 地址

安全邮件服务器 _____

公共域名 _____

配置客户程序的 IP 地址 _____

远程客户的 IP 地址 _____

您的 Windows NT Firewall 的根目录

(我们在整个文档中将它称为 ROOTDIR)

c:\winnt (我们假设 Windows NT 已安装在该目录中)

第3章 设置配置服务器和配置客户程序

本章论述了如何建立配置服务器和配置客户程序，（它们是 IBM Firewall 的图形用户界面（GUI））。

设置配置服务器

配置服务器是配置客户程序至 Firewall 的接口。 配置服务器处理来自配置客户程序的请求。它在 Firewall 机上运行，并可处理本地或远程机器上的配置客户程序的请求。一旦设置了它以后，可将它看作 Firewall 机器的一部分。

配置服务器的端口号在位于安装 Windows 操作系统中 `c:\winnt\system32\drivers\etc\services` 下 NT 服务文件中指定。端口号缺省为 1014，但为增加安全性，可以更改它，只需通过停止配置服务器服务，修改服务文件，然后重新启动配置服务器服务即可。

配置服务器一开始被设置为只接受本地机器上的配置客户程序的请求。初始请求没有加密。要更改这些选项，从命令行使用 `fwcfgsrv cmd=change` 。

localonly=

说明 Firewall 是否仅可以从本地的机器上进行管理。

localonly=yes

配置只能在本地机器上进行；这是缺省值。

localonly=no

配置可以在任何机器上进行。

encryption

表示配置服务器是否希望输入的数据通过安全套接字层（ssl）加密。

如果更改加密选项或 sslfile，则必须停止和重新启动配置服务器服务。

encryption=none

无加密；这是缺省值。

encryption=ssl

采用 SSL 加密。

sslfile=

表示 SSL 加密使用的 SSL 密钥文件的名称；系统设定值是 `ROOTDIR\config\fwkey.kyr`。 *ROOTDIR* 是安装进程中选定为目标的 IBM Firewall 的目录。要得到如何创建关键文件的详细信息，请参阅 *IBM eNetwork Firewall 参考大全*。

如果配置客户程序不能连接到 Firewall 机器，并且它在不同的机器上，则使用 `fwcfgsrv cmd=list` 来检查是否设置了 `localonly=no` 。同样，客户程序和服务器所使用的语言必须匹配。最后，通过打开服务面板并检查它的状态来确保配置服务器服务正在运行。要做到这点，转至控制面板，双击“服务”图标来检查每个服务的状态。如果没有运行，则应该重新启动服务。

设置配置客户程序（GUI）

在安装 IBM Firewall 时，会自动安装配置客户程序。配置客户程序也可以单独安装在任何不带 Firewall 的 Windows NT 机器上。 要启动配置客户程序应用程序，双击 IBM Firewall 程序组中的“配置客户程序”图标。当配置客户程序启动时，必须首先使用 Windows NT 管理员帐户注册到 Firewall 上。

只有 Windows NT 管理员和防火墙管理员（有适当的管理认证）才可以使用配置客户程序注册到 Firewall 上。

在安装了 Firewall 后，指定所有 Windows NT 管理员为主防火墙管理员。通过主防火墙管理员，使用配置客户程序注册到配置服务器上，同时定义附加的防火墙管理员用户名，（如果必要的话）。请参阅第69页的『第12章 管理防火墙上的用户』以获得有关如何使用配置客户程序来定义防火墙管理员的信息。

要设置较快或较慢机器的注册超时值，通过单击 IBM Firewall 配置客户程序图标，然后单击属性 做下列更改。使用**快捷方式**标签来修改属性。更改参数超时为*20*，这里 20 等于等待连接产生所用的秒数。较快的机器可以设置为 10，较慢的机器应当接受缺省值。

要增加 JAVA 控制台中调试信息的级别，运行 `ROOTDIR\cfgcli\gui` 中的 `ibmfw.bat` 代替使用配置客户程序图标。不过注意，启用控制台记录可能会降低性能。

注册到配置客户程序上

要注册到配置客户程序上（在本地或远程机器上）：

- 用户必须是防火墙管理员
- 防火墙管理员必须具有已经定义的一种认证方案。请参阅第74页的『用户认证方法』。
- 用户必须有执行特定配置功能的权限

通过配置客户程序启用远程配置

要通过配置客户程序启用远程配置，请确保要注册的管理员在 Firewall 机器上定义了下列属性:

- 如果管理员在网络的安全端并使用 Firewall 机器上的安全接口，则必须用适当的认证方法对他或她进行定义以进行安全管理。（不能设置为拒绝全部）。这也适用于从本地注册到 Firewall 上。
- 类似地，如果管理员处于非安全端并使用 Firewall 机器的非安全接口，就必须用适当的认证方法对他或她进行定义以进行非安全管理。（不能设置为拒绝全部）。

所有的用户属性都可以通过配置客户程序中的“修改用户对话框”或使用命令 `fwuser` 来设置。在安装了防火墙以后，所有的防火墙管理员将对所有上述字段进行适当的设置。请参考第69页的『第12章 管理防火墙上的用户』获得更多信息。

远程配置服务器的样本日志输出

以下为远程配置服务器的日志输出的一个样本:

```
Feb 03 13:52:15 1998 mr16n18: ICA9005i: Starting remote configuration server.

Feb 03 13:52:21 1998 mr16n18: ICA2024i: User administrator successfully
authenticated using NT authentication from secure network:127.0.0.
Feb 03 13:52:21 1998 mr16n18: ICA2169i: User administrator successfully
authenticated for Remote Administration Server using NT from secure network:127.0.0.1.
```

第4章 使用配置客户程序

使用配置客户程序，即一个图形用户界面来配置和管理 IBM Firewall。

当您第一次安装 IBM Firewall 时，它最初仅能接受来自本地机器上配置客户程序的请求。但是，您可以在另外一台机器上安装配置客户程序，远程地管理防火墙。欲知如何做到这些，请参阅第9页的『设置配置服务器』。

要设置配置客户程序以您特定的 本地环境语言启动，则单击“IBM Firewall 配置客户”图标，然后单击**属性**。使用**快捷方式**标签来修改属性。缺省情况下，使用主机的本地环境。 IBM Firewall 将支持这些场所:

- en_US - 美式英语
- ja_JP - 日语 PC
- ko_KR - 韩国语
- zh_CN - 简体中文 EUC
- zh_TW - 繁体中文(Big 5)
- fr_FR - 法语
- it_IT - 意大利语
- pt_BR - 巴西葡萄牙语
- es_ES - 西班牙语 PC

使用配置客户程序需要鼠标。

帮助按钮位于配置客户程序主面板靠近顶部的地方。单击**帮助**可获得关于任何功能的信息。

如何注册到配置客户程序上

1. 关于注册类型，如果与防火墙在同一台机器上，则选择“本地”。“本地”是缺省值。如果要以远程方式访问另一个防火墙，请选择“远程”。“远程”需要您输入一个主机名。
2. 如果选择了“远程”注册，就得输入您要注册到的防火墙机器的主机名或 IP 地址。
3. 选择“SSL”还是“无”将取决于防火墙使用了何种加密方式。对于客户程序，“本地”的缺省设置是“无”，“远程”的缺省设置是“SSL”。
4. 输入防火墙管理员或 NT 管理员的用户名。
5. 输入服务器所侦听的端口号。缺省值是 1014。
6. 关于方式，如果想要配置一台您正在注册的 Windows NT 防火墙机器，则选择“主机”。运用主机管理方式，管理员就可以在同一时刻以本地或远程方式更新一个防火墙。对于 AIX 防火墙管理的企业防火墙管理（EFM）选择企业。
7. 注册后可以看到认证信息，还可能会提示您输入口令（如果口令是为用户名而设置的认证方式的话）。如果提示您输入口令，请在“用户响应”字段中输入口令，然后按 Enter 键或单击“提交”。如果输入的口令不正确，会得到一条信息。单击“关闭”，然后重新启动注册进程。如果没有提示您输入口令，那么您的用户认证方式可能是允许全部。在这种情况下，将立即获得 IBM Firewall 配置客户面板。
8. 在认证成功后，将看到主配置面板。

图 4. 配置客户程序注册面板

浏览树

配置客户程序的左侧有一个可伸缩的树状导航辅助，如第15页的图 5中所示。

如果在一个节点或功能下有项目，则在节点的左侧会出现文件的文件夹图标。要查看子功能，可以通过双击图标来展开视图。再次双击该图标，该节点的视图就会收缩回原来的视图。

所单击的任何功能都被认为是选中的并突出显示。可以展开或收缩节点而不对右侧的窗口视图做任何更改。当展开的树超过了可用的垂直空间，就会在浏览树的右侧出现一个滚动栏。如果有任何一个功能名超过浏览树的边界，就会出现一个水平滚动栏。

图 5. 配置客户程序浏览树

主面板上的常规特性

在**报警显示**上，您将看到下列三个按钮，如第15页的图 5 所示。

帮助 **帮助**按钮位于配置客户程序主面板靠近顶部的地方。单击**帮助**以查看如何设置与运行 IBM Firewall 的信息。

用户指南

用户指南按钮位于靠近配置客户程序主面板顶部的地方。单击**用户指南** 以查看这个软拷贝出版物。

参考大全

参考大全按钮位于靠近配置客户程序主面板顶部的地方。单击**参考大全**以查看软拷贝出版物。

在主面板上将会看到的其它按钮有:

最新 **最新**按钮位于配置客户程序主面板靠近底部的地方。单击**最新**以查看最近的报警。

注销/注册

注销/注册按钮位于配置客户程序的右上角。这是一个重新连接按钮。为与另一个防火墙连接或注册为另一个管理员，您可重新启动注册序列。

要注销，单击“注销”，单击注册面板上的“取消”，然后关闭应用程序。

日志查看器

日志查看器按钮位于配置客户程序的右下角。该按钮允许您浏览防火墙日志。

上一个 **上一个**按钮位于配置客户程序主面板的底部。单击**上一个**以查看较早的警报。

报警显示

可以查看在主配置客户程序窗口右下方的系统日志监视器生成的报警记录，如 第16页的图 6中所示。

显示的报警记录是从第一个报警日志设施标识的文件中获得的，该设施定义在 ROOTDIR\config\syslog.conf 中。 如果没有定义报警日志设施，则会看到一个空白显示。请参阅第97页的『添加日志设施』获得有关定义报警日志设施的帮助。

面板显示了报警文件的名称和当前文件显示的行号。可以单击**最新**查看最近的警报。单击**上一个**可以让您查看较早的警报。

显示的每一行都有警报的日期和时间、发生警报的防火墙主机名、警报信息标记以及警报信息的正文。标记是警报类型的表示。

图 6. 警报显示

日志查看器

单击**日志查看器**可以显示一个日志查看器窗口，如第17页的图 7中所示。 日志查看器允许查看防火墙日志记录。可以指定一个日志文件以及一个记录数（缺省为 25）。

显示的报警记录是从第一个报警日志设施标识的文件中获得的，该设施定义在 ROOTDIR\config\syslog.conf 中。 可以从文件名字段的下拉菜单中选择另一个目标日志文件，也可以输入要查看文件的名称。

要请求一个特定启动行，请单击**开始行:** 。要请求最后的行,请单击**底部**，将您带到文件的底部。**下一行**将您带到文件的下一行。**上一行**将您带回文件的上一行。**顶部**将您带到文件的顶部。单击**是**，可任意将防火墙日志展开为可读文本。

请参阅第97页的『使用配置客户程序来创建并存档日志文件』和第89页的『第14章 监视防火墙记录』以获得关于日志文件、设施、监视和报警的更多信息。

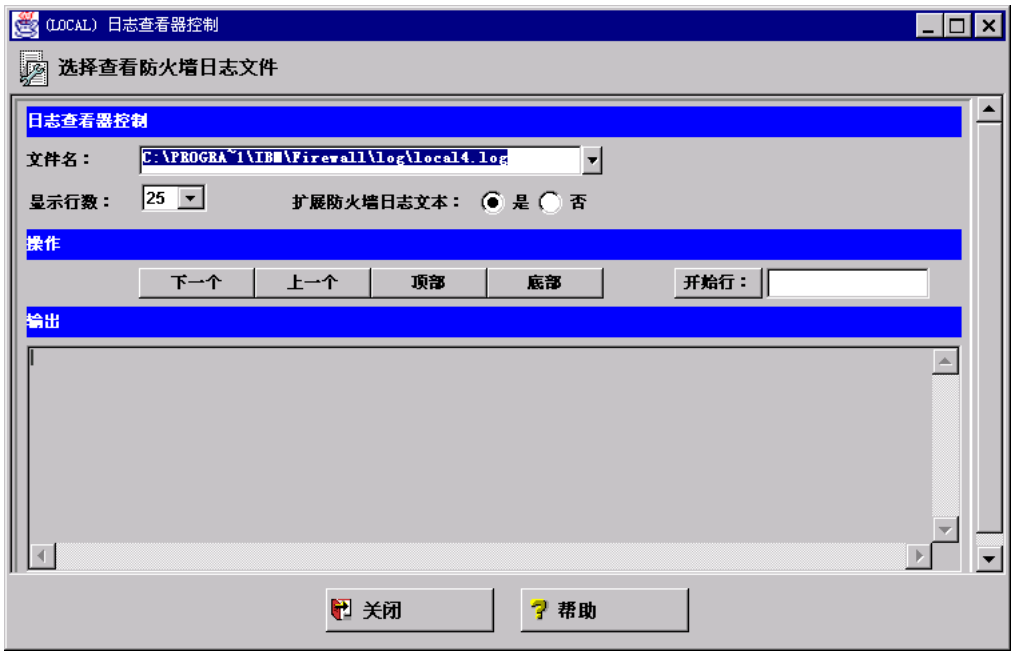

图 7. 日志查看器

其它特性

搜索字段位于某些面板靠近左上角的地方。您可输入一个搜索字符串然后单击**查找**。

在许多配置客户程序对话框中都会看到的其它按钮。

应用 单击**应用**可以用当前的选项来填充前一个面板中的字段或保存对面板的更改。**应用**按钮不会使窗口消失。

底部 单击**底部**可到达面板的底部。

取消 单击**取消**可关闭窗口而不保存任何更改。

关闭 单击**关闭**从显示器中除去该窗口。

复制 **复制**按钮可在向列表添加新项目时节省时间。当选择了列表中的某一项后，单击**复制**来创建一个和选中项目相同的项。单击**复制**创建一个和选中项目相同的项，该项目将打开一个新建项，它将由列表中选中的项复制字段值。然后您就可按需要为新建项修改字段值了。

删除 单击**删除**就可删除列表中选中的项目。

下移 选择列表中的一项然后单击**下移**，可以降低该项目在列表中的相对位置。每次单击会使得该项目下移一位。

上移 选择列表中的一项然后单击**上移**，可以升高该项目在列表中的相对位置。每次单击会使得该项目上移一位。

确认 单击**确定**以保存更改并关闭窗口。

打开 在选择列表中的一项后，单击**打开**以查看或修改该项。要添加一个新项目，单击列表中的**新建**项目然后单击**打开**。

刷新 单击**刷新**以重新访问防火墙中的数据然后将数据重新显示在面板上。

删除 单击**删除**从列表中除去一个选中的项。该操作将只从列表中删除该项。该操作对于其它地方定义的项目不起作用。

选择 单击**选择**以访问对于该功能有效的候选项目的列表。

顶部 单击**顶部**到达面板的顶部。

公共字段

在许多配置客户程序对话框中都会看到的公共字段。

输出 当已启动的命令继续执行时，会在此出现进展信息。

名称 为该项提供一个名称。该项目名对于防火墙中的这个特定功能必须是唯一的。该名称不应包含管道符（|）、单引号（或撇号）字符（'）或双引号（″）字符，因为它们是作为 SMIT 和文件定界符使用的。使用这些字符可能会产生不可靠的数据。

说明 该字段是可选的，在希望对该项提供注解或附加信息的情况下出现。

独特功能

有几个必须知道的配置客户程序的独特功能。

对于 Windows 95 或 Windows NT 配置客户程序来说，配置客户程序至少应使用 1024 象素 x 768 象素的分辨率。

如果按下鼠标左键滚动到旋转控制，并意外拖开鼠标时没有释放鼠标键，则旋转控制将继续。要停止它，用鼠标左键单击一个旋转控制方向箭头。

如果您使用 SSL 快速连续地两次或多次注册到 Firewall，连接将被拒绝。退出然后重新启动配置客户程序。

第5章 IBM Firewall 入门

本章提供您所需的设置 IBM 防火墙的基本配置步骤。 它说明如何定义一个安全接口，如何决定安全性策略及如何定义网络对象。

基本配置步骤

对于一个基本 IBM 防火墙的设置，应执行下列步骤:

1. 规划 IBM Firewall 设置。预先决定您要使用防火墙的哪些功能及要如何使用这些功能。下列各节会很有帮助:
   - 第1页的『第1章 介绍 IBM Firewall』
   - 第5页的『第2章 规划』
   - 第47页的『规划考虑事项』
2. 要让防火墙知道，它的哪一个接口是和安全网络相连的。您必须有一个安全接口和一个非安全接口以使防火墙正常工作。从配置客户程序浏览树中，打开“系统管理”文件夹并单击**接口**来查看在您防火墙上的网络接口列表。如果要更改一个接口的安全性状态，请选择一个接口并单击**更改**。请参阅第20页的『指定网络接口』 可获得更详细信息。

   如果您想连接至 Internet，请与您的 ISP 联系以获得 Firewall 非安全接口的注册 IP 地址。
3. 通过访问“系统管理”文件夹中的**安全性策略**对话框来建立常规安全性策略。对于典型的防火墙配置:
   - 允许 DNS 查询
   - 拒绝到非安全接口的广播信息
   - 拒绝 socks 到非安全适配器

   请参阅第20页的『使用配置客户程序来定义安全性策略』以获取详细信息。
4. 设置域名服务和邮件服务。从配置客户程序导航树的“系统管理”文件夹内访问这些功能。首先请阅读第27页的『第6章 处理域名服务』。
5. 使用配置客户程序浏览树中的**网络对象**功能定义防火墙的网络关键元素。网络对象通过防火墙控制通信。将下列关键元素定义为网络对象:
   - 防火墙安全接口
   - 防火墙非安全接口
   - 安全网络
   - 安全网络上的每个子网
   - 适当的 SDI 服务器和 NT 域服务器的主机网络对象

   请参阅第22页的『网络对象』以获取详细信息。
6. 启用防火墙上的服务。这些服务是安全网络用户访问非安全网络的方法（如 socks 或代理）。哪些服务能实现取决于您在规划阶段的决策。实现某一服务通常需要设置一些连接配置以允许特定类型的通信量。例如，如果要允许安全用户通过使用 HTTP

代理在 Internet 上冲浪 web，则不仅需要在防火墙上配置的 HTTP 代理精灵程序，还必需设置连接以允许 HTTP 通信。有关如何建立支持特定服务的连接的详细内容，请参阅第47页的『第9章 服务示例』。

7. 设置防火墙用户。如果您需要认证诸如出站 Web 访问的功能或认证防火墙管理员，则需要对防火墙定义这些用户。请参阅第69页的『第12章 管理防火墙上的用户』以获取详细信息。
8. 如果要使用 Windows NT 域口令作为认证，则必须配置 Windows 客户程序代码来实现以认证为目的的搜索可信任 Windows NT 域的能力，用 TCP 代替 NETBIOS。NETBIOS 将被禁用。可信赖的 Windows NT 服务器必须拥有 TCP/IP 主机名和地址，并且在这些服务器和防火墙之间必须具有 TCP/IP 连通性。防火墙管理员需要在防火墙和可信赖 Windows NT 服务器之间创建连接，以允许通信在两者之间流动。
9. 如果要使用网络地址转换，请首先与您的 ISP 联系以获取注册 Internet 地址，来使用多对一地址转换。然后，转至*添加 NAT 配置*面板将注册 Internet 地址添入*多对一 IP 地址*字段。如需要更多信息，请参阅第103页的『第16章 转换网络地址』。

遵循这些步骤应当能帮助您设置和运行一个基本的防火墙配置。IBM Firewall 还提供了其它功能，如帮助您确保网络安全性的系统日志。请参阅第97页的『第15章 管理日志和档案文件』以获取详细信息。

指定网络接口

本书对安全与非安全接口、网络和主机之间作出区分。安全接口将 IBM Firewall 主机与内部网中的主机网络（即想要保护的网络）相连接。 **您必须至少有一个用于防火墙工作的安全接口。**非安全接口将 IBM Firewall 与一个或一个以上外部网或与 Internet 连接。IBM Firewall 必须至少有一个非安全接口。

所有通过安全接口连接的网络都可视为安全网络。要区分连接到安全接口的各种子网，请使用专门的过滤器规则来拒绝或允许几种子网之间的访问（这些子网在基于 IP 地址或地址掩码的同一接口上）。

要指定安全和非安全接口，请使用配置客户程序浏览树上的“系统管理”文件夹。 将显示所有已知的接口（适配器）并将它们标识为安全或非安全。

必须在能执行特定接口过滤前为每个接口提供一个名称。

要将一个网络接口标识为安全或非安全网络接口:

1. 选择一个接口并单击**更改**。
2. 必要时重复上述步骤。
3. 单击**关闭**。

如果要将接口标识为安全或非安全，并为它起一个有意义的名字，则单击**打开**. 该名称将用于过滤器的特定接口过滤。

使用配置客户程序来定义安全性策略

配置 IBM Firewall 时要考虑的首要事情之一是安装的常规安全性策略。

IBM Firewall 提供了一个如第21页的图 8所示的帮助您设置安全性策略的对话框。

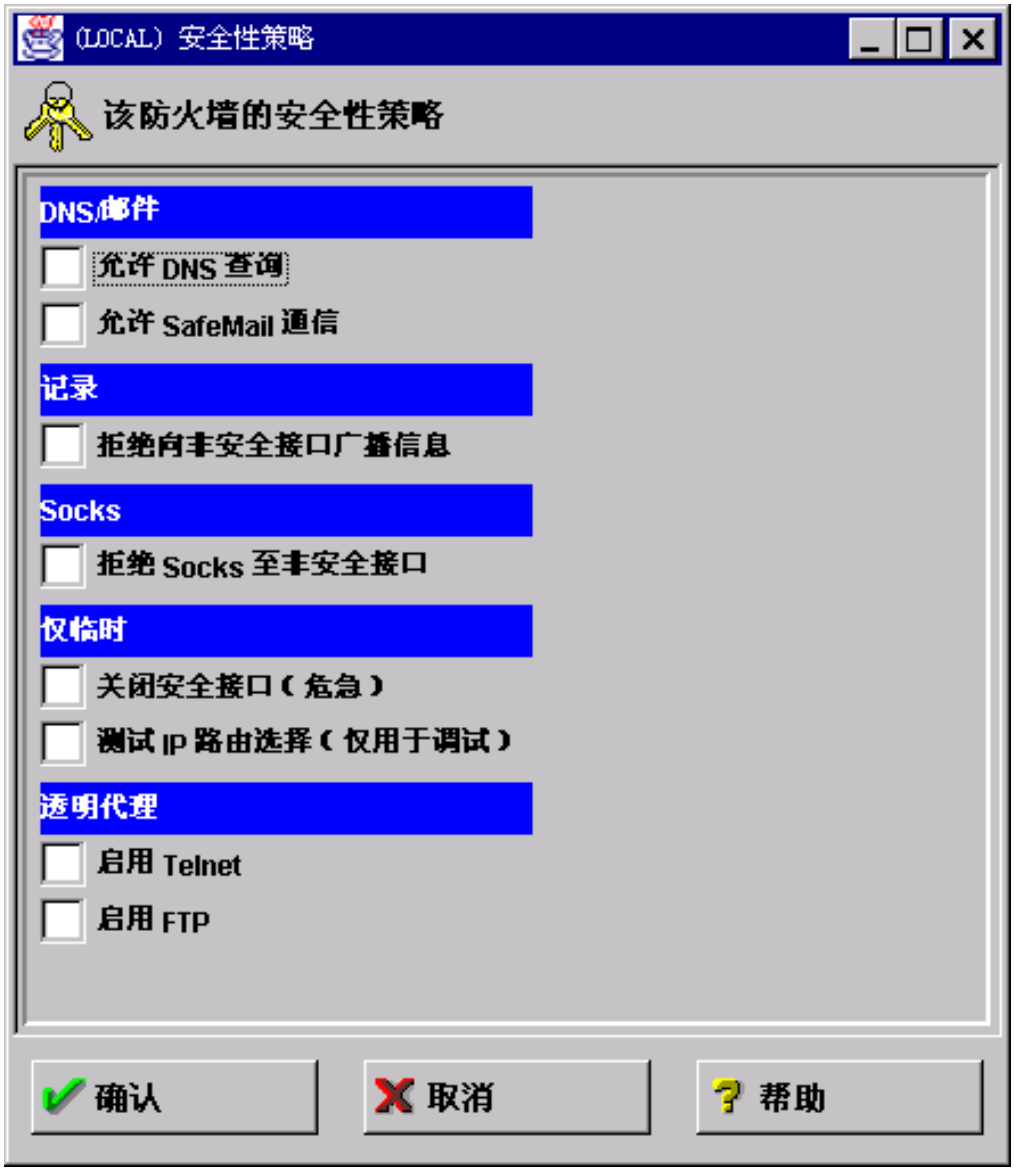

图 8. 安全性策略

单击“帮助”可获得有关安全性策略面板的详情。

安全性策略为管理员提供了一个快捷简单的设置防火墙全盘策略的方法。 安全性策略窗口中显示的大多数复选框都提供了一个选择特定“预定义服务”(适用于所有防火墙接收到网络通信量) 的快速路径。例外情况是“透明代理”选项，它只是简单地启用或禁用透明 Telnet 和透明 FTP。

当您选择了一个安全性策略，防火墙就会建立今后将要激活的过滤器规则。防火墙启用选定的服务并使其全局可用。

注意任何时侯选择了一个从属于“预定义服务”的复选框并单击**确认**时，都必须通过“连接激活”窗口激活这些更改。不必激活“透明代理”选择因为这些选项不属于“预定义服务”。请参阅第55页的『预定义服务』 以获得预定义服务的列表。

已提供了下列复选框列表，通过它们可以选择反映您站点安全性策略的属性。已选中的属性适用于在 IBM Firewall 两边的所有地址。

- 选择**允许 DNS 查询**以允许域名服务解析请求和应答。
- 选择 **SafeMail** 以允许邮件通信流经 Firewall。
- 选择**拒绝向非安全接口广播信息**，防止在非安全端口上接受到广播信息。如果防火墙的非安全接口连接到 Internet 上，该服务有助于减少在防火墙上记录的数量。
- 选择**拒绝 Socks 至非安全适配器**，不允许 socks 通信量从非安全网络进入防火墙。
- 选择**关闭安全接口（危急）**，不允许所有通信量在安全接口上进出防火墙。它只用于紧急情况。
- 选择**测试 IP 路由选择（仅用于调试）**，允许在任何接口上的全部通信量进出防火墙。请注意：如果更改该复选框的值，您必须单击**确认**并通过“连接激活”窗口激活它。**使用该服务可能导致防火墙安全性的曝光。使用时必须极其小心。**
- 选择**启用 Telnet** 以允许透明代理 Telnet。
- 选择**启用 FTP** 以允许透明代理 FTP。

网络对象

网络对象是对存在于网络中的组件的表示，比如主机、网络、路由器、虚拟专用网络或用户。 当创建连接时，网络对象指定服务的源和目的地址。

对象可由名称、图标表示、类型和说明来标识。存在几种类型的网络对象，但主机和防火墙是最普遍的。随 IBM Firewall 交付的缺省网络对象是“外部世界”。 它是一个全局对象，包括所有可能的 IP 地址。在填写了网络配置工作表后（请参阅第6页的『网络配置规划工作单』），就准备建立对象。

可以创建单个或组对象。所有网络对象由 IP 地址和地址掩码(子网掩码)定义，所以有可能一个对象表示整个网络地址的范围。

使用配置客户程序来定义网络对象

要定义单个网络对象，请从配置客户程序浏览树中选择**网络对象**。出现一个网络对象对话框。双击**新建**。出现**添加网络对象**对话框，如第23页的图 9 所示。

图 9. 添加网络对象

1. 输入对象类型。单击**对象类型**箭头以查看您所可以创建的对象。出于性能原因，最好创建网络类型对象而不是主机类型对象。您可创建的对象类型为:
   - 主机 - 网络上，一个掩码为 255.255.255.255 特殊节点。
   - 网络 - 一组由地址范围和特定的子网掩码所描述的网络地址范围。
   - 防火墙 - 一台安装了防火墙并且掩码为 255.255.255.255 的机器。只有一个防火墙网络对象可以是 IBM 或人工隧道的目标。
   - 路由器 - 在两个或两个以上的网络间路由通信量的主机，其掩码为 255.255.255.255。
   - 接口 - 机器上一个掩码为 255.255.255.255 网络适配器。它不一定是防火墙上的适配器。
2. 填入对象名。
3. 填入说明。该字段是任选的。
4. 输入此对象的点十进制 IP 地址。
5. 输入子网掩码，指定地址中的位与 IP 信息包的地址相比较。
6. 单击**确认**。

网络对象组

一个组表示网络对象的一个集合。组是作为设置连接时的便利设施使用，并可以消除重复的工作。其中一例就是将一些地址 (由网络对象单个表示) 组织成一个表示一个部门的网络对象组。该部门可用作针对一个连接的源或目的地址。

要定义一组网络对象，从配置客户程序浏览树中选择“网络对象”。 出现**网络对象**对话框。双击**新建组**。出现**添加网络对象**对话框。

1. 填入组名。
2. 填入说明。该字段是任选的。
3. 单击**选择**以选择该组的对象。
4. 单击**确认**。

提示: 在任何可能的时侯将连续的地址范围包含到单个网络对象中是一个好办法。 这将改进连接规则处理的性能。以下示例就解释了这点。

```
会计部门
  Kevin's machine  191.1.10.1
  Susan's machine  191.1.10.3
  Helen's machine  191.1.10.5
  Peter's machine  191.1.10.7
  Bob's machine    191.1.10.9
```

要创建该会计部门的网络对象，您将输入该组的 IP 地址信息为: 191.1.10.0，子网掩码为 255.255.255.0。这个网络对象，即会计部门，可用作针对一个连接的源或目的地。

备份防火墙配置

防火墙将所有配置文件存储于 ROOTDIR\config 中。如果要备份防火墙配置，但不备份所有防火墙文件，则备份 ROOTDIR\config 目录中的所有内容。

如果要恢复备份的防火墙配置，删除所有 ROOTDIR\config 目录中的现存文件，然后恢复文件的备份版本。必须在还原配置生效前重新生成并激活过滤器规则。

关键的防火墙配置文件列示如下。防火墙上的 \config 目录可能不包含在这里列出的每个文件。注意大多数防火墙配置文件是能用文本编辑器查看的简单文本文件，**不支持手工编辑这些文件**。

- carriers.cfg - 寻呼通信公司定义
- cfgfilt.output
- explode.cfg
- filters.active - 指示过滤器是否活动
- fwadpt.cfg - 网络接口定义
- fwconfig.map - 包含配置文件名称
- fwconns.cfg - 过滤器连接定义
- fwfilters.cfg - 当前活动的过滤器
- fwhttp.cfg - HTTP 代理配置
- fwmail.conf - SafMail 配置
- fwobjects.cfg - 网络对象定义
- fwpolicy.cfg - 安全性策略选项
- fwrules.cfg - 过滤器规则模板定义
- fwservices.cfg - 服务定义
- fwsocks.cfg - 来自配置客户程序的 Socks 5 规则

- fwtdefn.conf - 警报定义
- fwtpproxy.cfg - 透明代理定义
- fwusrdb.cfg - 防火墙用户数据库
- logmgmt.cfg - 存档定义
- modems.cfg - 调制解调器定义
- pager.cfg - 寻呼机定义
- rcsfile.cfg - 配置服务参数
- Socks5.conf - 生成的 Socks 5 配置文件
- Socks5.header.cfg - 生成的 Socks5.conf 的用户提供部分
- syslog.conf - 日志设施定义

第6章 处理域名服务

本章将说明如何配置与 IBM Firewall 相关的域名服务（DNS）。 DNS 的目标是在向安全网络外的主机不提供信息的同时为安全网络中的主机提供完整的域名服务。这将使安全网络内的用户可以访问 Internet 所提供的所有服务。但是，由于其拒绝泄漏有关安全网络的信息，将使一个入侵者更难寻找到一个可攻击的计算机。

需要三个域名服务器来完成这个目标:

1. 一个在 IBM Firewall 上
2. 一个在安全网络内
3. 一个在安全网络外

参考第27页的图 10 以查看 DNS 如何与 IBM Firewall 一起工作。

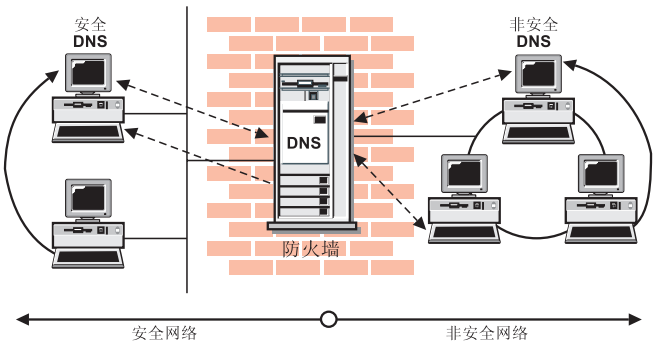

图 10. DNS

把防火墙配置成一个位于安全网络名称服务器和非安全网络名称服务器之间的网关。防火墙所扮演的角色用官方术语来说，称为*仅缓存的名称服务器*，因为防火墙的 DNS 自身不包含任何数据库文件。

第27页的图 10 说明了防火墙所扮演的角色。任何时侯，当防火墙需要解析它自己所使用的一个名字时，它就询问安全方的名称服务器。任何时侯，当一个查询转发至防火墙时，它将依次把查询转发至非安全名称服务器。

当安全网络上的客户程序想知道安全方信息时，它就把请求发送至它所要询问的安全方 DNS。当同一个安全网络上的客户程序要知道非安全方信息时，它将把请求发送至和上述相同的安全方 DNS。由于该查询所要知道的是非安全信息，安全方 DNS 不能回答，所以安全方 DNS 再把查询转发至防火墙。当一个非安全方 DNS 将一个请求转发到防火墙上，该请求将被转发到非安全 DNS 域，这样仍然没有泄漏敏感信息。

使用配置客户程序来配置 DNS

要配置 DNS，从配置客户导航树上选择“系统管理”。 双击文件夹图标以展开视图。选择**域名服务**。 IBM Firewall 显示了当前可以修改的 DNS 配置。

图 11. 域名服务

注: 当添加 DNS 时，防火墙将保存并重新命名所有现存的域名服务配置文件。

1. **安全域名**字段标识了一个域名，防火墙将把该域名添加到任何不合格主机名中。
2. **安全域名服务器**字段引用了一个服务器，该服务器用于解析由 IBM Firewall 从 Internet 所保护的主机名和 IP 地址。可以输入用空格分隔的点十进制的 IP 地址。
3. **非安全域名服务器**字段引用了服务供应商提供的服务器，用于解析有关非安全网络的信息。可以输入用空格分隔的点十进制的 IP 地址。

注: 当初始化一个名称服务器时，它将发出查询以获得 root 名称服务器的列表。大多数实现方法都在内存中保留了该列表。然而，Mircosoft 的实现方法是将该列表写回到配置文件中。这将不修改名称服务器的运行情况，但将修改**非安全名称服务器**字段中所显示的值。这不是我们所关心的问题。

配置安全名称服务器

必须把安全名称服务器配置成：把未解析的查询转发至防火墙。 如果有一个标准的 BIND 实现方法，则在安全名称服务器的 *boot* 文件中添加 *forwarders* 和 *cache* 语句。

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

创建高速缓存文件，*named.cache*，指向防火墙:

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

这里，*private.com* 指安全方使用的域名，而 *aaa.bbb.ccc.ddd* 指防火墙的 IP 地址。

另外，您还可能要把防火墙的主机名添加到 DNS 数据库中。使用这种方法，您的用户就可以使用防火墙的主机名代替其 IP 地址来访问防火墙的 Socks 服务器、HTTP 代理、Telnet 代理和 FTP 代理。如此，需要增加两个步骤，*第 4 章的 DNS 和 BIND* 对此已作了介绍。欲更详细地了解本书，请参阅*书目*。

首先添加一个 A 记录至域数据库文件:

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

再把一个 PTR 记录添加到反向查找文件:

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

如果您的安全网络不使用 DNS，那么您的防火墙就必须能自始至终对其本身的信息加以解析。按正常情况配置防火墙，但在**安全名称服务器**字段内列示防火墙的安全的接口。然后在 `c:\winnt\system32\dns\boot` 中添加下列各行:

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

创建与下列内容相似的 *fwnamed.rev*:

```
ccc.bbb.aaa.in-addr.arpa  IN SOA firewall.private.com. root.public.com. (
                          9        ; Serial
                          86400    ; Refresh after 1 day
                          300      ; Retry after 5 minutes
                          654000   ; Expire after 1 week
                          3600  )  ; Minimum TTL of 1 day
ccc.bbb.aaa.in-addr.arpa.          IN NS    firewall.private.com.
ddd.ccc.bbb.aaa.in-addr.arpa.      IN PTR   firewall.private.com.
```

配置安全客户程序

必须把安全网络中的客户程序配置成: 将其查询发送至安全名称服务器而非防火墙。这是非常重要的，因为这将保证防火墙的内存中的高速缓存中没有安全方的信息。而且，它节省了防火墙的工作负荷，因为除了一个查询要从安全方转发至非安全方，其它情况防火墙将无需参与。

如果您的安全网络不使用 DNS，那么您的客户程序必须将名称服务器指向防火墙。

向公众发布服务

许多组织都希望对 Internet 公众提供特定的服务。通常，这些服务包括 e-mail 和 Web 服务器，虽然任何类型的 TCP/IP 服务器都可以使用。为了能使用这些服务，您不但需要将服务器置于可获取这些服务的网络中，而且您还必须在公用 DNS 中列出该服务器，以便用户可以获得正确的信息。

可以通过两种方法来实现。一种方法是让您的服务供应商把您的服务器列入其域（也就因此放入了其名称服务器），作为该域的一部分；另一种方法是必须使用自己的名称服务器，并将它注册至 Internet。由 Internet 服务供应商（ISP）向您提供服务较为方便。如果您选择这种方法，您应当向他们提供您所希望列出的主机名和 IP 地址。例如，如果您以 *www.public.com* 来运行您的公用 web 服务器，其 IP 地址是 *50.100.150.200*，那么您应该让您的 ISP 在 *50.100.150.200* 上列出 *www.public.com*。

另外，如果您希望接收 e-mail，那么应当要求您的 ISP 把您的防火墙列为公用电子邮件域的*邮件交换器*。ISP 应当知道主机名*(gateway.public.com)*、它的 IP 地址*(50.100.150.201)* 以及您希望用于接收邮件的域名 *(public.com)*。

如果您的 ISP 不希望对您提供这些服务，那么您只能自己来完成。再次申明，您有两个附加选项。您可以将 DNS 服务器置于 DMZ 中，或者用您的防火墙作为名称服务器。

使用防火墙并没有附加的安全性风险，因为在那里放置的数据库文件不包含任何有关安全网络的信息。其中将只存储有关您要提供的公共服务。

涉及设置 DNS 服务器的细节包含在第 4 章 *DNS 和 BIND*，列在*书目*中。强烈推荐您阅读这一章，如有必要，应首先阅读那一章。建立一个 DNS 服务器并非是一个简单的任务，通常应留给专家来完成。如果您有这样一位专家，慎重考虑运用其专门知识。

请参阅第30页的『样本配置』以获取详细信息。

安装 Microsoft DNS 服务器

要安装 Microsoft DNS 服务器，请转至控制面板，单击**网络**，单击**服务标签**，单击**添加**，然后选择 **Mircosoft DNS 服务器**。将需要安装 CDROM。

故障检测 DNS 问题

IBM eNetwork Firewall 参考大全 中有一章是关于防火墙故障检测的。该章节中有一个特定部分是有关 DNS 问题的。这个部分建议使用 *nslookup* 命令来标识 DNS 系统的故障段。

样本配置

本节描述一些样本配置，其中可能布置一个防火墙。这些实例中的大多数着重于 DNS 操作必需的配置。这些实例中的一个描绘了您的网络是不太可能的，因此请注意理解每个实例，并对特殊安装应用适当的概念。

实例 1: 非安全接口上 DMZ 中的 DNS 服务器

第一个实例显示了需要在 DMZ 中操作名称服务器的文件，该文件位于非安全网络内，如第30页的图 12 所示。

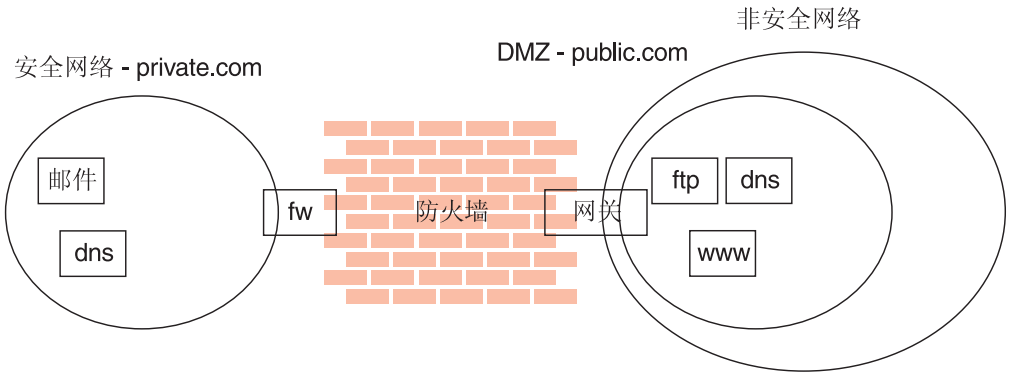

图 12. 安全网络内 DMZ 中的名称服务器

这张图说明一个专用网络，*private.com*，IBM Firewall 后面的安全接口称为 *fw.private.com*，非安全接口称为 *gateway.public.com*。公司的 DMZ 连接至非安全接口，并包含一个

名称服务器 *dns.public.com*、一个 FTP 服务器 *ftp.public.com* 和一个 web 服务器 *www.public.com*。*dns.public.com* 上实现该方案的文件如下:

db.public

```
public.com.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; serial number
                 10800       ; refresh after 3 hours
                  3600        ; retry after 1 hour
                 604800      ; expire after 1 week
                 86400  )    ; minimum TTL 1 day
;
; Nameservers
;
public.com           IN NS  dns.public.com.
;
; Hosts in the DMZ
;
dns.public.com.      IN A 50.100.150.202
gateway.public.com.  IN A 50.100.150.201
www.public.com.      IN A 50.100.150.200
ftp.public.com.      IN A 50.100.150.203
;
; Mail-related entries
;
public.com.          IN MX  0  gateway.public.com.
public.com.          IN CNAME gateway.public.com.
```

db.50.100.150

```
150.100.50.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; serial number
                 10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                 604800      ; expire after 1 week
                 86400  )    ; minimum TTL 1 day
202.150.100.50.in-addr.arpa.      IN NS dns.public.com.
203.150.100.50.in-addr.arpa.      IN PTR  ftp.public.com.
202.150.100.50.in-addr.arpa.      IN PTR  dns.public.com.
201.150.100.50.in-addr.arpa.      IN PTR  gateway.public.com.
200.150.100.50.in-addr.arpa.      IN PTR  www.public.com.
```

db.127.0.0

```
0.0.127.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; serial number
                 10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                 604800      ; expire after 1 week
                 86400  )    ; minimum TTL 1 day
0.0.127.in-addr.arpa.   IN NS  dns.public.com.
1.0.0.127.in-addr.arpa.   IN PTR localhost.
```

db.cache

该文件最好的一个选择是从 *ftp://ftp.rs.internic.net/domain/named.root* FTP 当前 root 名称服务器列表。

boot

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

要设置通信过滤器允许适当 DNS 通信，启用**安全性策略**面板上的*允许 DNS 查询*。

实例 2: 专用接口上 DMZ 中的 DNS

在第二个实例中，DMZ 的 DNS 仍在专用的名称服务器上，但这一次 DMZ 连接至与非安全网络接口不相同的接口。

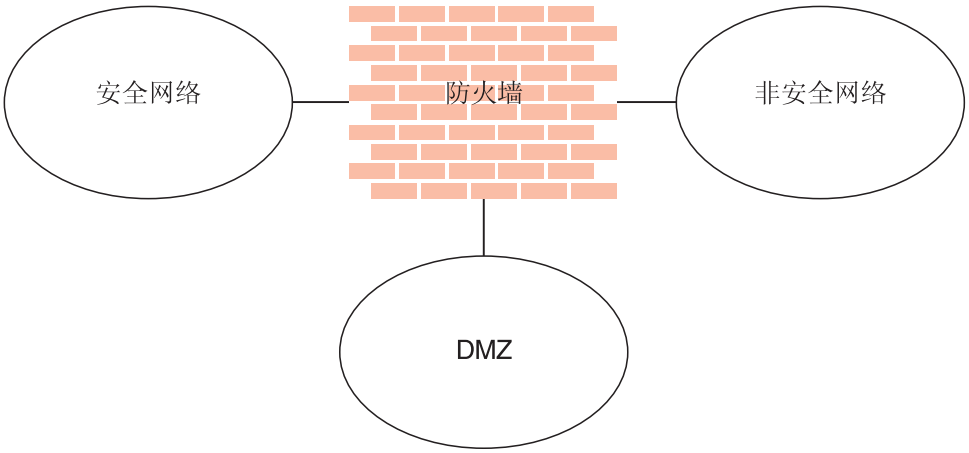

图 13. 专用接口上的 DMZ 中的 DNS

dns.public.com 上的 DNS 数据文件与前实例中的相同。为了使该名称服务器可从公用网络访问，必需要么打开通信过滤器要么执行区传送以将数据文件复制到防火墙。

要打开通信过滤器，复制三个规则模板，名为 *DNS 服务器查询*、*DNS 回答*和 *DNS 客户查询*。将每个规则上的路由选择设置从*本地*更改为*路由的*。然后在一个服务中包括这三个新建规则模板，并按如下设置流指示符:

- DNS 客户查询: --->
- DNS 回答: <---
- DNS 服务器查询: --->
- DNS 服务器查询: <---

在一个连接中包括该服务，该连接使用 *The World* 为源对象，使用 *dns.public.com* 为目的对象。

要执行区传送，需要设置通信过滤器并指示名称服务器复制适当的文件。要设置通信过滤器:

1. 在**安全性策略**面板上，启用*允许 DNS 查询*。
2. 从 *dns.public.com* (源对象)将一个连接添加至防火墙的 DMZ 接口(目的对象)，该目的对象包括名为 *DNS 传送*的服务。

要激活区传送，添加下列行至 `c:\winnt\system32\dns` 中防火墙的 *boot* 文件:

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

然后转至服务控制管理器，停止然后重新启动 DNS 服务器服务。

实例 3: 使用防火墙为安全名称服务器

要使用防火墙为安全名称服务器，则在防火墙上放置数据库文件(通常驻留在安全服务器上)。然后客户就能指向防火墙作为他们的 DNS 服务器。与这种方法相关联的风险即 DNS 服务器不能辨别该请求是来自安全方还是非安全方。因此，它将安全方信息提供给任何查询的客户；您不再能隐藏安全 DNS 信息。

要实现这种方法，通过使用配置客户程序配置防火墙 DNS 设施来启动。对于*安全域名*字段，列出将在安全网络上使用的域名。对于*安全名称服务器*，列出防火墙的接口。对于*非安全名称服务器*，通常列出 ISP 提供的名称服务器。然后必须创建防火墙上的反向查询文件以补充这种配置。

创建类似于下列例子的文件 `c:\winnt\system32\dns\fwnamed.rev`。

对于这个例子，防火墙的安全接口命名为 *fw.private.com* ，它的 IP 地址为 *10.100.100.1*。

```
100.100.10.in-addr.arpa.   IN SOA fw.private.com. admin.fw.private.com. (
                 1           ; serial number
                 10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                 604800      ; expire after 1 week
                 86400  )    ; minimum TTL 1 day
1.100.100.10.in-addr.arpa.         IN NS fw.private.com.
1.100.100.10.in-addr.arpa.         IN A  fw.private.com.
```

然后在 `c:\winnt\system32\dns\boot` 中添加下列行:

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

在该方案中，必须配置客户程序指向防火墙 (10.100.100.1) 为他们的 DNS 服务器。防火墙将辅助外部信息的解析，但没有安全方信息的解析。这意味着，任何想连接至防火墙上的配置服务器或任何代理服务器的安全方客户必须通过 IP 地址而不是主机名来引用防火墙。

第7章 SafeMail

IBM Firewall 的 SafeMail 网关提供一个用于 SMTP 通信的网关。 它将报文从安全 mailserver 传送至非安全方，同时隐藏了敏感的域名。它将报文从非安全方传送到安全邮件域，使安全网络免遭攻击。

虽然 SafeMail 不执行内容筛选，但是 SafeMail 提供了一个用户出口，通过该出口来执行内容筛选。欲知详情，请参阅第36页的『SafeMail 用户出口』。

SafeMail 实时地将报文从发送者传送到接收者。这将避免了维护防火墙上报文队列的风险和复杂性。这就需要对邻近邮件域作一些特定的配置。在某些情况下，这些需求对于一个特殊安装并无实用价值。若是这种情况，可以单独购买多种 SMTP 服务器中的任何一个，然后将其安装以替代 SafeMail 。如果您选择安装一个完整的 SMTP 服务器，那么请在配置时考虑其安全性。参阅第37页的『使用 SMTP 服务器来代替 SafeMail』以获取详细信息。

使用配置客户程序来配置 SafeMail

要配置 SafeMail，请从配置客户程序浏览树选择系统管理。双击文件夹图标以展开视图。选择 **SafeMail**。IBM Firewall 将显示已配置的邮件服务器和域的列表。您必须为正在配置的每个专用方邮件域配置一个项。

1. 要添加一个域，选择**新建**，然后单击**打开**。出现**添加邮件服务器**对话框。
2. **安全域名** 字段包含名称，通过该名称，防火墙安全方的用户可得知正被描述的邮件域。
3. **安全邮件服务器名**字段包含了该项使用的主机名或邮件服务器的点十进制的 IP 地址。该服务器必须在某一安全网络上。可以仅为一个给定域列出一个邮件服务器。
4. **公用域名**字段包含名称，通过该名称，在非安全防火墙方的用户可得知正被描述的邮件域。为隐含安全网络的拓扑图，该名称将被安全域名替代。
5. 单击**确认**。

更改邮件配置项

要更改一个邮件配置项，请在列表中选择一个项，然后单击**打开**。出现**更改邮件服务器配置**对话框。

安全域名字段是禁用的，但可以更改其它字段，如第35页的『使用配置客户程序来配置 SafeMail』所示。

注:

1. 如果您以前已配置 SafeMail 并在此指定一个安全邮件服务器，则该邮件服务器替换您先前已配置的邮件服务器。
2. 如果您以前 “没有” 配置过 SafeMail，且在此指定了一个安全邮件服务器，则该邮件服务器将加入此配置。

删除邮件配置项

要删除 SafeMail 配置项，请在列表中选择一个项，然后单击**删除**。将得到一个删除警告。单击**确认**以删除该项，若您改变了主意，则单击**取消**。

配置安全服务器

您必须配置安全邮件服务器，用以列出视为未知域网关的防火墙。这将导致发送给非安全网络的邮件先要转发至防火墙。同时，必须把每台服务器配置成可接受地址为专用域名以及地址为公用域名的报文。当防火墙转发一条来自非安全网络的注释时，将列出所有带公用方域名的收件人。

如果在安全网络中存在不止一个的不同的邮件域，那么必须将每台服务器配置成将要发送给另一安全方域的邮件直接转发到该台服务器上，而无须再通过防火墙。这将减轻防火墙不必要的工作负荷，并将使防火墙的实时传递机构的功能运用得恰到好处。

配置公用域

在非安全网络中唯一要配置的是：将您的防火墙列为您网络的邮件交换器。让您的服务供应商在他们的 DNS 服务器中添加必需的信息。请参阅第27页的『第6章 处理域名服务』，以获取有关对该机制的其它特殊考虑。

其宗旨是为每个公用域名列出作为*邮件交换器*的防火墙，您可以使用这些公用域名接受邮件。例如，如果您在安全网络内使用域名 *private.com*，并且在安全网络之外使用 *public.com*，您就可以将防火墙命名为 *gateway.public.com*。在这种情况下，您应要求您的供应商列出作为主机（通常和 ″A″ 记录和 ″PTR″ 记录一起列出）的防火墙主机名和 IP 地址。然后，因为您希望接受地址是 *user@public.com* 的邮件，所以应让供应商为域 *public.com* 添加一个 MX 记录，该域将列出 *gateway.public.com* 作为该域的邮件交换器。如果还希望接收地址为 *user@somethingelse.com* 的邮件，可列出一个同样指向防火墙的附加的 MX 记录。

SafeMail 用户出口

SafeMail 提供了一个用户出口，在安装了 SafeMail 后，通过该出口将使 SafeMail 能够拒绝潜在的非法通信量。请参阅 *IBM eNetwork Firewall 参考大全*以获得为此提供的软件开发组件的详细说明。

这项功能将使您能够创建函数 *UsrCheck()*，它会在每次 SafeMail 从发送人处接收一个包时得到呼叫。一个包含了多个和系统状态相关的字段的结构将传送到这个函数。该结构包含了一个唯一的会话 ID，正在发送和接收的服务器的 IP 地址，前面已接收到的命令指示符和一个包含欲作分析的信息包的纯文本缓冲区。

可在这个函数中实现的校验类型有:

- *禁止的*主机列表
- 对不允许使用的字符序列（如不适当的语言或项目代码名）的扫描
- 对嵌入的引用字符串的检查

- 信息长度限制

如愿意，用户出口还可用于实现对一个第三方内容筛选产品的接口。

如果用户出口函数决定不处理信息，该函数将会返回一个原因码至 SafeMail。SafeMail 则立刻拒绝和正在发送的 SMTP 服务器的连接。同时，信息将被写入防火墙日志，包括由用户出口返回的原因码。

当对用户出口进行写操作时，切记每个已接收到的信息包都要呼叫该函数。进行写操作时，请尽可能小心，以防止对系统性能的负面影响。并且，请记住，该函数将运行于多线程环境下，因此必须以使线程安全的方式写入。您可以使用任何支持多线程操作的编译器写用户出口，并可以使用 *_cdecl* 链接约定。我们为 IBM Visual Age C++ 和 Microsoft Visual C++ 提供了样本 makefile。

使用 SMTP 服务器来代替 SafeMail

禁用 SafeMail

如果为了防止和另一个 SMTP 服务器产品发生冲突而禁止使用 SafeMail，那么就应禁止使用**服务控制管理器**中的 SafeMail 服务。从 Windows 的**开始**菜单中，选择**设置**、**控制面板**、**服务**。滚动滚动条，选择 *IBM Firewall SafeMail 服务器*。单击**启动**。在**启动类型**字段中，选择**禁用**。单击**确认**。

配置 SMTP 服务器

当您把一个完整的 SMTP 服务器和 SafeMail 安装在同一个地方时，应对多个方面加以考虑。本节将讨论 SafeMail 的安全性功能，这将有助您配置 SMTP 服务器，使其执行相似的功能。某些 SMTP 服务器可能无法执行某些任务，所以在购买产品之前，请仔细研究可用方案和您的要求。

存在某些将使邮件队列上溢或者混乱的破坏。虽然没有完全暴露的服务器可在无邮件队列的情况下操作，但如果您专门使用一个磁盘卷来完成此项任务，就可以减少与邮件队列有关的风险。这将使一个上溢队列对防火墙其它操作的影响的机会最小。

邮件服务器隐藏安全网络信息也是非常重要的。按照 SMTP 规则，每个转发邮件的服务器都应插入一首行 *Received:*。这些首行都可能被一个攻击者用于映射安全网络。当 SafeMail 处理一个注释时，它将去除所有这些首行；将您的 SMTP 服务器作同样的配置。同时， SafeMail 将为公用域名重写所有的专用方主机名。这样就能除去比可用于映射网络的信息更多的信息。

记录 SafeMail 输出的范例

下面是一个记录 SafeMail 输出的范例。

```
Feb 03 13:46:11 1998 mr16n18: ICA2163i: safemaild started.

Feb 03 13:41:14 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e7a19
received from RACK3BD.
Feb 03 13:41:21 1998 mr16n18: ICA2179i: SafeMail has forwarded 215575
bytes for connection 0xd71e6118 from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:21 1998 mr16n18: ICA2178i: SafeMail session 0xd71e7a19
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:23 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e831a
```

```
received from RACK3BD.
Feb 03 13:41:36 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e901b
received from RACK3BD.
Feb 03 13:41:56 1998 mr16n18: ICA2179i: SafeMail has forwarded 215567
bytes for connection 0xd71e7a19 from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: SafeMail session 0xd71e831a
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: SafeMail session 0xd71e901b
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail has forwarded 346
bytes for connection 0xd71e901b from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail has forwarded 358
bytes for connection 0xd71e831a from 9.67.144.52 to 9.67.131.250.
```

日志信息指示下列:

- ICA2177 - 指示新连接的开始。
- ICA2179 - 指示成功终止。
- ICA2178 - 指示已与接收 SMTP 服务器取得联系。
- ICA2181 - 指示 SafeMail 拒绝会话。参阅 *IBM eNetwork Firewall 参考*大全以得到原因码信息。
- ICA2180 - 指示会话终端。
- ICA2182 - 指示用户出口决定拒绝会话。

第8章 控制通过 Firewall 的通信

本章讲述了如何使用配置客户程序来控制经由 Firewall 的网络通信。 使用专家过滤器，防火墙以多个标准为根据（如一天的时间、IP 地址和子网）在会话层过滤包。过滤器在安全与非安全网络接口之间工作。它们不影响防火墙路由表。

缺省时，Firewall 不允许任何通信在安全和非安全网络间流动。必须创建连接来允许特定类型的通信在安全和非安全网络间流动。

使用配置客户程序来建立连接

使用第40页的图 14 中描述的配置客户程序的组件来创建网络对象、规则模板、服务和连接。

连接 把网络对象和服务和/或 socks 模板关联起来以定义端点之间允许的通信类型。每个连接定义一个 IP 特定类型的通信，该 IP 通信在源和目的网络对象之间被允许或拒绝。

服务 由一个或多个规则模板建立。定义 IP 通信的类型，该 IP 通信在源和目的对象之间被允许或拒绝。例如，可以构成一个服务，允许 Telnet 或拒绝 Ping。（一种 FTP 服务包括八个规则模板）。 IBM Firewall 与系统设定服务集合一起使用。 不能删除这些预装的系统设定服务，但可以修改某些字段。不过，如果这些预定义的服务不能满足要求，则可以通过使用规则模板来创建新的规则，以此来添加服务。详见 第58页的『定义服务』。

规则模板
为 Firewall 提供指令，根据它们的不同属性允许或拒绝 IP 包。

Socks 模板
为防火墙 Socks 精灵程序提供指令，根据它们的不同属性允许或拒绝 IP 包。

网络对象
表示各种与 Firewall 交互组件，如主机、用户和子网。它们由 IP 地址和地址掩码定义，所以有可能一个对象表示整个网络地址的范围。网络对象可以分类。

网络对象组
表示一个或多个网络对象。它们作为设置连接时的便利设施使用，并可以消除重复的工作。其中一例就是将几个地址组成一组，放在一个网络对象组中以表示一个部门。然后该网络对象组就可以作为针对一个连接的源或目的使用。

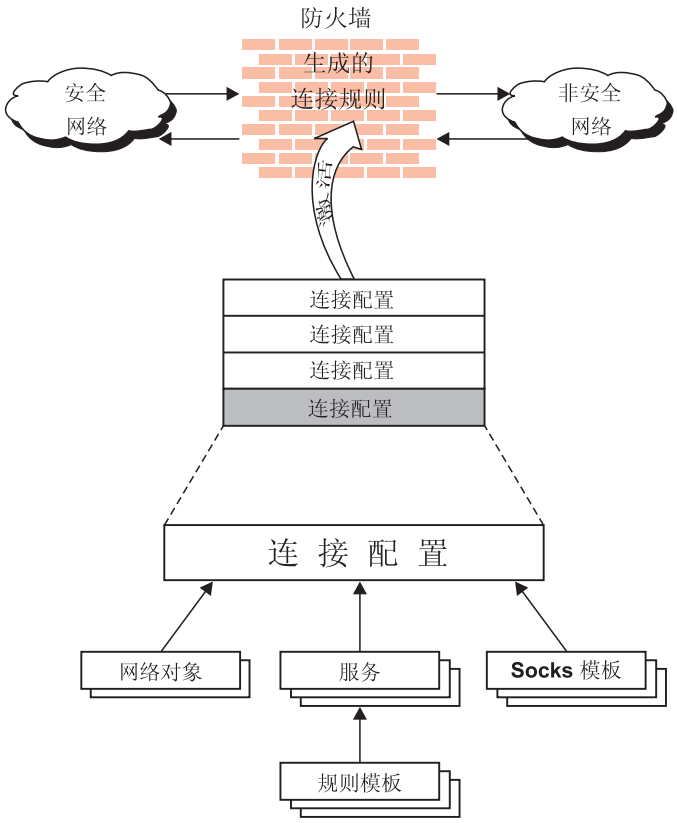

图 14. 建立连接

使用预定义服务建立连接

为了允许或拒绝在两个命名的网络对象或网络对象组之间（作为端点）特定类型的通讯，需要建立一个连接。

定义了网络对象之后，创建这些连接。为通过 Firewall 的通信流，选择一个网络对象或组作为源，另一个网络对象或组作为目的。

要建立一个连接，从配置客户程序浏览树中选择通信控制，然后双击文件的文件夹图标以展开视图。 选择**连接设置**。出现**连接列表**对话框。选择**新建**并单击**打开**。出现**添加连接**对话框，如第41页的图 15 中所示。

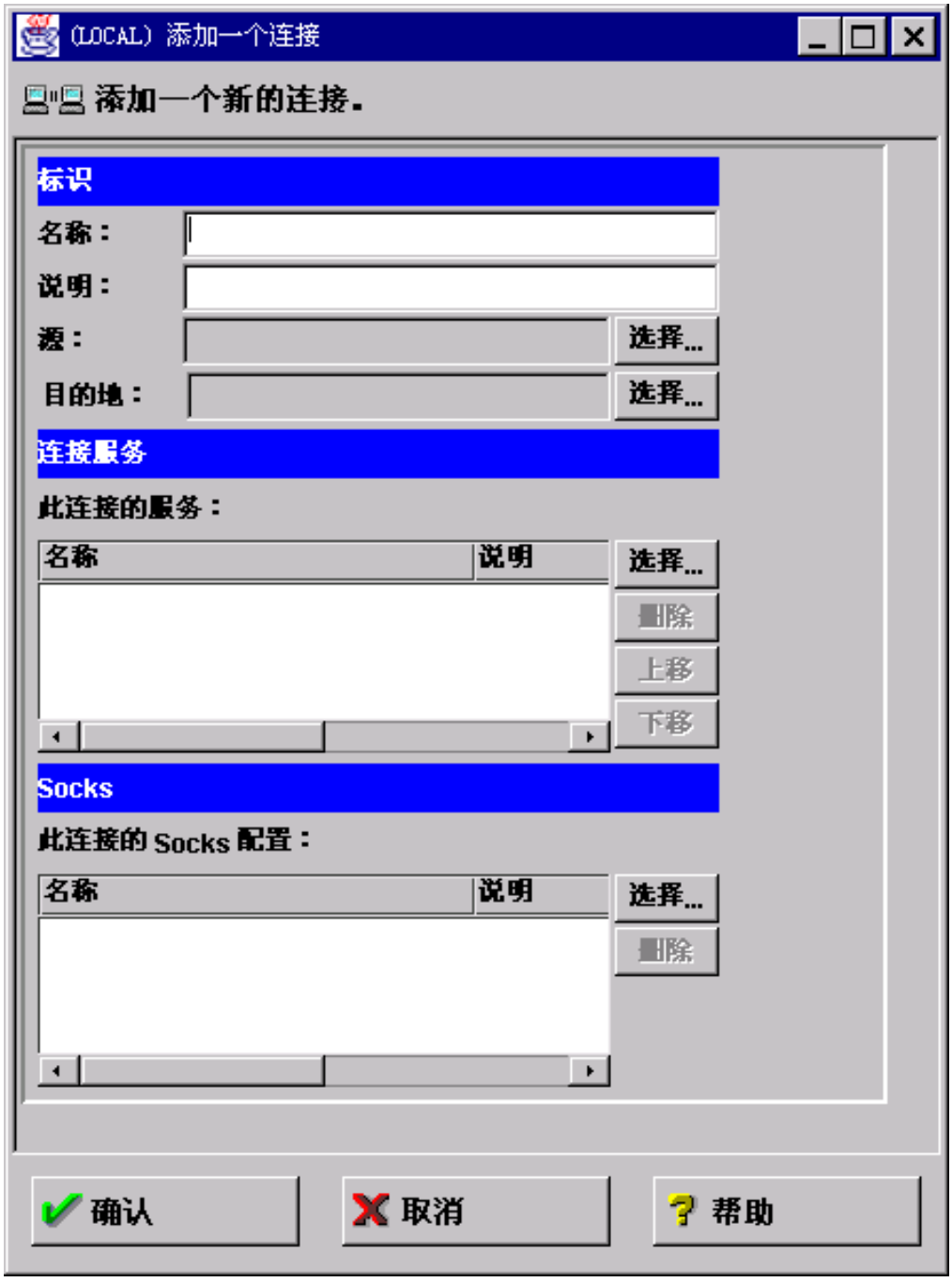

图 15. 添加一个连接

1. 为连接填入名称。
2. 填入连接的说明。
3. 对于源字段，单击**选择**并从**网络对象**对话列表中选择一个网络目标。
4. 对于目的字段，单击**选择**并从**网络对象**对话列表中选择一个网络对象。
5. 要对于该连接选择服务，单击**选择**并选择在端点之间想要控制的通信的类型。
6. 从列表中选择一个或多个服务，为连接添加服务。

7. 可通过选择一个服务并单击**上移**或**下移**来重新排序列表。请参阅第42页的『为连接排序』。
8. 可通过选择一个服务并单击**删除**来删除一个服务。
9. 使用**此连接的 Socks 配置**。按照步骤 5-7 来进行 Socks 连接。
10. 在已定义了所有东西后，单击**确认**。
11. 激活所有连接。见第42页的『连接激活』。

为连接排序

大多数 IBM Firewall 用户的规则都少于 1000。规则越多，对性能的影响越大。

当在一个网络接口上接收到一个包时，是进还是出防火墙主机，应从生成的连接规则的顶部开始应用规则。当来自包的信息与规则中的信息相匹配时，操作（允许或拒绝）就起作用。如果搜索了整个文件后也都没有发现匹配，则拒绝请求。

提示: 将更特定的连接放在较上端，将不很特定的连接放在较下端。例如，可能有一个部门 ABC，地址为（1.1.10.X），并且有一台机器在部门 ABC 中作为服务器使用，地址为（1.1.10.7）。如果因为机器 1.1.10.7 不是应该用于 telnet 通信的服务器而希望排除它，必须把连接 `Deny telnt for Dept ABC server` 放在 `Permit telnet for Dept ABC` 连接前。如果把连接顺序反过来，就再也不会遇到拒绝连接。

连接激活

注: 在激活连接前，确保定义了安全接口。

从配置客户程序浏览树中选择**连接激活**，进行以下任何操作:

重新生成连接规则并激活
Firewall 从连接配置中建立生成的连接规则并激活那个规则集合。

释放连接规则
Firewall 现在由系统设定规则保护。

列示当前连接规则
可以看见最近生成的连接规则设置。如果以前停用了规则，那么现在将不使用它们。

验证规则生成
创建的规则是有效或无效的。

启用连接规则记录
Firewall 记录了所选择的通信至防火墙日志设施中。

禁用连接规则记录
停止 Firewall 记录。

出现**连接激活**对话框，如第43页的图 16 中所示。

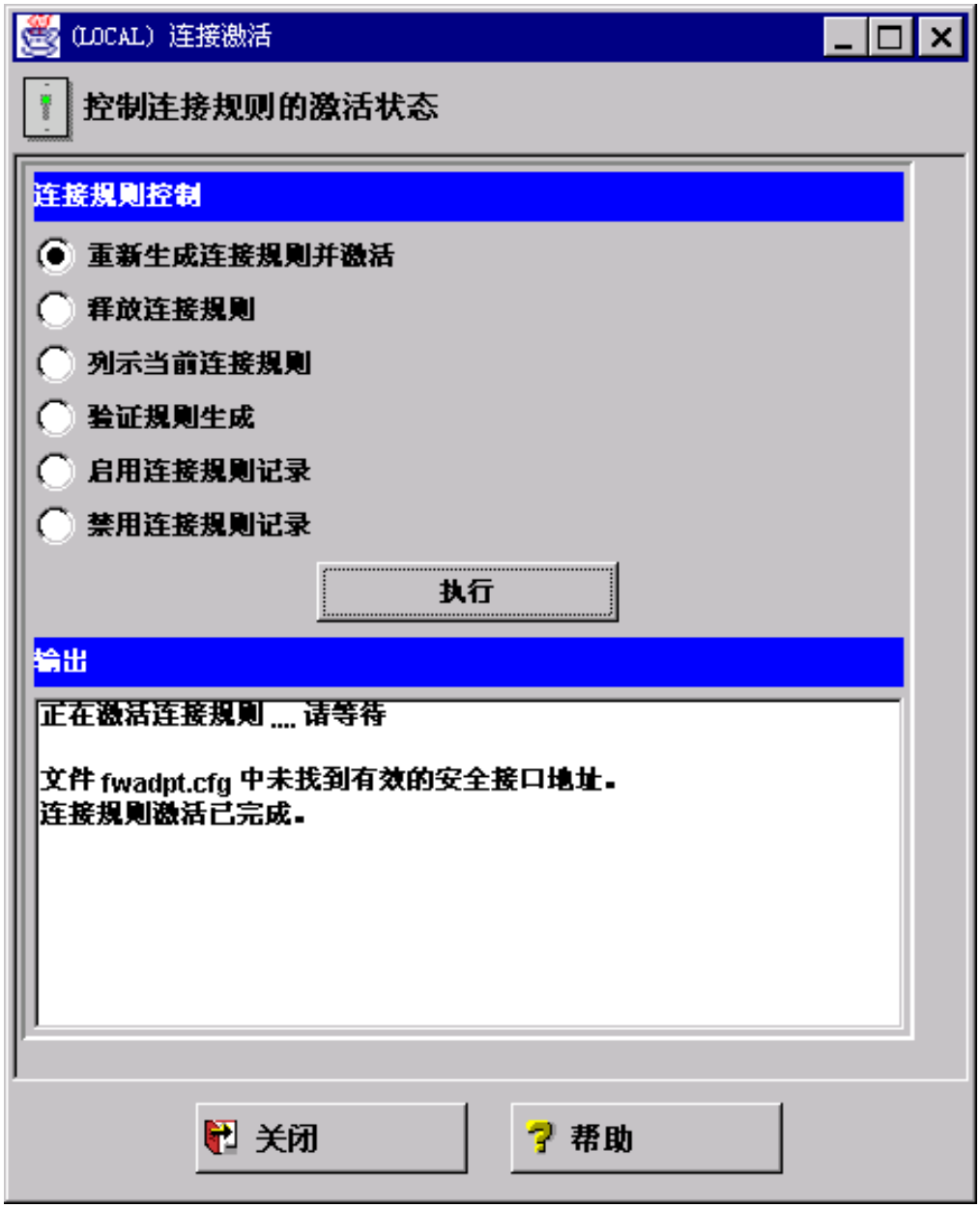

图 16. 连接激活

在进行选择以后，单击**执行**。

当重新生成并激活连接规则时的样本日志输出

以下为当重新生成并激活连接规则时的日志输出的一个样本。

```
Feb 03 13:46:53 1998 mr16n18: ICA9037i: Firewall interfaces being updated
automatically on Tue Feb  3 13:46:53 1998.

Feb 03 13:46:55 1998 mr16n18: ICA1032i: Filter rules updated at
13:46:55 on Feb-03-1998

Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 eq 53 both local both l=n f=y t=0 e=none a=none
```

```
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp gt  1023 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 gt  1023 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:4 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp     gt  1023 eq 25 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:5 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp/ack eq  25 gt 1023 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:6 permit 9.67.144.49 255.255.255.240
9.67.130.154 255.255.248.0 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:7 permit 9.67.130.154 255.255.248.
0 9.67.144.49 255.255.255.240 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:8 permit 9.67.144.49 255.255.255.240
9.67.131.250 255.255.255.255 tcp     gt  1023 eq  21 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:9 permit 9.67.131.250 255.255.255.255
9.67.144.49 255.255.255.240 tcp/ack eq  21 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:10 permit 9.67.131.250 255.255.255.
255 9.67.144.49 255.255.255.240 tcp     eq  20 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:11 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp/ack gt  1023 eq  20 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:12 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp     gt  1023 gt  1023 secure local inbound
l=n f=y t=0 e=none a=none
.
.
.
Feb 03 13:46:58 1998 mr16n18: ICA1037i: #:100 deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
all any 0 any 0 both both both l=y f=y t=0 e=none a=none
```

确定规则状态

IBM Firewall 规则可能处于以下状态之一:

1. 配置是不活动的。

   还没有使用配置客户程序来激活配置，或者已释放了配置。这是首次安装 IBM Firewall 并引导系统或释放过滤器规则时的配置状态。当首次安装 Firewall 时，有系统设定过滤器保护网络不受侵害。

   Firewall 访问:

   - 缺省过滤器配置允许所有本地入站通信和出站通信。

2. 配置是活动的，但有错误。

   已激活了配置。不是配置中有错误（非有效规则），就是什么也没有配置。错误和警告在“激活”输出窗口中显示。

   Firewall 访问:

   - 允许所有本地入站通信量。
   - 允许所有出站通信量。

3. 配置是活动的，而且是有效的。请注意，可能已经有了一些警告，很明显地重复过滤器规则。

   已激活了使用配置客户程序的通信量控制部分来定义的配置。

   注: 配置文件可能是有效的但仍然不包含任何规则。在这种情况下，起作用的是隐含的『拒绝所有访问』规则。

Firewall 访问:

- 访问由配置文件决定。

  检验了由任何网络接口接收的或将要由网络接口发送的每个包，其内容与生成的连接规则中的每个规则作比较。当找到一个匹配时，就执行对那个规则的操作（允许或拒绝）。
- 如果没有匹配数据报的规则，有一个拒绝访问的隐含的『拒绝全部』规则。

第9章 服务示例

本章描述如何配置 Firewall 执行特定的公共任务。列出的任务只是示例，但理解了这些例子后，您就可以配置自己的防火墙来使用所提供的任何服务了。

规划考虑事项

Firewall 的通信控制是按照连接来组织的，而连接定义了各对端点间允许或禁止的通信类型。因此，按照这些端点来计划您的连接是极为关键的。

如第39页的『第8章 控制通过 Firewall 的通信』中所描述的，网络对象代表到 Firewall 的端点。如果还没有这样做，应当完成在第5页的『第2章 规划』的网络规划工作表中列出的每件事并创建代表网络所必需的网络对象。

本章中的例子使用下列网络对象:

安全接口
Firewall 的安全接口。

非安全接口
Firewall 的非安全接口。

安全网络
通过 Firewall 的安全接口可访问的地址范围。这可能是一个包含几个不同域的网络对象组，每个域由自己的网络对象来表示。

The World
非安全网络。

每个期望的通信类型必须按照所涉及的端点至端点通信来查看。在这一阶段，要考虑您的防火墙是否将一直由代理提供这些通信，或者 Firewall 是否会路由这些通信。

如果防火墙作为代理，则它将以安全用户的身份执行必要的工作，而非安全主机将永远不会知道安全主机的存在。如果防火墙要路由通信量，则安全主机和非安全主机将直接通话。

如果使用 Firewall 作为代理，则通信的端点将包括防火墙，如第48页的图 17 中所示。

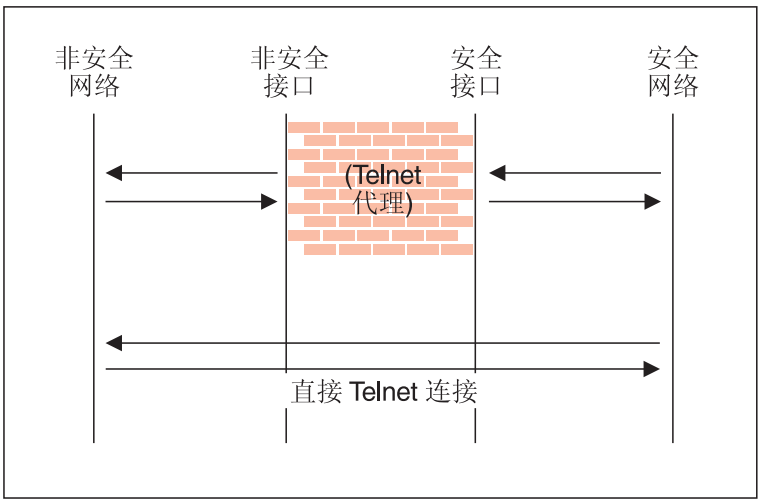

图 17. Telnet 代理和直接 Telnet 连接

Telnet 代理示例

第一个例子是直接出站 Telnet 代理连接。在该例中，允许安全网络上的用户使用防火墙的 Telnet 代理来访问非安全网络中主机上的 telnet 服务。

如第48页的图 17中所描述，发生了两个连接:

1. 安全网络中的客户程序与防火墙的 Telnet 代理连接。
2. 防火墙的 Telnet 代理以安全用户的身份与非安全网络中的主机连接。

要为这种通信配置 Firewall 的通信控制，我们需要设置两个连接:

表 1. Telnet 代理

源对象	目标对象	所需的服务
安全网络	安全接口	Telnet Proxy out 1/2
非安全接口	The World	Telnet Proxy out 2/2

过滤的 Telnet 示例

将上例与一个简单的经过过滤的 telnet 连接对照。在这种情况下，安全一方的客户机将与非安全一方的主机进行直接连接。

表 2. 经过过滤的 Telnet

源对象	目标对象	所需的服务
安全网络	The World	Telnet direct out

如前所述，在安全客户程序连接到非安全主机时，该配置将公开安全客户程序的地址。

代理 HTTP 示例

大多数安装希望允许在他们的安全客户程序中至少有一些可以在网络上冲浪。 IBM Firewall 提供预先定义的 HTTP 出站直接服务以允许路由的 HTTP，其功能恰如经过过滤的 Telnet 示例。除此之外，Firewall 还提供 HTTP 代理。

HTTP 协议与 Telnet 不同，因为 HTTP 可以封装其它的协议。甚至对于简单的冲浪，大多数用户不仅需要 HTTP，还需要 FTP 服务。要提供全系列的 HTTP 功能，还应该允许 Gopher 和 WAIS，尽管这些协议很少用到。

注意，即使在使用这些附加协议时，它们还封装在客户程序和代理之间的 HTTP 中。因此通信会与 第49页的图 18图中相似。

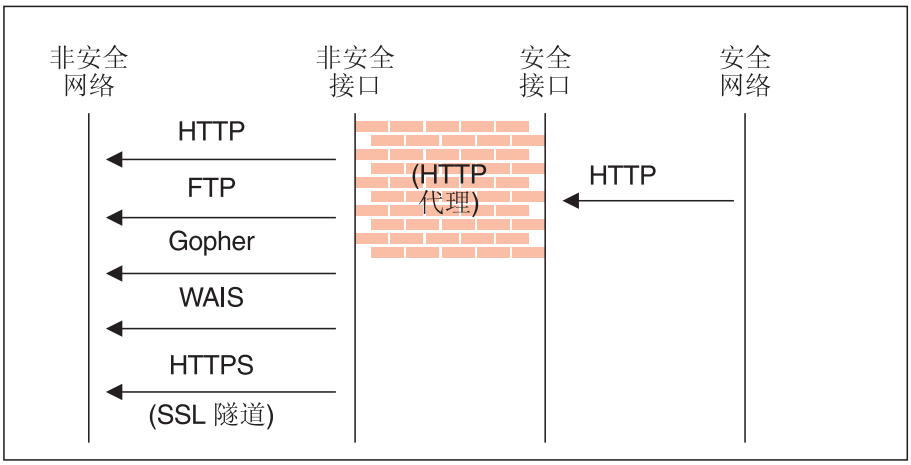

图 18. 代理 HTTP

因为涉及到两对端点，必须为两个连接编码。

表 3. 代理 HTTP

源对象	目标对象	所需的服务
安全网络	安全接口	HTTP proxy outbound 1/2
非安全接口	The World	从中选择... • HTTP proxy out 2/2 • FTP proxy out 2/2 • Gopher proxy out 2/2 • WAIS proxy out 2/2 • HTTPS proxy out 2/2

如需有关 HTTP 代理的更多信息，请参阅第81页的『第13章 配置代理服务器』。

Socks 示例

Socks 提供了一个与 HTTP 代理类似的口令查询，其中 socks 精灵程序处理许多不同的协议并将其封装入 Firewall 和客户程序间的单个数据流中。 Socks 比 HTTP 代理更为灵活，因为它可以容纳任何面向 UDP 和 TCP 的协议，并且防火墙可以独立于过滤器进行配置，以便进一步控制通信。

因为添加了这种灵活性，配置 socks 除了需要我们用 HTTP 代理演示的连接之外，还需要第三个连接。这两个基本连接允许包流入或流出 Firewall；第三个连接用于告诉 socks 精灵程序，一旦接收到包就代理这些请求。

表 4. Socks

源对象	目标对象	所需的服务
安全网络	安全接口	Socks 1/2
非安全接口	The World	从中选择... • HTTP proxy out 2/2 • FTP proxy out 2/2 • Telnet proxy out 2/2 （任何希望为之提供支持的下半个代理服务）
安全网络	The World	在 Socks 配置窗口中，选择... • 允许 socks 化的 HTTP • 允许 socks 化的 FTP • 允许 socks 化的 Telnet

当然，安全网络中的客户程序必须是经过 socks 化的并且必须配置成使用防火墙作为它们的 socks 服务器。

如需更多有关 Socks 的信息，请参阅第63页的『第11章 配置 Socks 服务器』。

DNS 的提示

如果不提供 DNS 解析，就不能进行有效的通信。对于有关配置 DNS 的细节，请参阅第27页的『第6章 处理域名服务』。不要忘记在安全性策略中启用 “允许 DNS 查询”。

非安全 Socks 客户程序的提示

安全性策略面板上有**拒绝至非安全接口的 Socks**。这种服务将拒绝任何从非安全接口寻址到 socks 精灵程序的包，将使您的防火墙安全得多。

如果要允许客户从非安全网络输入您的网络，您*必须不*选该校验框。

第10章 定制通信控制

本章将帮助定义过滤器规则和服务。 服务是一个规则集合或一个指令集合，用以允许或拒绝通过 Firewall 的通信量的特定类型，例如，一个 telnet 会话。可以用规则模板来创建新规则，再添加到服务中去。也可以删除服务。 Socks 服务适用于含有 socks 的连接。

IBM Firewall 预装有一套系统设定服务集。可以为特殊需要定制任何预先定义的服务或创建新的服务。

使用配置客户程序来创建规则模板

使用该过程来向可用的规则模板列表添加新规则。

1. 从配置客户程序浏览树中选择“通信量控制”然后双击文件夹图标。选择**连接模板**并然后选择**规则**。
2. 在**规则列表**对话框中，双击**新建**。

   IBM Firewall 显示一个**添加 IP 规则**对话框，如第52页的图 19 所示，这样就可以定义一个规则。

图 19. 添加 IP 规则

3. 输入规则名称。
4. 输入规则说明。该字段是任选的。
5. 单击操作箭头来选择允许或拒绝到 Firewall 的访问。
6. 单击协议箭头并从以下列表中选择:

   all 任何协议都将匹配该规则。

   tcp 信息包协议必须是传输控制协议（TCP）以匹配该规则。

tcp/ack
信息包协议必须是经确认的 TCP 以匹配该规则。

udp 信息包协议必须是用户信息包协议（UDP）以匹配该规则。

icmp 信息包报协议必须是网际控制报文协议（ICMP）以匹配该规则。

ospf 信息包协议必须是开放的最短路径第一协议（ospf），从而匹配该规则。当把 ospf 指定成协议，则源端口操作和源端口值被用于 ospf 记录类型值。过滤也能够在 ospf 类型上执行。可以指定一个 **any** 的类型值，但同时目的端口字段必须指定为 **any 0**。而其它的将被忽略。

ipip 信息包协议必须是 IP-in-IP 协议（IPIP）以匹配该规则。当指定了 IPIP 时，端口字段必须指定为 **any 0**。

esp 信息包协议必须是封装安全性协议以匹配该规则。该协议由虚拟专用的网络所使用，用于发送 IP 信息包。

ah 认证首部协议是由虚拟的专用网络所使用的信息包协议，它用于发送具有相关认证令牌的 IP 信息包。

7. 数值型协议允许通过使用它的十进制值（根据 RFC-1700）来指定一个协议。有效值范围从 1 至 252。请注意，在使用该选项时，该规则的端口字段必须被指定为 0（指定任何端口）。请参阅 RFC-1700 以获得所有协议的列表。或者，可使用浏览器直接访问 Internet 分配的号码权限（IANA）。
8. 运算和端口号操作数要一起使用。源和逻辑运算说明了用于信息包的端口号（目的地或起始地）和源端口（port#）以及目的端口（port#）操作数之间的关系。例如，如果信息包目的地端口为端口 20 且目的操作和目的端口（port#）为 『ge 15』，则信息包匹配。（20 大于或等于 15）。

   如果使用了一个带有**任何**值的源操作或目的地操作，则过滤器就不会看端口号；任何端口将匹配。端口号在这种情况下无法更改。

   对于 ICMP 协议来说，并不需要指定一个源端口而是要指定一个 ICMP 类型，并且在目的地端口处指定一个 ICMP 代码。指定的逻辑运算符被用于类型或代码，而对于端口来说，一个 any 运算符意味着任何类型和/或代码值都将匹配该规则。端口号在这种情况下无法更改。

   操作的值为:

   - 任何（Any）
   - 等于（Equal to）
   - 不等于（Not equal to）
   - 小于（Less than）
   - 大于（Greater than）
   - 小于等于（Less than or equal to）
   - 大于等于（Greater than or equal to）

   这里是一些需要保护的比较重要的端口。端口号的值必须在 1 到 65535 范围内:

   端口 使用

   20 FTP 数据

   21 FTP 控制

   23 Telnet

25 邮件

53 域名服务器

70 Gopher

80 HTTP

111 RPC

161 SNMP

1080 socks

这里是一些 ICMP 类型和代码:

类型 **代码和说明**

0 0 - Ping 回答

8 0 - Ping 请求

3 1 - 主机无法到达

3 3 - 端口无法到达

5 1 - 主机重定向

9. 单击**接口**箭头来选择接口（适配器）的类型。

   两者 用于在安全或非安全接口上来往的信息包。

   安全 用于在安全接口上来往的信息包

   非安全 用于在安全或非安全接口上来往的信息包。

   特定 如果已赋值了名称给接口，则当选择一个接口时，请使用接口名称字段。

10. 如果为该接口类型选择“特定”，则特定接口的名称将出现在名称字段中。
11. 单击所期望的传递:

    两者 用于所有通信量。

    本地 暗示信息包位于防火墙主机。这说明:

    - 入网的本地信息包是由接口来接收的，而且是为该防火墙主机而指定的；它们不会被传递至另一个主机。它们的目的地是本地。
    - 出网的信息包是从接口中发送的，但它是源自防火墙主机。它们的起始地是本地。

    路由 暗示信息包是由防火墙主机传送的。这说明:

    - 入网的本地信息包是由接口来接收的且目的地是其它一些主机的信息包；它们不会留在 Firewall 上。它们的目的地是远程。
    - 出网的信息包是从接口中发送的，但它源自其它一些主机。它们的起始地是远程。

12. 单击所期望的方向:

    两者 用于进出于所选接口的包

    入站 用于从网络进入所选择接口的包

    出站 用于从选中接口输出到网络的包

13. 如果对日志控制字段选择“是”，则每个匹配那个规则的信息包都将以错误的优先级记入防火墙日志。如果没有指定该参数，缺省值为“否”。

14. 单击**片段控制**箭头以选择期望的片段控制。为使 IP 包信息与一个规则片段控制规范相匹配，则该控制的解释如下:

    是 该规则将匹配片段首部、片段和非片段。对于片段来说，将忽略端口信息且假设它是匹配的。

    仅 只有片段和片段首部能够匹配。对于片段首部，端口信息必须匹配。对于片段，将忽略端口信息。

    否 只有非片段可以匹配。片段首部和片段都被该参数排除在外。

    首部 只有非片段和片段首部才能够匹配。片段被该参数排除在外。

    如果没有指定该参数，则对于“允许”规则和“拒绝”规则的缺省值都为“是”。

    注: 无论该控制的设置如何，带有一个一（1）偏移量的 IP 片段都将被废弃。该操作消除了一个使用包片段来覆盖 TCP 首部标志的已知攻击。

为使一个包首部与一个已定义的 IP 规则相匹配，则包信息必须与所有在编码规则中指定的参数相匹配。对于包片段，除端口信息以外的所有参数被用于确定一个匹配。

如果以前的规则（用“是”或“仅”编码）不允许片段，则总是附加在规则文件的底部的最后的规则将拒绝信息包片段。

更改 IP 规则配置项

要修改一个已经创建的 IP 规则:

1. 在**规则列表**中一个现存的规则上双击。出现**修改 IP 规则配置**对话框。
2. 如第51页的『第10章 定制通信控制』中所描述的那样，修改适当的字段，并单击**确定**以应用这些更改。

删除规则配置项

要删除一个规则，从**规则列表**中选择一个规则并单击**删除**。

预定义服务

IBM Firewall 预装有一套系统设定服务集。 服务是一个规则集合或一个指令集合，用以允许或拒绝通过 Firewall 的通信量的特定类型，例如，一个 telnet 会话。可以用规则模板来创建新规则，再添加到服务中去。

预装的缺省服务是:

All non-secure
拒绝所有通信通过非安全接口

All permit
允许所有的通信（只用于调试目的）

All permit, in one direction
允许所有的通信（只用于调试目的）

All secure
拒绝所有通信量通过安全接口（在违反安全性的情况下）

All shutdown
拒绝所有的包（关机或调试）

Anti 电子欺骗
拒绝带有安全源地址的入站非安全包

Broadcasts
拒绝广播信息到非安全接口

Config Client non-secure
允许使用来自非安全网络的配置客户程序

Config Client secure
允许使用来自安全网络的配置客户程序

CU-SeeMe
在缺省端口 7649 和 7648 上的 CU-SeeMe 视频

DNS queries
（安全性策略） 允许 DNS 查询

DNS transfers
允许 DNS 区传送（用于次级名称服务器）

Domain Controller Authentication
对于用户认证允许域控制器的使用

FTP proxy in 1/2
允许非安全网络到 Firewall 的 FTP 入站

FTP proxy in 2/2
允许 Firewall 到安全网络的 FTP 入站

FTP proxy out 1/2
允许安全网络到 Firewall 的 FTP 出站

FTP proxy out 2/2
允许 Firewall 到非安全网络的 FTP 出站

Gopher proxy in 2/2
允许 Firewall 到安全网络的 gopher 入站

Gopher proxy out 2/2
允许 Firewall 到非安全网络的 gopher 入站

HTTP deny non-secure
拒绝至非安全接口的 HTTP

HTTP direct out
允许直接从安全网络到非安全网络的 HTTP

HTTP proxy in 2/2
允许 Firewall 到安全网络的 HTTP

HTTP proxy out 1/2
允许安全网络到 Firewall 的 HTTP （端口 8080）

HTTP proxy out 2/2
允许 Firewall 到非安全网络的 HTTP

HTTPS direct out
允许安全网络到非安全网络的 HTTPS （SSL）

HTTPS proxy out 2/2
允许 Firewall 到非安全网络的 HTTPS （SSL 隧道）

IDENTD
允许带有 Socks 协议的用户标识（用户 ID）

Mail （安全性策略） 允许通过 Firewall 的邮件通信

NetBT Name Services broadcasts
允许 TCP/IP 上的 NetBIOS 名称服务广播

Ping 允许 Ping 将安全网络出站到任何地方

SDI authentication
允许连接到安全网络中的 SecurID ACE 服务器

Socks 1/2
允许安全网络到 Firewall 的 Socks 使用

Socks deny non-secure
拒绝从非安全适配器来的 Socks

Socks in 1/2
允许非安全网络到防火墙的 Socks 使用

Telnet direct out
允许安全网络到非安全网络的 Telnet 出站

Telnet proxy in 1/2
允许非安全网络到 Firewall 到 Telnet 入站

Telnet proxy in 2/2
允许 Firewall 到安全网络的 Telnet 入站

Telnet proxy out 1/2
允许安全网络到 Firewall 的 Telnet 出站

Telnet proxy out 2/2
允许 Firewall 到非安全网络的 Telnet 出站

VDOLIVE Direct In
允许至安全服务器的非安全客户程序

注意，用户必须配置个别的游戏者为仅使用 UDP 端口 7001。

VDOLIVE Direct Out
允许至非安全服务器的安全客户程序

WAIS proxy in 2/2
允许 Firewall 到安全网络的 WAIS（z39.50）

WAIS proxy out 2/2
允许 Firewall 到非安全网络的 WAIS（z39.50）

定义服务

在已经定义了规则后，需要将规则添加至一个服务。从配置客户程序浏览树中选择通信控制并在连接模板上双击，然后选择“服务”。出现服务列表对话框。双击“新建”以获得添加服务对话框，如第59页的图 20 所示。


(LOCAL) 添加服务
添加服务
标识
服务名：
说明：
服务组合
规则对象
流向
名称
选择...
删除
上移
下移
流向
服务覆盖值
覆盖日志控制：
不覆盖
覆盖片段控制：
不覆盖
覆盖隧道 ID：
选择...
时间控制
按每天的时间控制
开始：
结束：
按日期控制：
星期
开始：
日
结束：
日
时间控制操作：
在指定时间内激活服务
在指定时间内释放服务
确认
取消
帮助

图 20. 添加一个服务

使用配置客户程序创建服务

1. 输入服务名称。
2. 输入一个说明。
3. **覆盖日志控制**字段提供了一种方法，用以覆盖在已选中用于该服务的规则模板中日志控制的设置。例如，如果包括了一个规则模板的集合，其日志控制设置为“否”，就可以将该设置覆盖成“是”以满足该服务的需要。覆盖设置将在该服务中的所有规则上起作用。在**覆盖日志控制**字段中，输入下列选项之一:
   - 不覆盖 - 已关闭覆盖，在规则的设置选项仍然适用
   - 是 - 当匹配该服务中的任何规则时，写入一个日志记录。
   - 否 - 当匹配该服务中的任何规则时，不写入日志记录。

   当为一个过滤器规则写一个日志记录时，在日志记录中所显示的值都是 IP 信息包中的实际值。日志匹配的过滤器规则可以提供有价值的信息，这些信息是关于由 Firewall 所参照的 IP 信息包的内容，例如，实际协议和端口号。
4. **覆盖片段控制**字段提供了一种方法，用以覆盖在已选中的用于该服务的规则模板中片段控制的设置。例如，如果包括了一个通常含有片段的规则模板，就能将该设置覆盖成“是”以满足该服务的需要。覆盖设置将在该服务中的所有规则上起作用。在覆盖片段控制字段中，输入下列选项之一:
   - 不覆盖 - 已关闭覆盖，在规则的设置选项仍然适用
   - 是 - 匹配任何 IP 信息包，例如，非片段、片段首部以及不带首部的片段
   - 否 - 仅匹配非片段信息包，不匹配片段首部或不带首部的片段
   - 只有 - 仅匹配片段首部和不带首部的片段，不匹配非片段
   - 首部 - 仅匹配非片段和片段首部，不匹配不带首部的片段
5. 时间控制允许将一个时间范围与每个服务相关联。所以，该服务将只在一个指定的时间周期内有效。如果服务没有时间规范，则那个服务在任何时间都有效。

   按每天的时间控制

   如果要根据一天中的开始和结束时间来激活或释放该服务，就选择它。使用 24 小时制格式。如果没有启用该字段，则“每天的时间”字段将每天 24 小时都有效。

   按日期控制

   如果要根据基于星期的天数或日期的计划来激活或释放该服务，就选择它。请注意，一项服务是激活的还是释放的，取决于时间控制操作字段中的值。

   时间控制操作

   如果要该服务在指定时间内被激活，就选择**在指定时间内激活服务**。该服务将在超出指定时间范围时被释放。

   如果要该服务在指定时间内被释放，就选择**在指定时间内释放服务**。该服务将在超出指定时间范围时被激活。
6. 单击**选择**来选择包括该服务的规则。
7. 使用流动双向开关来确定写入规则库文件时，连接的源和目的值将如何赋值给过滤器。

---> 左到右表明在写入规则库文件时，连接的源和目的文件直接写入规则。

<--- 右到左表明在写入规则库文件时，连接的源和目的反向。

8. 当接收包时，IBM Firewall 将包中的信息和规则配置文件（在文件顶部启动）中的规则相比较。当找到第一个匹配时，它将停止比较，并执行规则中的操作。

   一旦将一系列规则添加到服务中去，就可以更改它们的次序。从**服务对象**列表选择一个规则并单击**上移**或**下移**按钮来重新定位规则。或者可以通过单击**删除**来删除一个规则。配置客户程序显示了一个规则的刷新列表。单击**确认**来保存更改。

第11章 配置 Socks 服务器

Socks 是电路层网关的一种 Internet 标准。 如果应用程序使用了 TCP，例如 Web 浏览器、FTP 或 Telnet 应用程序，那么您可以使用 Socks 服务器进行地址转换。Socks 能帮助您访问 Internet，同时隐藏内部的 IP 地址。

对于出站请求，从安全客户程序到非安全服务器，Socks 服务器与代理服务器有相同的目的：在 Firewall 上断开会话并提供安全门，允许用户从这里访问外部的、非安全网络，而同时保护内部网络的寻址方式和网络结构。Socks 服务器对用户来说具有简单的优势，很少有额外的管理性工作。

Socks 服务器能拦截那些跨越内部网络和 Internet 的所有出站 TCP 请求。 Socks 服务器提供远程应用程序接口以便在安全范围内由客户程序执行的功能可以通过防火墙工作站上的安全服务器，从而隐藏客户的 IP 地址。访问是由与 Socks 规则相关联的过滤器控制的。

Socks 服务器与代理服务器类似。但是代理服务器在 Firewall 上执行了 TCP/IP 功能，而 Socks 服务器只是对用户进行标识然后通过 Firewall 来重定向功能。事实上 TCP/IP 功能是在客户工作站上执行的，而不是在防火墙上。它节省了在 Firewall 上作的处理。在安全网络中的用户能使用支持 Socks 标准的多种 TCP/IP 产品。 图 21 说明 Socks 服务器截取来自安全网络内部的客户程序的 HTTP 请求。

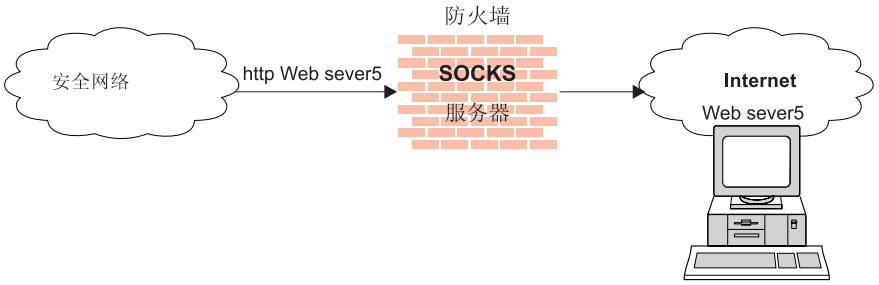

图 21. Socks 服务器

Socks 服务器有效地对外部世界隐藏了内部的 IP 地址。

IBM Firewall 提供了 Socks 协议版本 5，它使在安全网络内的客户能在访问非安全网络中的应用程序以前经过一个认证阶段。对于认证的类属代理及一些流型声频和视频的协议，它也一样提供。

Socks 精灵程序象 Windows NT 服务一样，自动在启动系统时启动。另外，提供了一个监视代理，允许服务器的监视。可以手动启动监视代理。

IBM Firewall 提供了一个平滑的迁移路径，由三个认证概要组成，因此用户在引入 Socks 协议 5 客户的同时可继续在使用已安装的 Socks 协议版本 4 客户。

1. 最宽容的概要不允许出站认证，而它允许任何用户，（无论是使用 Socks 版本 4 还是 Socks 版本 5 客户程序来连接的）。在这种情况下，将拒绝入站连接。
2. 迁移概要允许 Socks 协议版本 4 用户不经认证地通过，但需要 Socks 协议版本 5 用户被认证。拒绝入站 Socks 协议版本 4 连接，并且需要入站 Socks 协议版本 5 连接来认证。这是缺省概要。

3. 最安全概要需要所有的用户使用 Socks 协议版本 5 客户程序并提供有效的认证。

当安装了 Firewall 后，启用 socks 服务器，但在 socks 配置文件中没有规则。对于要使用 Socks 服务器的 Socks 客户程序，必须使用配置客户程序来配置 Socks。 请参阅第50页的『Socks 示例』以获得如何设置 Socks 服务的示例。

Socks 协议版本 5 服务器支持的协议

Socks 协议版本 5 服务器支持以下 TCP 和 UDP 协议以及其它许多协议:

- Archie
- Finger
- FTP
- Gopher
- HTTP
- HTTP 代理
- News
- SNMP
- Telnet
- TFTP
- RealAudio
- RealPlayer
- Whois
- X-Windows

另外，支持大多数电子邮件客户。对这些协议的支持取决于它们实际的实现。

使用配置客户程序配置 Socks 服务器

Socks 模板是通过控制 Socks 服务器的安全性规则。 socks 模板允许定制、添加到、复制或删除已存在的 socks 模板。这些模板，可依次地用于 Firewall 连接的定义中（相同于规则模板使用的方法）。

添加新的 Socks 规则

要使用配置客户提供的模板添加规则到 socks 配置文件中，在配置客户导航树中选择通信量控制（Traffic Control）。双击文件的文件夹图标以展开该视图。选择连接模板。双击文件的文件夹图标以展开该视图。选择 **Socks**。出现 **Socks** 对话框。

1. 双击**新建**来添加一个新的 socks 模板。

   出现**添加 Socks 规则**对话框，如第65页的图 22 中所示。

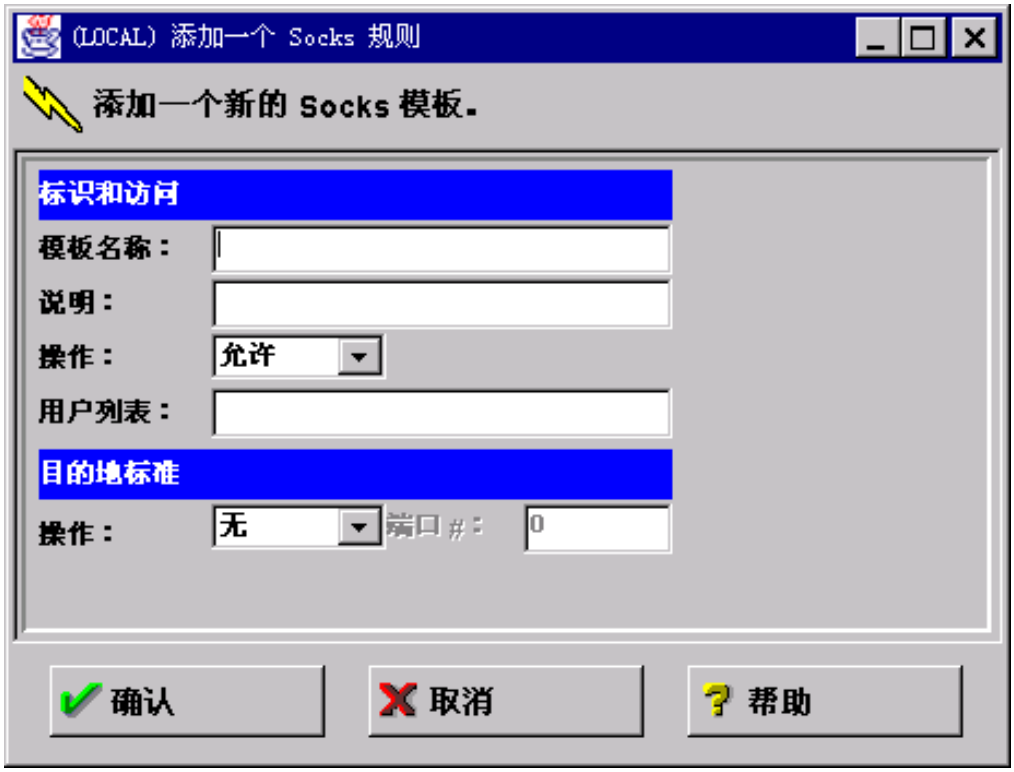

图 22. 添加 Socks 规则

2. 在**模板名称**字段，输入 Socks 项的名称。该名称必须是唯一的且不应该包含那些作为文件定界符的管道符号（|）、单引号（或撇号）字符（'）或双引号（″）字符。这些字符的使用将导致产生不可靠的数据。
3. 填入说明。
4. 单击操作箭头来选择允许或拒绝从源到目的地的访问。

   当数据报进入 Socks 服务器时，该服务器将数据报规范与配置文件的每一个规则相比较（从第一个规则开始），直到发现完全匹配的规则为止。然后它停止搜索并执行该规则上的适当的操作（允许或拒绝访问）。如果没有发现匹配，则自动拒绝访问。
5. 在**用户列表**字段中，可以输入一个用户 ID、一个用户 ID 的列表、一个文件名或一个文件名的列表。 如果输入一个列表，则用逗号将各项分开。不要在用户列表中使用空格、制表符、管道符号（|）或双引号（″）。
   - 用户列表限于 396 个字符。
   - 用户 ID 必须是在请求主机上的用户 ID，而不是在目的地主机或 Socks 服务器上的。
   - 用户 ID 可包含 1 到 8 个字符，包括:
     - a 到 z
     - A 到 Z
     - 0 到 9
     - _（下划线）
6. 用户 ID 不应该包含下列字符: 管道符号（|）和双引号（″）。

7. 如果使用文件名，它们必须是全限定的（即以 “/” 开头，防止将它们认为是用户 ID）。每个文件可包含用户 ID 的列表，每行中有一个或多个，用逗号分开，并且可任选地包含用 “#” 字符定界的注解。整个注解行 - 即那些已 # 号开始的。在该文件中的每一行可以是长达 1023 字符，它必须由一个 “newline” 字符终止。
8. 在**操作**字段中，输入将在端口号上执行的逻辑运算:

   eq 等于（Equal to）

   neq 不等于（Not equal to）

   lt 小于（Less than）

   gt 大于（Greater than）

   le 小于等于（Less than or equal to）

   ge 大于等于（Greater than or equal to）

   当和端口号一起使用时，逻辑运算建立了一种必须满足的关系。例如，如果输入操作 gt 和端口号 23，则对于要调用规则的端口号必须大于 23。
9. 在**端口 #** 字段中，输入端口号。端口号与操作一起使用以建立必须满足的关系。例如，如果输入操作 gt 和端口号 23，则对于要调用规则的端口号必须大于 23。如果省略操作和端口号，规则适用于所有的目的端口号。

使用**添加 Socks 规则**对话框允许或拒绝防火墙对基于 IP 地址的网络主机的访问。

修改 Socks 规则

1. 在 **Socks** 对话框上的一项上双击。

   出现**修改 Socks 规则**对话框。
2. 按如第64页的『添加新的 Socks 规则』中描述的那样更改适当的字段，并单击**确认**。

删除 Socks 规则

从 **Socks** 对话框中选择一项并单击**删除**。系统会询问是否确实想要删除该 Socks 规则。单击**确认**来删除规则。

激活连接规则

因为有了过滤器规则，需要激活 Socks 规则。 单击配置客户程序浏览树上的**连接激活**，选择**重新生成连接规则并激活**然后单击**执行**。

Firewall 将规则从 Socks 配置文件复制到防火墙规则，然后激活该规则。当激活规则时，新规则记录到防火墙日志文件中。

Socks 的样本日志输出

以下为 Socks 的日志输出的一个样本。

```
Feb 03 13:46:20 1998 mr16n18: ICA3123i: Sockd server starting
Feb 03 13:47:31 1998 mr16n18: ICA3010i: Session start
Feb 03 13:47:31 1998 mr16n18: ICA3011i: Session start
Feb 03 13:49:15 1998 mr16n18: ICA3007i: Too many threads
Feb 03 13:58:31 1998 mr16n18: ICA3015i: Session termination
```

使用 Socks 服务器的客户程序考虑事项

大多数 Web 浏览器都经过 Socks 化（soksified），并且可以获得大多数平台的 Socks 化的堆栈。其它 TCP/IP 应用程序 Socks 化的客户程序可从许多资源上获得。 如需 Socks 实现的特定客户程序，请参考该客户程序文档。如需附加信息，请参考:

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

http://www.socks.nec.com

Socks 服务器式连接

Socks 服务器式连接是一个功能，通过它一个 Socks 服务器可驻留在另一个 Socks 服务器后，仍允许对在最外面 Socks 服务器边的网络进行访问。 (它可被认为是 Socks 化一个 Socks 服务器)。这是非常有用的局域网方案。

要与 Socks 服务器一起建立 Socks 服务器式连接，编辑 `socks5.header.cfg` 文件。该文件驻留在 Firewall 的 `config` 子目录中。添加以下项:

- 一个 *no proxy* 命令 - 指示您的 Firewall 直接存取哪一个子网
- 一个 *socks4* 命令 - 指示通过 SOCKS 协议版本 4 服务器可存取的子网
- 一个 *socks5* 命令 - 指示通过 Socks 协议版本 5 服务器可存取的子网

例如，考虑以下网络。研究部门有一个小型的专用网络， *q.private.com*，在它们自己的防火墙后面。研究部门的子网是 10.007.007.0/255.255.255.0。公司的专用网包括，*private.com*，包含了整个 10.0.0.0/255.0.0.0 网络。公司的 Socks 协议版本 4 服务器，*socks.private.com*，提供了对互联网的访问。

在研究部的 Socks 服务器，*socks.q.private.com* 上，将以下两行添加至 `socks5.header.cfg`。

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

最后，添加一个通信控制连接以允许 *socks.q.private.com* 与 *socks.private.com* 通信。这可能已由一个更常规的服务完成。添加一个源是 *q.private.com* Firewall 的非安全接口，目的地是 *socks.private.com*，并且包含 *Socks Proxy-Chaining* 服务的连接。然后重新激活您的通信控制规则。

第12章 管理防火墙上的用户

本章描述了如何用 IBM Firewall 来执行日常的管理任务，包括:

- 将用户添加至 IBM Firewall，以便他们可以访问在受保护的网络之外的主机。
- 更改访问防火墙的用户的属性
- 删除不再需要访问外界网络的用户

不要直接编辑配置文件；否则，IBM Firewall 用户属性将无法正确设置。用配置客户程序对话框或命令行来进行所有 IBM Firewall 的管理。

将用户添加至 IBM Firewall

IBM Firewall 定义了三种类型的用户，并将有关他们的信息存储在两个不同的用户数据库中。

用户类型

IBM Firewall 将用户分成三类:

代理用户

使用防火墙服务（如 HTTP 代理服务）来从公司网络访问 Internet 上的网络站点。代理用户能够使用通过防火墙的服务，但是他们不能访问防火墙机器，并不能执行对 Firewall 机器的本地注册。

防火墙管理员

能够使用 Firewall 代理服务，但是也能够通过使用配置客户程序和从远程主机注册到 Firewall 来配置 Firewall。如同代理用户一样，防火墙管理员不能执行到 Firewall 机器的本地注册。

防火墙管理员能够为用户创建并修改定义，但是不能创建或修改其它防火墙管理员的定义。

主防火墙管理员

与防火墙管理员拥有相同的能力。他们也能够执行对 Firewall 机器的本地注册。主防火墙管理员能够创建并修改其它防火墙管理员的定义。

数据库的类型

用户数据库有两类。

防火墙用户数据库

包含了每个代理用户和管理员的防火墙相关属性。包括的属性如用户防火墙口令、口令规则以及应该使用哪种认证方法来认证用户的每个服务。

若代理用户不在防火墙用户数据库中定义，且用户试图使用防火墙代理服务，则将使用系统设定的用户记录 `fwdfusr`，以定义用于验证用户的属性和认证方案。

主防火墙管理员不能在防火墙用户数据库中定义。使用系统设定的防火墙管理员记录 `fwdfadm`，以将属性指定为管理员。

如同代理用户，如果防火墙管理员也在 Windows NT 用户数据库中定义，则若用户请求必须使用 Windows NT 注册口令的任何认证时，将使用其 NT 注册口令。

Windows NT 用户数据库

包含用户的 NT 注册口令。一般地，不必在 NT 用户数据库中定义代理用户，除非他们准备使用他们的 NT 注册口令来认证。

如果要使用其它认证方法来认证代理用户，则在 Windows NT 用户数据库中不必定义他们。

主防火墙管理员与 Windows NT 用户是同义的，这些 Windows NT 用户是 NT 管理员组中的成员，并必须在 Windows NT 用户数据库中定义。

使用配置客户程序添加用户

将用户添加至 IBM Firewall，并授予他们访问外部网络的权力。

1. 从配置客户程序浏览树中选择“用户”。显示**用户管理**对话框。
2. 从**用户管理**对话框中选择**新建**并单击**打开**。出现**添加用户**对话框，如第71页的图 23 中所示。

图 23. 添加用户

3. 提供以下信息:

权限级别

为该用户指定权限级别。单击**权限级别**箭头来选择用户类型。

Socks/代理用户

正在定义的用户是用于 Socks 服务器访问和代理服务器访问的。用户没有管理权限。这是系统设定值。

防火墙管理员

拥有用户的所有属性，但是管理员也可以注册入 Firewall 并执行管

理任务。管理员有附加的属性，该属性定义了允许管理员所能执行的管理功能。防火墙管理员能够创建防火墙用户，但是不能创建其它防火墙管理员。 Firewall 管理员不能本地注册到 Firewall 机器。他们必须从远程机器访问配置服务器。

主防火墙管理员

允许主防火墙管理员本地注册到 Firewall 机器。他对所有的管理功能都有全部访问权。他也能够创建除了防火墙管理员的其它防火墙管理员。

通过创建一个 NT 数据库中的用户，并使该用户成为 NT 管理员组中的一员来定义主防火墙管理员。修改 fwdfadm 记录，以定义主防火墙管理员的属性。

用户名 为该用户指定名称。这是在 IBM Firewall 上向 telnet 或 FTP 服务器进行注册时使用的用户名。不一定要是用户的 TCP/IP 用户名或主机名，但它们可以是相同的。

用户名可由 1 至 20 个字符构成，包括:

a 到 z

A 到 Z

0 到 9

_（下划线）

用户名不分大小写。

Firewall 带有两个预先安装的用户:

a. 系统设定的用户或 fwdfuser。若用户未在防火墙数据库中定义，则使用 fwdfuser 来确定用户的防火墙属性，诸如，认证用户时所使用的认证方法。

   安装时，当创建了 fwdfuser 时，所有认证方法将设置为拒绝全部。fwdfuser 的许可权 控制防火墙处理未定义用户的方式。

   管理员可以使用配置客户程序或命令行来查看 fwdfuser 或更改指定的认证方法。不过，不能删除 fwdfuser 而且它必须始终存在于防火墙中。另外，防火墙口令和 SNK 不是 fwdfuser 的有效认证类型。详见 *IBM eNetwork Firewall 参考*大全。

b. 缺省的主防火墙管理员 fwdfadm，定义所有主防火墙管理员的防火墙属性。 因为主防火墙管理员在防火墙数据库中没有自己的记录，所以本记录用来定义用于认证主防火墙管理员的认证方法。

   安装时，fwdfadm 的所有认证方法都设置为*拒绝全部*，除了设置为 NT 注册口令的安全、非安全管理方法。主防火墙管理员能够查看并修改本记录，但是本记录不能被删除。另外，防火墙口令和 SNK 不是 fwdfadm 的有效认证类型。

用户全名

指定一个用户描述。

以下字段适用于认证方法。单击箭头以从认证方式列表中选择。在第74页的『用户认证方法』 中有对它们的说明。

安全 Telnet

表明在从安全网络中进行注册时，用户的身份是否必须用某些方法进行认证。

非安全 Telnet

表明在从非安全网络中进行注册时，用户的身份是否必须用某些方法进行认证。

安全 FTP

指定该用户需要用 FTP 来从安全网络访问 Firewall 的认证级别。

非安全 FTP

指定该用户需要用 FTP 来从非安全网络访问 Firewall 的认证级别。

安全 Socks

指定来自防火墙安全方的 Socks 客户程序连接的 Socks V5 认证方法。单击箭头以从选项列表中选择。在第74页的『用户认证方法』 中有对它们的说明。

非安全 Socks

指定来自防火墙非安全方的 Socks 客户程序连接的 Socks V5 认证方法。单击箭头以从选项列表中选择。在第74页的『用户认证方法』 中有对它们的说明。

安全 HTTP

当出栈 HTTP 代理请求时，指定一个认证的用户 ID/口令类型。单击箭头以从选项列表中选择。在第74页的『用户认证方法』 中有对它们的说明。

浏览器为用户 ID 和口令作出提示，这样如果您正在使用 SDI，则在口令提示处填入密码。

用户供给必须注意，Socks/password 不能支持交互式对话框及相应行为。

安全管理

指定用于通过安全接口从配置客户程序进行注册的认证方式。请注意，当以本地方式进行注册时（通过在注册面板上选择“本地”），则始终处在安全环境下，所以这是您将要使用的认证方法。

非安全管理

指定用于通过非安全接口从配置客户程序进行注册的认证方式。

SecureNet Key

指定由一位拥有 AssureNet Pathways SecureNet Key 卡的远程用户输入的字符序列。输入将在密钥卡中加注的密钥代码。请参阅 SecureNet Key 信息获得关于选择和安装密钥代码的指示。

注:

a. 本字段不用于 SecurID 卡。

b. 必须为每个用户创建唯一的随机密钥。

c. 当在 SecureNet key 卡中安装密钥时，请使用 AssureNet Pathways 安装过程并选择**方式 5**。

请参阅第77页的『认证方法』以获取详细信息。

用户认证方法

用户认证的选项有:

拒绝全部

用户被拒绝访问。

允许全部

无需认证。

NT 注册口令

防火墙口令比 NT 注册口令更保险。但是，若用户已在 Windows NT 域中定义，则能够使用 Windows NT 注册口令，用户就不需要多个口令。

若选择该认证方法，将对照本地 Windows NT 用户数据库来认证用户 ID 和口令。若 Firewall 配置为信任其它 Windows NT 服务器，则将搜索这些受信任服务器中的用户定义。

在 Windows NT Firewall 和受信任的 Windows NT 服务器之间建立起信任关系之前，必须建立连接以在两台机器之间允许 TCP/IP 通信的通信。

使用下列预先定义的服务来设置该连接:

1. 域控制器认证 - 允许用户认证的域控制器的使用
2. NetBT 名称服务广播 - 允许 TCP/IP 上的 NetBIOS 名称服务广播

使用 Windows NT 配置实用程序，以定义信任关系。

SecureNet Key

使用 AssureNet Pathways SecureNet Key 来完成认证。

在 SecureNet Key 字段中，输入将在密钥卡中加注的密钥代码。

注:

1. 必须为每个用户创建唯一的随机密钥。
2. 随机密钥的 8 个八进制值中的每一个必须在 1-377 范围内。
3. 当在 SecureNet key 卡中安装密钥时，请使用 AssureNet Pathways 安装过程并选择**方式 5**。

请参阅第77页的『认证方法』以获取详细信息。

SecurID 卡

使用 Security Dynamics SecurID 安全卡或 pinpad 卡来完成认证。不要使用 SecureNet Key 字段。PIN 必须在对 IBM Firewall 使用认证方法之前设置。

对于 FTP 来说，不支持 SDI 新的 PIN 方式和下一个令牌方式。

请参阅第77页的『认证方法』以获取详细信息。

用户提供的认证 1、2 和 3

由用户提供的认证。在 Firewall 上，最多可以安装三种用户提供的认证方法。对于有关如何创建并编译用户提供的认证的子程序，请参阅 *IBM eNetwork Firewall 参考大全*。

Firewall 口令

必须提示用户，并由用户输入一个有效的口令。当完成该面板时， IBM Firewall 提示为这个新用户指定一个口令。

防火墙口令比 Windows NT 注册口令允许更多的安全口令和口令规则，所以建议这种口令选择。

要求用户更改

单击“是”或“否”，以指示是否要求用户在下一次认证时更改其口令。

锁定口令

单击“是”或“否”，以指示是否锁定口令。当超过注册失败的最多次数或未在“口令锁定前的最长时间”中所指定的周数之内使用口令时，设置该项为“是”。

管理员能够将该字段设置为“是”，以防止用户使用口令认证。

注:

1. 口令是区分大小写的。如果输入了一个大小写混合的用户口令，则用户必须输入一个与之一模一样的口令。如果某些工作站只能使用大写字体，请用大写字体为那些用户输入口令。
2. 操作系统允许定义口令规则。这些口令规则当用户更改他或她的口令但不是当管理员进行口令更改时适用。口令规则如下:

   期满前的警告天数

   口令期满的天数，在这几天内，Firewall 给予用户更改口令的选择。

   期满前的最大周数

   要求用户更改口令前的周数。

   锁定前的最大周数

   锁定口令之前，不使用口令的周数。

   允许的最大注册重试次数

   口令锁定前，注册尝试失败的最多次数。

   再使用前的口令

   口令历史列表中存储的口令个数。不能将口令更改为当前在历史列表中的任何口令。本参数仅当“口令再使用前的周数”为零时才有效。

   口令再使用前的周数

   口令保持在口令历史列表中的周数。不能将口令更改为当前在历史列表中的任何口令。

   最小长度

   口令中最少的字符数。

   最少字母字符数

   口令中最少的字母字符数。

   最少其它字符数

   口令中最少的非字母字符数。

   最多重复字符数

   口令中任何单个字符重复的最多次数。

   最小不同字符数

   口令中最少的不同字符数。

单击**Firewall 口令**标签来为每个用户定制这些值，如第76页的图 24 中所示。

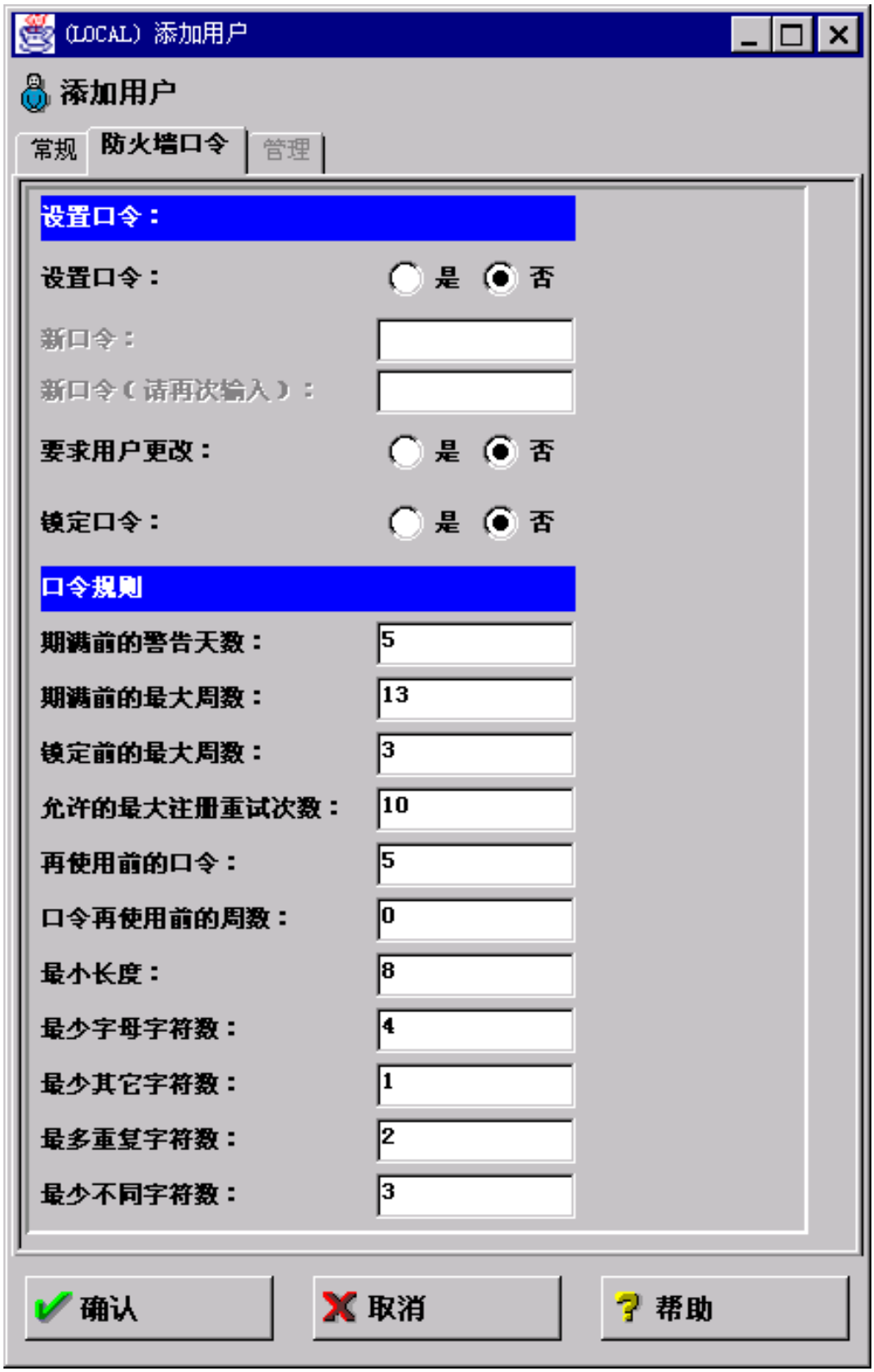

图 24. Firewall 口令标签

更改用户的存取权限

在 Firewall 上添加一个用户之后，可以从**修改用户**对话框来更改此用户的安全性属性。

1. 从**用户**对话框中选择您想更改的用户，并单击**打开**。
2. 当**修改用户**对话框出现时，更改适当的字段。请参阅 第69页的『将用户添加至 IBM Firewall』 以获得可以更改的用户属性列表。
3. 做完更改后，单击**确定**。

从 IBM Firewall 中删除用户

注: 请勿删除用户 `fwdfuser` 或 `fwdfadm`。

要删除用户，在**用户列表**上单击**删除**。

管理员权限的功能级别

只有 *主防火墙管理员* 能够创建并修改管理员，并确定他们对哪些防火墙功能有权限。例如，可以将一个特定的管理员限制在仅授权执行“用户和监视器”功能。

在**添加用户**对话框中，为**权限级别**字段选择 Firewall 管理员。请请参阅第69页的『将用户添加至 IBM Firewall』 以获得完成**添加用户**对话框的更详细情况。

然后，在**添加用户**对话框的顶部选择**管理员**标签。选择授权管理员使用的功能。

认证方法

以下是各种用户认证方法。

拒绝全部

IBM Firewall 禁止访问服务器。

允许全部

不需要认证。服务器未尝试认证；但它继续一个命令提示，这样能访问一个外部主机。

Firewall 口令

服务器在继续之前询问防火墙口令（口令不显示）。

口令:

输入防火墙口令。这是与您的用户名一起添加入防火墙的相同的口令。

SecurID 卡认证

如果有 SecurID 卡且网络使用安全性动态 ACE/服务器，则可用此法。

代理服务器在继续之前询问 PASSCODE （口令不显示）。

```
输入 PASSCODE:
```

在这点上，输入 4 位数 SecurID PIN 代码，后跟一个逗号，然后是 SecurID 卡的代码。例如， 当 SecurID 卡显示代码 179091 时，要登录为一个带指定的 1234 PIN 的用户 NEWUSER，应输入:

```
登录: NEWUSER
输入: 1234,179091
```

如果用户最初使用 FTP，则因为 FTP 没有允许口令更改的选项，所以 SecurID 卡认证将失败。用户必须在第一次尝试进行 SecurID 卡认证（通过它，他们将创建一个 PIN）时，使用 telnet。用户随后可对于以后的认证如 FTP、HTTP 等等使用 PIN。

如果 SecurID 卡是按新的 PIN 模式，则必须在与 IBM Firewall 一起使用该认证模式之前设置 PIN。

SecureNet Key 认证

如果有一个 Assurenet Pathways SecureNet Key 卡，则用此法。 当初始化 SNK 卡时，使用下列:

- 显示格式（十六进制）
- ERASE 功能（开或关）
- 单个数字查问口令能力（关）

在继续之前，代理服务器将询问由 SecureNet Key 卡提供的一个响应。

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

口令 ######## 是一个可输入 SecureNet Key 卡的 8 位数。

1. 当接收到这个提示符，激活 SecureNet Key 卡，并输入 PIN 代码。 PIN 代码与卡一起提供。
2. 输入由服务器提供的口令。

   例如: 登录到服务器; 服务器提示:

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

   将值 78987648 输入 SecureNet Key 卡。然后该卡显示响应，它是由您提供给代理服务器的。
3. 将该响应输入给服务器。

   如果 SecureNet Key 卡显示 8AE222A9 以响应对口令的查问，则将 8AE222A9 输入给服务器:

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

已通过 AXENT** 技术重新命名 SecurNetKey （SNK） 为 Defender Handheld Token** （DHT）。

NT 注册口令

若选择该认证方法，将对照本地 Windows NT 用户数据库来认证用户 ID 和口令。若 Firewall 配置为信任其它 Windows NT 服务器，则将搜索这些受信任服务器中的用户定义。

用户提供的认证 1、2 和 3

可对 FTP 和 telnet 使用用户提供的认证方法。 对于更多信息，请参阅 *IBM eNetwork Firewall 参考大全*。

第13章 配置代理服务器

本章包含有关如何从您安全网络内外的工作站使用和配置代理服务器的一般信息。

HTTP 代理

HTTP 代理通过 IBM Firewall 消除了用于 Web 浏览的 socks 服务器的需要，有效地处理浏览器请求。 用户可访问 Internet 上有用的信息，而不泄露内部网络的安全性并且不用改变其客户环境就实现 HTTP 代理。

HTTP 代理不是一个服务器。最终用户不能从该代理下载文件或将文件放在该代理上。同样，它也不是高速缓存代理。防火墙上没有存储任何代表 HTTP 请求的内容。

持续会话

持续连接允许客户和服务器发出 TCP 连接关闭的信号。该信号使用连接首部字段。

IBM Firewall 代理支持客户和代理间的持续连接。*最大持续请求*条件和*持续连接超时*条件控制该连接将存在多长时间。只要出现这些条件中的一个，代理和客户间的套接字连接都将关闭。如果*最大持续请求*条件和*持续连接超时*条件不匹配，该连接将保持打开，且由客户负责决定何时请求完成。

如果不正确确定，可能导致当没有通信量时，会显示连接上有通信量。有关它的一个实例是，即使已装入完整页面，但浏览器的动画图标仍继续运行。单击**停止**来停止动画。请参阅第83页的『最大持续请求数』 和第83页的『持续连接超时』以获得有关这些参数的信息。

使用配置客户程序配置 HTTP 代理

要配置 HTTP 代理，请按下列步骤:

1. 在 HTTP 代理可正确工作之前，您必须允许 DNS 查询。这样做的一个简单方法是在配置客户程序浏览树上单击系统管理文件夹内的“安全性策略”并单击“允许 DNS 查询”。
2. 激活过滤器
3. 添加连接。请参阅第49页的『代理 HTTP 示例』，可获得如何在您网络不安全的一边设置连接的例子。
4. 要配置 HTTP 代理，请从配置客户程序浏览树选择 HTTP。 IBM Firewall 显示 **HTTP 代理**对话框，显示在第82页的图 25中。

图 25. HTTP

5. 要停止该代理，请选择我的电脑/控制面板/服务。选择 IBM 防火墙 HTTP 代理然后单击*停止*。

   可执行的 phttpd 是一项系统服务，当启动系统时它自动启动。

在 **HTTP 代理**对话框上配置这些参数。如果更改任何参数，Firewall HTTP 代理服务将停止并重新启动。活动的代理用户将终止他们的请求，直到代理重新启动(几秒钟时间)。

代理端口号

用此参数来指定端口号，该代理侦听此端口号获得请求。如果更改端口号，则必须配置过滤器来允许或不允许经过端口的流。小于 1024 的端口号是为 TCP/IP 应用程序保留的。用于代理 Web 服务器的公共端口为 8080 和 8088。

在端口 8080 上设置缺省过滤器规则来禁止入站和非安全通信量，但在相同端口上允许安全通信量经过。代理将仅拒绝不安全的代理需求。缺省值为 8080。如果更改它，则为此配置所设置的服务中的端口号也要作更改。如果更改这些设置中的任何一个，则必须重新启动 phttpd 进程。

最大内容缓冲区长度

用此参数为由服务器产生的动态数据设置缓冲区大小。动态数据是从 CGI 程序 （服务器方所包括的），及 API 程序输出。它不是从代理来的数据。

以千字节 (K) 为单位指定值。缺省值为 50K。

线程池大小

用此参数设置您一次所需的修订活动线程数。代理挂起新的请求，直到另一个请求结束并且线程变为可用。一般，机器的功率越大，则您所用该参数的值也越大。如果机器开始花费过多的时间在系统开销任务，如交换内存上，则尝试减少该值。指定一个整数，例如 60。缺省值为 200。

用户的级别

该参数告知代理要认证何种级别的用户。指定 all、new 或 none 这类值。缺省值为 none。这些值是:

all 所有浏览器将发送代理认证响应以指示浏览器应提示给用户用户标识符和口令。如果浏览器不支持此代理认证响应，则错误页面将显示指示此内容。如果浏览器支持，则将显示用户标识符和口令提示符。

new 用作移植辅助。它将仅发回一个 407 代理认证响应，告知浏览器发出一个用户标识符/口令提示符，客户浏览器标识其自身作为 HTTP/1.1 浏览器。您可在 Internet Explorer 4.0 中设置一个开关，这样它将用 HTTP/1.1 标识符广播请求。Netscape 及其它将其自身标识为 HTTP/1.0 请求。

none 不选定浏览器请求。不提示任何用户标识符/口令。

超时

该参数告知代理在请求用户认证其自身前需等待客户程序请求多少时间。用户由在这段空闲时间的原始认证时所给定的特定 IP 地址和用户标识符获得认证。以分钟为单位指定时间。缺省值为 60 分钟。

只要用户一直在积极地浏览，该时间窗口不会期满。

最大持续请求数

该参数指明一个代理可在 HTTP/1.1 持续连接上接收到的请求的最大值。它是直接影响认证超时的一个性能工具。当处于一个持续会话中，不进行任何用户认证测试，除非持续会话终止。指定一个整数值，例如 25。缺省值为 5。

持续连接超时

该参数以秒为单位指明一旦 HTTP/1.1 从浏览器用代理启动会话，与客户浏览器保持 HTTP/1.1 持续连接的时间。它是直接影响认证超时的一个性能工具。当处于一个持续会话中，不进行任何用户认证测试，除非持续会话终止。以秒为单位指定时间。缺省值为 60。

HTTP 记录管理

该参数告知代理要记录启动/关机和所有到防火墙日志的代理请求。它使用 LOG_NOTICE 记录级。如果您希望监视 HTTP 请求活动，则将它设置为开。事件记录在 防火墙日志设施中。

浏览器配置

必须配置客户浏览器来连接到 HTTP 代理正在侦听的端口。

如果使用 HTTPS，则也要指出作为安全性代理的 IBM Firewall 上的 HTTP 代理。

如果要把 Internet Explorer 浏览器表示为至代理的 HTTP/1.1 浏览器，执行下列操作:

- 打开*查看*下拉菜单。
- 选择 *Internet 选项*。
- 选择*高级*标签。
- 下卷至 HTTP 1.1 设置选项并设置开关为开。

SSL 连接

用于与其它服务器 HTTP 安全连接的 SSL 通道是受支持的。 IBM Firewall 在该例中充当一个网关。该通道从客户程序穿过防火墙到服务器。如下例所示，使用作为 HTTP 安全连接的标准端口 443:

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

而且，使用预定义的服务 `HTTPS proxy out 2/2`。

如果使用 HTTPS，则也要指出作为安全性代理的 IBM Firewall 上的 HTTP 代理。

如需更多信息，请参阅第49页的『代理 HTTP 示例』。

受支持的方法

HTTP 代理支持下列浏览 Internet 的不同方式:

- FTP
- Gopher
- HTTP
- HTTPS
- WAIS

HTTP 代理日志输出的样本

以下是 HTTP 代理认证的 get 请求记录的输出样本。

```
Mar 06 14:04:50 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication UNSUCCESSFUL
for user <Unknown>, on 9.67.140.162, thru secure network ... RC:30.
Mar 06 14:04:50 1998 fire3: ICA2099i: httpd --> Status: 407 from client
9.67.140.162, who requested "GET http://9.67.128.69/ HTTP/1.1" for 0 bytes.
Mar 06 14:05:05 1998 fire3: ICA2024i: User fred successfully authenticated
```

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

记录活动说明如下:

- ICA2099i - 显示一个 407 返回码并且意味着认证获取请求失败。

  浏览器然后对用户要求一些认证。浏览器询问用户标识符和口令。
- ICA2140i - 对于用户 fred, 认证成功。

认证在每次获取 Web 页面上的每个元素时发生。

FTP

1. 用 FTP 代理访问防火墙主机。 (我们将使用 ftp_gw.domain.net.com 作为防火墙的主机名)。

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

   代理服务器将询问您的用户名:

   ```
   login:
   ```
2. 输入您的用户名作为使用防火墙的特许:

   ```
   login: jane_doe
   ```

服务器依靠将您的用户名添加入防火墙时所选定的认证方案来验证您的身份（请参阅 第69页的『将用户添加至 IBM Firewall』）。请参阅第77页的『认证方法』, 可获得有关用户如何通过代理服务器获得认证的信息。

在您得到认证后, 代理服务器显示一个 FTP 命令提示。

```
ftp>
```

使用 quote 和 site FTP 命令来与外部主机连接:

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

外部主机现将询问用户名和口令, 用于您的连接。这很可能是一个与您过去常 FTP 到防火墙的用户名和口令所不同的用户名和口令。

登录的缺省超时值为 60 秒而空闲代理的缺省超时值为 7200 秒。要更改缺省超时值, 请参阅第87页的『覆盖 FTP 和 Telnet 代理中的超时值』。

透明 FTP

您可通过防火墙透明地 ftp。透明代理不需要防火墙认证，因此不必将透明代理的用户定义为防火墙代理用户。 仅允许透明代理由防火墙安全方去向其不安全方。为让透明代理工作，必须在安全性策略配置客户程序面板上选中它。

1. 使用 ftp 访问防火墙主机。(我们将使用 ftp_gw.domain.net.com 作为防火墙的主机名。)

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

2. 代理服务器将询问您的用户名:

   ```
   USER:
   ```

3. 在非安全网络输入您的用户名:

   ```
   USER: username@remote_site_host_name
   ```

4. 然后目标主机提示您在上一步输入的 username 的口令。

   ```
   password:
   ```

5. 输入口令。

登录的缺省超时值为 60 秒而空闲代理的缺省超时值为 7200 秒(两小时)。要更改缺省超时值，请参阅第87页的『覆盖 FTP 和 Telnet 代理中的超时值』。

Telnet

使用 telnet 代理登录到防火墙代理服务器。 您可使用主机名或 Internet 地址。然后，在您的凭证得到认证后，可使用防火墙的 telnet 命令登录到要使用的主机。例如，让我们使用 telnet 从安全网络内通过带 telnet_gw 主机名的防火墙来访问您的最终目的地，forhost.network.outside.com。

1. 要启动进程，请使用 telnet 访问防火墙主机。(我们将使用 telnet_gw.domain.net.com 作为防火墙的主机名。)

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

2. 代理服务器将询问您的用户名:

   ```
   login:
   ```

3. 输入授权使用防火墙的您的用户名:

   ```
   login: jane_doe
   ```

服务器根据将您的用户名添加入防火墙时所选定的认证方案来验证您的身份(请参阅第69页的『将用户添加至 IBM Firewall』)。请参阅第77页的『认证方法』，可获得有关用户如何通过代理服务器获得认证的信息。

您将正在使用 oneact 外壳。通过 IBM Firewall 代理 telnet 精灵程序，所有的通信都经由防火墙。

如果您正使用 oneact 外壳，则在您得到认证后，代理服务器将显示:

```
ENTER DESIRED HOST:
```

输入

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

外部主机询问在那主机上是已知的您的用户名和口令。它们可能不同于您在防火墙代理服务器上所使用的用户名和口令。

登录的缺省超时值为 60 秒而空闲代理的缺省超时值为 7200 秒。要更改缺省超时值，请参阅第87页的『覆盖 FTP 和 Telnet 代理中的超时值』。

透明 Telnet

您可通过防火墙透明地 telnet。透明代理不需要防火墙认证，因此不必将透明代理的用户定义为防火墙代理用户。仅允许透明代理由防火墙安全的一边去向其不安全的一边。为让透明代理工作，必须在安全性策略配置客户程序面板上选中它。

1. 使用 telnet 访问防火墙主机。(我们将使用 ftp_gw.domain.net.com 作为主机名。)

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

2. 代理服务器将询问您的用户名:

   ```
   Login:
   ```

3. 在非安全网络输入您的用户名:

   ```
   Login@remote_host
   ```

外部主机询问您的用户名和口令，因为您在那主机上是已知的。它们可能不同于您在防火墙代理服务器上所使用的用户名和口令。

登录的缺省超时值为 60 秒而空闲代理的缺省超时值为 7200 秒。要更改缺省超时值，请参阅第87页的『覆盖 FTP 和 Telnet 代理中的超时值』。

覆盖 FTP 和 Telnet 代理中的超时值

FTP 和 Telnet 都有登录和空闲等待的超时值。按缺省值，在登录和用户认证期间每 60 秒至少必须有一次会话活动。这就是所谓的 loginTimeout。

一旦成功地完成登录，则每 7200 秒至少在会话上有一次活动或断开会话。

您可通过在 ROOTDIR\config 目录下创建 fwTimeout.cfg 文件并以秒为单位指定新的超时值来覆盖这些缺省值。 fwTimeout.cfg 文件应有下列格式。

```
telnet
proxyTimeout=7200
loginTimeout=60

ftp
proxyTimeout=7200
loginTimeout=60
```

第14章 监视防火墙记录

本章描述如何实现时监视警报的记录。当违反配置的阈值时，将生成一个警报。

根据用户定义的阈值，IBM Firewall 监视器监视由于潜在的危机情况而发送至防火墙日志的信息。一旦出现阈值违规，防火墙就以防火墙管理员所指定的方式发出一个警报。

阈值定义

一个阈值包括计数值和时间参数 -- 如果在指定时间内（分钟），超过计数值（特定事件数），则会违反阈值并产生警报信息。日志监视器可以识别四种类型的阈值:

1. 认证失败总数
2. 对任一特定用户 ID 认证失败
3. 从任一特定主机上产生的认证失败
4. 日志中一个信息标记的出现次数

使用配置客户程序或命令行界面能配置所有的阈值。任何对阈值定义所作的更改都将自动由 IBM Firewall 收集。

警报信息

当达到某一阈值时，IBM 防火墙将产生一个警报信息。 警报信息的传递可采用下面四种形式中的任一种:

1. 日志文件中的项:
   - 利用 alert 日志设施，该设施可通过配置客户程序或命令行来进行配置。
   - 在防火墙日志中
2. 将 e-mail 信息发送到用户列表
3. 使用配置的寻呼机。请参阅第91页的『寻呼机通知支持』。
4. 执行一个用户定义的命令，用警报信息作为第一个参数

警报信息中包含与违反特定阈值相关的信息。例如:

```
ICA0001e: ALERT -- 20 认证失败。
ICA0002e: ALERT -- 10 超级用户认证失败。
ICA0003e: ALERT -- 15 来自主机 56.67.78.89 的认证失败
ICA0004e: ALERT -- 带有 3 个日志项的 Tag ICA1234e 。
```

来自日志监视器的警报信息及其他信息不受监视。

使用配置客户程序配置日志监视器

这部分描述如何使用配置客户程序来配置实时日志监视器。 从配置客户程序浏览树中选择系统日志。双击文件夹图标以展开视图。单击**日志监视器阈值**。

从**日志监视器阈值管理**对话框中，您可以添加、更改或删除阈值定义。

添加日志监视器

要添加阈值定义，可从**日志监视器阈值管理**对话框中选择**新建**并单击**打开**。出现**更改日志监视器**对话框。 填写下列字段:

1. 单击**级别类型**箭头来从级别类型列表中选择级别类型。级别类型有:
   - 邮件通知
   - 执行命令
   - 每个用户认证失败阈值
   - 认证失败总数阈值
   - 每个主机认证失败阈值
   - 信息阈值
2. 如果您选择的级别类型为: 邮件通知，请输入电子邮件地址。您可以定义多个邮件通知类。

   所有违反阈值的信息将发送到指定的电子邮件地址。
3. 如果您选择的级别类型为: 执行命令，请填写一个命令文件名。

   日志监视器将执行该命令，并使用警报信息作为它的第一个参数。您可以仅定义一个执行命令类。
4. 如果您选择的级别类型为: 信息阈值，请填写一个信息标记，它是一个您要监视的 IBM Firewall 日志信息中的标准标记。
5. 如果您选择了阈值类中的一个，请填写阈值计数值字段。

   阈值计数值是在指定时间内允许失败事件的最大数量。
6. 如果您选择了阈值类中的一个，请填写阈值时间字段。

   阈值时间是指自首次发生一个事件以来的分钟数。
7. 如果您选择了阈值类中的一个，单击是或否来表明您是否想激活寻呼机通知。
8. 填写注解是任选的。
9. 单击**确认**。

更改阈值定义

要更改阈值定义，请在**日志监视器管理**对话框中选择要更改的项目并单击**打开**。出现**更改日志监视器**对话框。

1. 输入要更改的阈值计数值和阈值时间字段。

   阈值计数值是在指定时间内失败的认证信息的最大值。阈值时间是指自首次发生一个事件以来的分钟数。
2. 单击**确认**。

删除阈值定义

要删除阈值定义，请在**日志监视器阈值**对话框中选择要删除的项目并单击**删除**。将会要求您对删除操作进行确认。单击**是**以确认。注意删除并不意味着从日志文件中删除。它代表删除定义。

寻呼机通知支持

当防火墙上有侵入警报时，向管理员的蜂鸣器发送信息可呼叫系统管理员。要设置寻呼机通知支持，需要配置下列三个寻呼机组件。

1. 命令定制 - 该组件必须用配置客户程序来创建和修改。它为寻呼机命令设置缺省值，该命令由日志监视器使用并能从命令行使用。它包含定义寻呼机环境的唯一项。请参阅第92页的『命令定制』可获得定义和定制该组件的详细信息。
2. 通信公司管理 - 必须在连接您的调制解调器之前定义一个适当的通信公司。该组件包含一列在美国使用的缺省通信公司。如果您正使用的通信公司并非其中之一，那么可将其添加入该组件中。如需详细信息，请参阅第93页的『通信公司管理』。

   从您的通信公司获得这些号码可验证该通信公司现在的电话号码。在与通信公司交涉时，一定要获得该公司的调制解调器电话号码及其他适用于您已订购的特殊服务的设置。
3. 调制解调器管理 - 在连接您的调制解调器之前，必须先创建一个适当的调制解调器定义。这些定义将包括所有相关的调制解调器信息，而寻呼机通知支持将使用这些信息。该组件包含您可选择的调制解调器的列表。但也可将某些与您的通信公司的支持不兼容的调制解调器添加入该表中。如需有关维护调制解调器定义的信息，请参阅第94页的『调制解调器管理』。

注: IBM Firewall 支持寻呼机通信支持支持的 Tele-AlphaNumeric 协议 (TAP)通信协议。

可支持哪些通信公司和调制解调器

通信公司数据库文件包含一个通信公司的列表和相关的传输参数。 可以添加其它通信公司。除通信公司名称和调制解调器电话号码之外的其它参数有:

- 字母数字寻呼机的最大信息长度及数字寻呼机的最多数字位。
- 波特率、奇偶性、数据和停止位长度

在使用特定的通信公司之前，请确认通信公司使用的是 TAP 协议。

寻呼机代码带有缺省调制解调器定义。它们是:

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

配置寻呼机通知支持

寻呼机设置程序是用来配置命令定制文件和维护通信公司及调制解调器的。如果您正使用寻呼机，那么在使用日志监视器前必须使用寻呼机设置来定制您的寻呼机环境。

启动前，需要得到正确的调制解调器电话号码，寻呼机 ID 和您的通信公司的调制解调器参数。

要配置寻呼机通知支持，从配置客户程序浏览树中选择系统管理。 双击文件夹图标以展开视图。选择**系统日志**。双击文件夹图标以展开视图。选择**寻呼机设置**。

命令定制

当您选择**寻呼机设置**时，可选择一家通信公司和调制解调器以使用和编写寻呼机信息。

命令定制设置

当您从浏览树选择**寻呼机设置**时，可以得到一个带有命令定制设置的**寻呼机设置**对话框，这个对话框与第92页的图 26 中所示的对话框类似。

图 26. 寻呼机设置

在要添加的输入字段中输入或选择值。

1. 输入寻呼机 ID。它通常是由通信公司指定给您寻呼机的一个唯一的 PIN。
2. 输入寻呼机信息。它是一个字符串，包含用户要发送的缺省信息。对于数字寻呼机，只能是数字信息。对于字母数字寻呼机，可以是文本信息。不要超过通信公司设置所指定的字母数字传呼机的最大信息长度，否则信息将被截断。不要使用冒号（:）。如果使用的话，它将会被空格符替代。
3. 如果没有通信公司名称，单击**选择**以定义通信公司。您将得到**寻呼通信公司管理**对话框。请参阅第93页的『通信公司管理』 如何填充该面板以获得详细细节。
4. 如果没有调制解调器名称，单击**选择**以定义调制解调器。您将得到**寻呼机调制解调器管理**对话框。请参阅第94页的『调制解调器管理』 如何填充该面板以获得详细细节。

5. 单击**确认**。

更改命令定制

当您从浏览树选择**寻呼机设置**时，将会得到带有命令定制设置的寻呼机设置对话框。

1. 在输入字段中输入或选择值，以修改现存的定制输入字段的值。
2. 单击**确认**。

删除命令定制

1. 您可以通过从列表中选择项并双击**删除**，来删除**寻呼通信公司管理**对话框或**寻呼机调制解调器**对话框中的项。

   将会要求您对删除操作进行确认。
2. 单击**是**以确认删除操作或单击**否**以返回**寻呼机设置**对话框。

如果没有定制项存在，那么寻呼机通知支持将不能发送寻呼。

通信公司管理

从**寻呼机设置**对话框，转至通信公司名称字段，并单击**选择**。您将得到与第93页的图 27 所示对话框相似的**寻呼通信公司管理**对话框。

图 27. 寻呼通信公司管理

添加一个通信公司

要添加一个新的通信公司，请从**寻呼通信公司管理**对话框中选择**新建**，并单击**打开**。在适当的输入字段中输入或选择值:

1. 输入通信公司名称。它可以是任何名字，只要是唯一的且可为您确认是哪一家通信公司提供足够的信息。
2. 输入通信公司的电话号码，该号码是这家通信公司的某一调制解调器的电话号码，而不是其声音寻呼机或其它服务的号码。它必须是数字或字母寻呼机覆盖地区或国家范围的正确的调制解调器号码，对您已签约的服务和寻呼机设备来说是必需的。
3. 输入 TAP 可获得寻呼方法；只允许该值。
4. 如果通信公司允许或需求则输入口令。

5. 输入字母数字寻呼机的最大信息长度及数字寻呼机的最多数字位。
6. 输入波特率。单击箭头并从列表中选择值。
7. 对于奇偶性字段单击 **Even**、**Odd** 或 **None**。
8. 选择缺省数据位；单击 **7** 或 **8**。
9. 选择缺省的停止位；单击 **1** 或 **2** 。
10. 单击**确认**。

更改通信公司

1. 从**寻呼通信公司管理**对话框中选择您想更改的通信公司，并单击**打开**。
2. 参考第93页的『添加一个通信公司』，以获得要更改字段的说明。通信公司名称本身不能更改。该字段将被禁用。
3. 进行期望的更改。
4. 单击**确认**。

删除通信公司

1. 从**寻呼通信公司管理**对话框中选择要删除的通信公司，并单击**删除**。
2. 将会要求您对删除操作进行确认。单击**是**以确认。

注: 通信公司数据库总是包含至少一个通信公司。如果没有定义通信公司，那么寻呼机通知支持将失败。

调制解调器管理

调制解调器手册将包含如何初始化调制解调器的相关信息。您可能需要协调调制解调器设置与通信公司。一般，仅支持使用标准调制解调器命令的 Hayes 可兼容调制解调器。

从**寻呼机设置**对话框，转至调制解调器名称字段，并单击**选择**。您将得到与第94页的图 28 所示对话框相似的**寻呼机调制解调器管理**对话框。

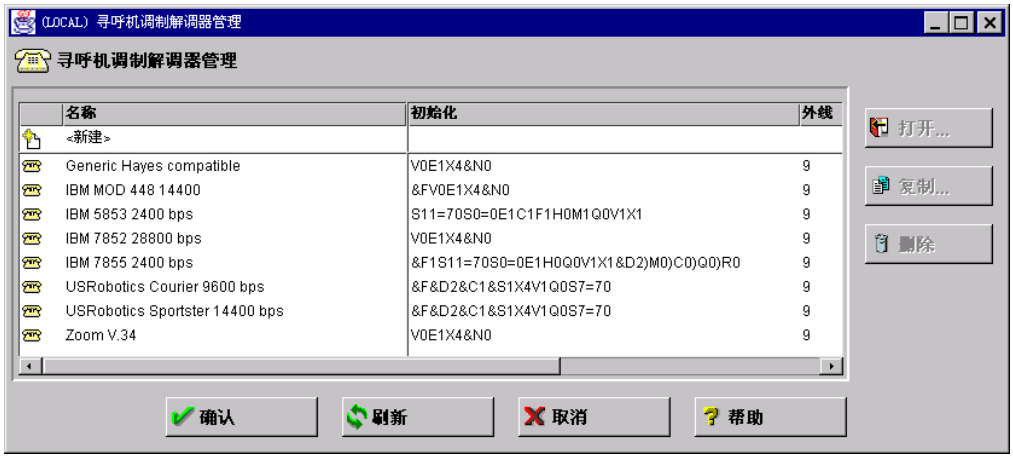

图 28. 寻呼机调制解调器管理

使用该对话框，您可以添加、更改或删除各种不同的调制解调器。

添加调制解调器

要添加新的调制解调器定义文件，从**寻呼机调制解调器管理**对话框中选择**新建**，并单击**打开**。在**添加调制解调器**对话框中，在输入字段输入或选择值。

1. 输入调制解调器名称。它可以是任何名字，只要它在其他定义中是唯一的且为您确认是哪一个调制解调器提供了足够的信息。
2. 输入 COM 端口号，它定义了与调制解调器相连的串行 COM 端口。输入一个小于 10 的数。当调制解调器作为硬件配置给端口，它不应定义为 Windows NT；如果定义的话将导致寻呼机访问端口的功能受拒绝。如果调制解调器不匹配硬件设置选项，则寻呼机代码将重试一段时间并最终失败。
3. 输入初始化字符串，它将调制解调器定义为一个在 X level4 上带回显和有固定波特率 (由本地位置定义) 的数据调制解调器。不包括 AT 命令。寻呼机功能将其放在初始化字符串的开始。
4. 输入外部行前缀。这个号码可拨号至公司外部。
5. 单击**确认**。

更改调制解调器

1. 从**寻呼机调制解调器管理**对话框中选择调制解调器名称，并单击**打开**以更改调制解调器定义文件。

   在**更改调制解调器**对话框中，您会看到调制解调器定义中可更改的字段列表。参考第95页的『添加调制解调器』，以获得这些字段的说明。

2. 单击**确认**。

删除调制解调器

1. 从**寻呼机调制解调器管理**对话框中选择调制解调器名称，并单击**删除**以删除调制解调器定义文件。
2. 将会要求您对删除操作进行确认。单击**是**以确认。

寻呼机通知记录

寻呼机通知进程使用防火墙日志实用程序来编写输出日志。将所有的寻呼机信息和错误都写入常规防火墙 syslog 设施。 要获得如何建立和使用防火墙日志文件的详细信息，请参阅第97页的『第15章 管理日志和档案文件』。

测试寻呼机的设置

您可通过使用寻呼机命令来验证寻呼机的设置。请参阅 *IBM eNetwork Firewall 参考*大全以获详情。向您强烈推荐：在为保证系统、调制解调器、通信公司和寻呼设备能互相正确地交流且可真实地发送和接收页面而定义或更改设置时，请使用寻呼机命令 。

执行命令

可以指定一个程序，该程序在每次到达警报阀值时被调用。要指定一个程序:

1. 单击**日志监视器管理**，然后双击**新建**。

   出现**更改日志监视器**对话框。

2. 在**级别类型**下拉框中选择**执行命令**。它启用面板的**命令文件名**字段。

3. 在**命令文件名**字段中，输入当到达警报阀值时想调用的程序的全限定路径名。

   由日志监视器执行的命令的工作目录是 `\winnt\system32`。因为命令外壳是从系统进程启动的，所以仅设置了系统环境变量。没有设置用户环境变量。通常，被启动的程序应该使用全限定文件名，而不是依靠路径变量。

   防火墙会如下将全部的报警信息作为程序的第一个参数传送出去:

   ```
   总计认证失败警报:  ICA0001e
   每个用户认证失败警报:  ICA0002e
   每个主机认证失败警报:  ICA0003e
   信息阈值警报:  ICA0004e
   ```

请参阅 *IBM eNetwork Firewall 参考*大全以获得这些信息的完整说明。

第15章 管理日志和档案文件

本章描述了如何通过配置客户程序来使用日志设施。 当用户试图通过各种 IBM Firewall 服务器来访问主机时，由 IBM Firewall 将输入项写入由 IBM Firewall 记录服务来维护的日志文件中。

根据防火墙是如何配置的，IBM Firewall 能生成大容量的日志信息。日志项可来自多种地方，例如 socks 和专家过滤器。另外，可将日志文件写入多种错误严重性级别；例如*调试*，*信息*，或*错误*。本章还阐述了如何使用日志管理和日志档案管理设施来管理日志和档案文件的大小。

使用配置客户程序来创建并存档日志文件

可使用配置客户程序来进行日志管理和日志档案管理。 假设可用的磁盘空间足以包含所有的日志信息。防火墙生成例行程序调试和出错信息到仅防火墙日志设施。只有主防火墙管理员才有权访问防火墙日志设施。报警信息转至报警日志设施中。 管理的审查日志信息转至审查日志设施中。

为了报告实用程序能正常运行，重要的是应只有防火墙日志信息在输入文件中出现。 不应该将其它设施指向与防火墙日志相同的文件，所以相应地设置防火墙注册。

若要查看主配置客户程序面板上的报警，则必须将报警传至指定为一个报警日志设施的文件中。不应该再为那个文件指定什么内容。

下列的优先级是递增的，由*调试*来捕捉最多的信息。*关键*只捕捉最严重的防火墙事件。

- 调试
- 信息
- 警告
- 出错
- 关键

建议由*信息*级别开始，直到防火墙过程稳定。然后可以更改为*警告*或*出错*，以减少注册活动和系统日志的大小。

优先级别不精确地与消息标记后缀相关，后缀是 *(i,e,w,s..)*。. 您可能需要经验来确定如何*关闭*某些消息。

添加日志设施

从配置客户程序浏览树中，双击“系统管理文件”文件夹图标，以便扩大视图。双击“系统日志文件”文件夹图标，以便扩大视图。选中“日志设施”。**日志设施**对话框出现，显示了当前启用的日志设施集。

1. 选中**日志设施**对话框中的**新建**，并单击**打开**，以便将一个 syslog 项添加到那些当前启用的日志设施的设置中去。

   出现**添加日志设施**对话框，如第98页的图 29 中所示。

图 29. 添加日志设施

2. 单击**类型**箭头来选择类型。类型是文件名。
3. 日志设施确定获得记录的信息的类型和源。单击**设施**箭头，选择下列日志设施之一：
   - 防火墙日志 - 一般的防火墙日志，包括过滤器日志
   - 报警日志 - 日志监视器的精灵程序状态和阈值的违反警告，用于报警显示
   - 邮件日志
4. 单击**优先级**箭头，以便选择优先级。日志的优先级以错误严重性的递增次序列出。所选中的优先级将为记录的最小级别。
5. 填入日志文件名。日志文件名必须有绝对路径（以 drive 和反斜杠 \ 开始）且到达文件的路径必须存在。
6. 档案管理只能与一个*文件名*类型日志设施一起使用。当启用后，可在周期的基础上减少日志文件大小。启用档案管理表示设置 `fwlogmgmt` 命令所取决的参数。请参阅 第99页的『档案日志』。可以启用或禁用档案管理参数。
7. 选择完整的天数，直到活动的日志中的记录应该存档。值必须大于等于 0。当 `fwlogmgmt -l` 命令找到符合该标准的活动的运行记录时，才存档。当计算保留日志记录的天数时，日志管理不包括当天。
8. 输入一个档案文件名和完整路径。 IBM Firewall 提供了一个使用目录的系统设定存档函数。但是若需要，可以使用 plug-in 存档功能。

9. 选择完整的天数，直到存档的日志文件应该从档案中删除。值必须大于等于 0。当 `fwlogmgmt -a` 命令找到符合该标准的存档文件时，才清除。当计算保留存档文件的天数时，日志管理不包括当天。
10. 单击**确认**。

更改日志设施

1. 从**日志设施**对话框中选择要更改的防火墙记录项，并单击**打开**。

   将出现**更改日志设施**对话框。
2. 更改期望的字段。如需字段的详细说明，请参阅第97页的『添加日志设施』。
3. 单击**确认**。

删除日志设施

1. 在**日志设施**对话框中那些当前启用的输入项中选择一个防火墙记录项，并单击**删除**。

   出现**删除警告**面板。
2. 若要继续删除时，单击**确定**。若不要继续删除，则单击**取消**。这不会删除实际的日志文件。

档案日志

存档过程:

- 从活动的日志中删除符合的记录
- 将它们放入分散的文件
- 压缩结果文件
- 将新文件放入存档目录

要启动日志管理程序以便存档积累的日志记录时，可以作两种选择:

1. 运行 `fwlogmgmt -l` 命令
2. 设置 `fwlogmgmt -l` 命令为 NT 预定服务。

清除日志档案包括从档案目录中删除适当的已存档文件。

要清除已存档文件有两个选项:

1. 运行 `fwlogmgmt -a` 命令
2. 设置 `fwlogmgmt -a` 命令为 NT 预定服务。

适合的记录和文件由日志设施定义中指定的值来确定，如第97页的『添加日志设施』 中所描述的。

运行日志管理进程最有效便捷的方法是将其设置为一个 NT 预定服务。需要启动它，请通过使用控制面板上的服务对象。

例如，若要将日志管理存档进程设置为在每天 3:00 AM 运行，则输入

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

插件 DLL

请参阅 *IBM eNetwork Firewall 参考大全*以获得有关能使用来替换 Firewall 缺省 DLL 的日志档案库插件 DLL 的信息。

日志管理输出

在用任何管理行为执行之前，日志管理设施会执行一些初始完整性检查。若找到了任何问题，则当从命令行运行 `fwlogmgmt` 命令时，将发送诊断到防火墙日志设施。

邮件或 admin 审查 (local0) 日志设施取决于不同的档案规则而不是其它设施。所有日志设施需要启用档案以存档。不过，防火墙 (local4) 和报警 (local1) 日志记录被存档仅当在运行存档进程时，它们的日期超过了在设施定义中指定的标准，另一方面，将每次存档整个 mail 或审查日志文件。同样，在邮件日志中的信息是考虑为用于调试目的的并且一般存档它时有少量值。其它的，一般更多有用的邮件信息记录在防火墙 (local4) 日志中。

报告实用程序

可以使用报告实用程序功能，以从当前或档案日志文件中辅助生成报告。 报告实用程序生成管理信息的制表文件，这些文件被组织和格式化使其易于映射到关系数据库的表中。 这些表帮助防火墙管理员分析:

- 防火墙的一般用法
- 防火墙处理中的错误
- 对安全网络的未授权访问的尝试

通过使用实用程序和防火墙日志，管理员可以建立一个常规的信息文本文件。此外，可生成表格化的文件并将其调入关系数据库系统(诸如 DB2 系列产品)中的表。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。

报告实用程序作为防火墙安装的一部分进行安装。也可单独安装它们，并在非防火墙主机上运行。配置客户程序可用来在防火墙上运行它们。在非防火墙上机器，使用命令行。

为了报告实用程序能正常运行，重要的是应只有防火墙日志信息在输入文件中出现。不应该将其它设施指向与防火墙日志 相同的文件，所以相应地设置防火墙日志设置。

请勿尝试使用 IBM Firewall AIX 版 V3R1 上一个任何日志文件上的报告实用程序。但是，可以使用报告实用程序以处理来自 IBM Firewall AIX 版 V3R1 或更新版本的日志文件。您也可使用它们来处理 AIX su 日志。有关报告实用程序更详细的信息，请参阅 *IBM eNetwork Firewall 参考大全*。

使用配置客户程序来运行报告实用程序

从配置客户程序浏览树中，双击“系统管理文件”文件夹图标，以便扩大视图。双击“系统日志文件”文件夹图标，以便扩大视图。选择**报告实用程序**。出现**报告实用程序**对话框，如第101页的图 30 中所示。

图 30. 报告实用程序

1. 对于 IBM Firewall 提供的缺省存档标志，日志档案路径名是包含压缩了的日志文件的目录。在“日志档案路径名”字段输入在**日志设施**对话框的“档案目录”字段中指定的目录。 输入档案目录的绝对路径名。若要查看未存档的日志文件，则将该字段置为空。
2. 选择**报告类型**。需要产生扩充的日志信息正文，选择**文本日志**。要创建 DB2 用法的制表文件，选择**表日志**。若将结果文件调入了 DB2，则可在日志数据上执行 SQL 查询。如需得更多信息，请参考 *IBM eNetwork Firewall 参考*大全。
3. 日志文件名是任何压缩的档案日志文件、其它有效的防火墙日志或一个 AIX su 日志文件的名称。若在“日志存档目录”字段中设了一项，则能够单击**日志文件名**箭头，以选择工作的日志。若未在步骤 1 输入一个日志挡案文件名，则在这里输入的必须是一个有效的、未压缩的防火墙日志文件名称或是一个 AIX su 日志文件。必须指定全路径。
4. 选择**日志类型**、**防火墙**或 **AIX su**。
5. 输入**输出文本的路径和文件名**。

6. 选择**是**将表日志请求的结果添加到现存的制表文件，或选择**否**来替换现存文件。
7. 该字段允许您选择要放入输出文本文件的信息的特定类型。该字段的内容被认为是放入标准 Windows NT 查找命令中的参数。例如，如果输入 ″ICA0″ 到字段(必须包括引号)，仿佛您正在运行下列命令:

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

   这儿是一些能将它们放入该字段的实例项和结果:

   ```
   过滤器                    结果
   "ICA0"          列出日志监视器阈值警报信息
   "ICA3"          列出 Socks 关联的信息(#ICA3000 - 3999)
   "ICA2010"       仅列出 ICA2010 出现信息
   /V "ICA3"       列出所有信息除了 Socks 信息
   /C "ICA001"     计算 ICA0001 信息数
   ```

8. 单击**确定**，在防火墙机器上指定输出目录中产生请求文件。
9. 报告实用程序结果区域显示任何来自运行的报告实用程序的错误信息。要查看从文本日志报告类型导出的日志文本，单击主防火墙配置客户面板上的**日志查看器**，并输入全限定输出文件名。可装入从表日志报告类型导出的 .tbl 文件到数据库中，如 *IBM eNetwork Firewall 参考大全中所描述*。

第16章 转换网络地址

随着 Internet 的爆炸性增长，IP 地址的枯竭问题显得越来越重要。网络地址转换（NAT）提供了一个基于地址重使用来解决 IP 地址枯竭问题的方案。

可以从一个很大的地址空间(典型地是 10.0.0.0 A 类地址空间)分配地址给专用网络中的地址。这些地址是专用的，而且不会暴露给 Internet。所以这些地址可以由另一个 IP 网络重使用。使用单个已注册的 IP 地址可以隐藏很多专用的网络地址。 NAT 将未注册的地址和端口号转换成有效的已注册 Internet 地址和端口号。在入站方向时，NAT 再将已注册的 Internet 地址和端口号转换回未注册的地址和端口号。 NAT 的优点是它显而易见地允许使用专用或非法地址的网络与 Internet 上的主机通信，从而有效地允许专用网络拥有很大的地址空间。而且通过使用 NAT 提供了附加的安全级别，能将专用网络中的地址隐藏起来，使外部世界不能看到它们。

第103页的图 31 说明了 IBM Firewall 环境中的基本 NAT 操作。

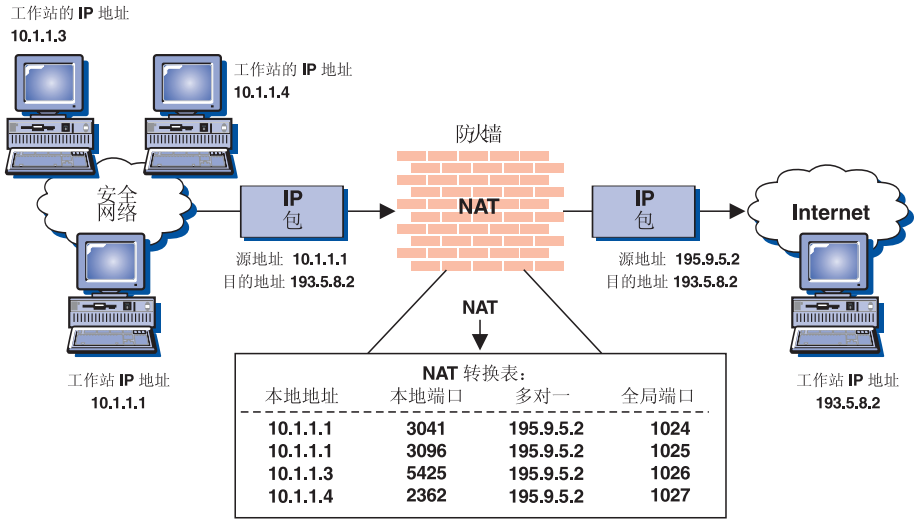

图 31. 网络地址转换

安全主机生成的 TCP/UDP 包将它们的源地址替换成已注册的 Internet 地址。安全主机的端口将转换成一个唯一的端口号。所有的出站包都将拥有相同的源地址和一个唯一的端口号。这种转换形式称为多对一转换，它允许很多安全主机隐藏于单个地址之后。 IP 首部和 TCP/UDP 伪首部中包的检验和被更新。并行连接的最大数被限制为 64536(实际上是 64512)，因为端口 0-1023 是保留端口。入站连接受静态(而不是动态)转换表项支持。例如，只有当 NAT 转换表中存在映射 195.9.5.2 到 10.1.1.1 的静态项时，主机 193.5.8.2 才能启动与主机 10.1.1.1 的 TCP 连接(使用全局地址 195.9.5.2)。

所有 TCP/UDP 应用程序生成的包都能被转换。如果 IP 包中包含的应用程序数据包含 IP 地址，则会产生问题。地址转换的一个特别棘手的应用程序是 FTP。FTP 控制连接发出报文中含有 ascii 编码的 IP 地址的"PORT"命令或"PASV"回答。在这种情况下，NAT 不仅必须修改 IP 首部中的地址，还必须修改酬载中的 ascii 地址和端口号。

随着即将发行的 APAR，NAT 的多对一和 MAP 转换选项将允许转换入站和出站的 ICMP 包。仅当存在使用重定向异常的转换表项时，才能转换入站 ICMP 回答包(ping,

时间戳记，地址掩码)和所有的出错包(不可到达的目的地、源被消除、重定向、超时和错误包信息)。 ICMP 重定向将不经转换通过 NAT 传送。允许或拒绝 ICMP 重定向取决于您的过滤器规则。

通过转换包的安全地址和 ICMP 查询标识符来支持出站查询/回答 ICMP 包(ping 请求/回答、时间戳记请求/回答，地址掩码请求回答)，以便来自不同安全主机的 ICMP 包能共享单个已注册的地址。

管理员应该警惕，不要允许某些特定的 ICMP 包，特别是地址掩码/回答和重定向，在安全和非安全网络间流动。有关允许 ICMP 通信量通过 Firewall 时会引起的安全性危害，请参阅下列红皮书。已在书目中列出，题为: *使用 IBM eNetwork Firewall NT 版 3.2 防守门户（Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2）*。

IBM eNetwork Firewall NAT 实现

IBM Firewall NAT 实现支持如上所描述的基本地址转换，但带有下列说明:

- 酬载中包含 IP 地址信息的 TCP/UDP 应用程序(除了下面所描述的 FTP)只能如上所述转换包首部字段。这暗示着 UDP 应用程序(例如 DNS 或 SNMP)不能转换酬载中包含的地址信息。
- 完全转换 FTP PORT 命令。但是，在 PASV 响应包中嵌入的地址将不被转换。
- 转换 ICMP 请求/回答和加密信息。这允许，例如，出站 ping 能象 TCP 路径 MTU 发现一样正确操作。
- NAT 不检测 TCP 断开，但它在删除动态转换表项和将已注册的 IP 地址插回可用的地址池前宁愿依赖一个可配置的空闲超时。

NAT、过滤器和隧道间的实例交互

第105页的图 32 说明了一个 NAT、过滤器和隧道间的实例交互。

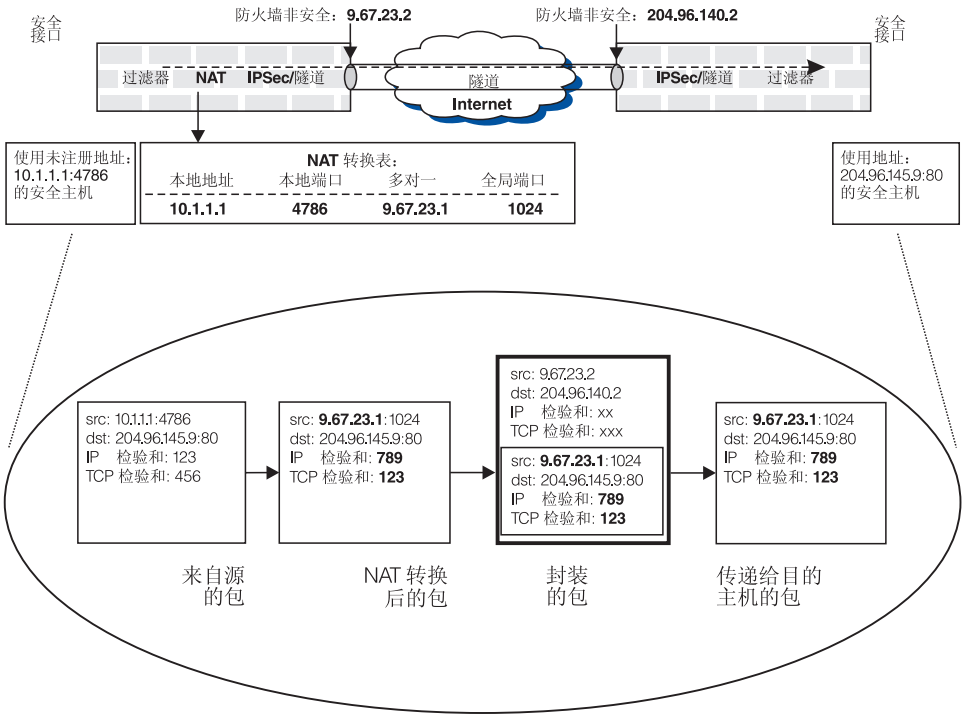

图 32. NAT、过滤器和隧道间的实例交互

假设在防火墙 9.67.23.2 和 204.96.140.2 之间手工建立了一个 IPSec ESP 隧道。 NAT 仅在 9.67.23.2 防火墙端激活，因为这个安全网络使用专用地址。隧道另一端处的安全网络不使用 NAT。除了说明基本 NAT 转换(左起第二个包中的粗体字字段说明了在出站地址转换期间包中被修改的字段)之外，第105页的图 32 还说明了来自主机的已转换的包被封装在一个未转换的 IP 包。

一般情况下，过滤先于 NAT 适用于出站包，且在 NAT 转换后才适用于入站包。因此过滤器规则是基于未转换的地址的。当包含 NAT 和隧道时，有 NAT 激活的防火墙端的过滤器规则也基于未转换的地址。在隧道的另一端(假设在该防火墙端 NAT 未激活)，入站包的过滤器规则是基于已转换的源和目的地址(分别针对入站和出站的不同情况)。如果在隧道的两端 NAT 都是活动的，则上述讨论同时适用于两个方向。

以第105页的图 32 中说明的方案为例，假设目的是要允许安全主机 10.1.1.1 通过隧道与安全主机 204.96.145.9 通信，则连接到 10.1.1.1 的防火墙必须有允许 10.1.1.1 通过隧道与 204.96.145.9 通信的过滤器规则。连接到目的地主机的其它防火墙，则需要有允许通过隧道在 9.67.23.1 和 204.96.145.9 之间通信的过滤器规则。

有关 NAT 的更多信息

如果想允许下列事项，则使用 NAT：

- 为了保护安全机器的地址，直接存取防火墙后机器的非安全位置。
- 相当数量含未注册地址的机器共享一个已注册地址，以便它们能访问 Internet 上的站点。
- 其它来自非安全位置的机器存取防火墙后的服务器。

从您的 ISP 获得 NAT 的已注册地址。所有用于 NAT 的地址都不能用于其它目的。

NAT 有四种选项:

多对一 包含正在转换包的安全地址和端口号以便很多(最多 65536)内部地址能共享一个已注册的 IP 地址。这个共享的已注册 IP 地址将隐藏本地地址，但是除了它之外，您还需要另一个用于 Firewall 非安全地址的已注册 Internet 地址。 NAT 配置将标识使用多对一项的端口转换所用的已注册 Internet 地址。

转换 用于创建将被转换的安全地址列表。

排除 用于创建将不会被转换的安全地址列表。

映射 用于为特定安全地址保留特定已注册地址。

使用配置客户程序配置网络地址转换

1. 从配置客户程序浏览树中，双击“地址转换文件”文件夹图标以扩充视图。双击“NAT 文件”文件夹图标来扩充视图。
2. 请选择 **NAT 设置**来配置网络地址转换模块。

   出现**网络地址转换列表**，如第106页的图 33 所示。

图 33. 网络地址转换列表

3. NAT 配置文件中包含的网络地址转换项将显示在该对话框中。您可以添加、更改或删除 NAT 项。

添加 NAT 项

1. 从**网络地址转换列表**中选择**新建**，并单击**打开**以添加新项到 NAT 配置文件中。

   出现**添加 NAT** 对话框。
2. 从**添加 NAT** 对话框，单击 NAT 类型字段中的箭头从下列选项中选择一项:

- 多对一已注册网络地址: 添加指定的 IP 地址到保留的 IP 地址。参数是保留的 IP 地址，且超时与转换表有关。
- 转换安全网络地址: 指定需要网络地址转换的安全 IP 地址的范围。
- 排除安全网络地址: 指定应该从网络地址转换中排除的安全 IP 地址的范围。
- 映射安全网络地址: 定义一个一对一的、安全 IP 地址到已注册 IP 地址的静态转换。

多对一已注册网络地址

多对一已注册地址项转换包的安全地址和端口号以便很多(最多 65536)内部地址能共享一个已注册的 IP 地址。 这样就能使用一个已注册 IP 地址来隐藏很多本地地址。 (您将需要一个用于防火墙非安全地址的附加的已注册 Internet 地址)。

当一个安全主机将包发送到非安全网络时，会分配一个已注册的 IP 地址。这个唯一的已注册 IP 地址是用于在 IBM Firewall 和安全网络外部的机器之间传送 IP 帧。

如果您从添加 NAT 屏幕上选择了多对一，请输入下列值:

已注册 IP 地址
从您的 ISP 取得它。这将成为所有安全地址都隐藏于后的点十进制 IP 地址。

要选择一个网络对象，请单击**选择**获得**选择网络对象**对话框。选择一个网络对象并单击**确认**。在**添加 NAT 配置**对话框的网络对象字段中就添加了该网络对象。或者，如果没有预先创建网络对象，则将值直接输入该字段。

超时值 输入一个在 NAT 能释放已注册 IP 地址之前，地址转换可保持空闲的分钟数。超时值仅适用于由该项指定的 IP 地址范围中使用的已注册 IP 地址的地址转换。

缺省值为 15 分钟。值的范围从 5 到 45。

转换安全网络地址

转换安全 IP 地址项定义了需要 NAT 来执行 IP 地址转换的安全网络地址集。 缺省情况下，NAT 执行转换安全 IP 地址集中所有安全 IP 地址的地址转换。

如果您从添加 NAT 屏幕中选择了转换，请输入下列值:

安全 IP 地址
指定一个点十进制的 IP 地址，来标识需要网络地址转换的安全 IP 地址的范围。

要选择一个网络对象，请单击**选择**获得**选择网络对象**对话框。选择一个网络对象并单击**确认**。在**添加 NAT 配置**对话框的网络对象字段中就添加了该网络对象。或者，如果没有预先创建网络对象，则将值直接输入该字段。

安全 IP 地址掩码
指定一个掩码，类似于一个子网掩码指定了安全 IP 地址中的位，用于标识一个 IP 地址范围。这些掩码中的二进制位若设置为 0 表示该二进制位上是一个 0，若设置为 1 表示该位包含于 IP 地址范围之内。所以，在掩码中指定 255.255.255.255 表明仅有一个安全 IP 地址是包含在这个转换项内的，但是 255.255.255.0 的掩码表明 C 类 IP 地址都需要地址转换。

排除安全网络地址

一个排除安全 IP 地址项定义了不需要 NAT 执行 IP 地址转换的安全网络地址集。 缺省情况下，NAT 执行转换安全 IP 地址集中所有安全 IP 地址的地址转换。

如果您从**添加 NAT 配置**对话框屏幕中选择了排除，请输入下列值:

安全 IP 地址
指定一个点十进制 IP 地址，来标识应该从网络地址转换中排除的安全 IP 地址的范围。

要选择一个网络对象，请单击**选择**获得**选择网络对象**对话框。选择一个网络对象并单击**确认**。在**添加 NAT 配置**对话框的网络对象字段中就添加了该网络对象。或者，如果没有预先创建网络对象，则将值直接输入该字段。

安全 IP 地址掩码
指定一个掩码，类似于一个子网掩码指定了安全 IP 地址中的位，用于标识一个 IP 地址范围。这些掩码中的二进制位若设置为 0 表示该二进制位上是一个 0，若设置为 1 表示该位包含于 IP 地址范围之内。所以，在掩码中指定 255.255.255.255 表明在此项中只指定了一个安全 IP 地址，但是掩码 255.255.255.0 表明从地址转换中排除了 C 类 IP 地址。

映射安全网络地址

映射安全 IP 地址项定义了从安全 IP 地址到已注册 IP 地址的一对一的映射。 这个一对一的 IP 地址映射允许外部应用程序客户，例如 FTP 或 telnet 客户，与安全网络内部的服务器建立 TCP 会话。在映射安全 IP 地址项中的已注册 IP 地址，能重叠由保留已注册 IP 地址项指定的 IP 地址空间。

如果您从**添加 NAT 配置**对话框中选择了映射，请输入下列值:

安全 IP 地址
将被转换成指定的已注册 IP 地址的点十进制 IP 地址。

要选择一个网络对象，请单击**选择**获得**选择网络对象**对话框。选择一个网络对象并单击**确认**。在**添加 NAT 配置**对话框的网络对象字段中就添加了该网络对象。或者，如果没有预先创建网络对象，则将值直接输入该字段。

已注册 IP 地址字段
指定的安全 IP 地址将被转换成的点十进制 IP 地址。

要选择一个网络对象，请单击**选择**获得**选择网络对象**对话框。选择一个网络对象并单击**确认**。在**添加 NAT 配置**对话框的网络对象字段中就添加了该网络对象。

更改 NAT 项

从 **NAT 配置**对话框中选择一个现存的 NAT 项，并单击**打开**以在 NAT 配置文件中更改网络转换项。

删除 NAT 项

1. 从 **NAT 配置**对话框中选择一个现存的 NAT 项，并单击**删除**以在 NAT 配置文件中删除网络转换项。

   出现一个确认对话框。
2. 选择“是”或“否”。

NAT 激活

1. 从配置客户程序浏览树中，双击“地址转换文件”文件夹图标以扩充视图。双击“NAT 文件”文件夹图标来扩充视图。
2. 选择 **NAT 激活**，将出现一个和第109页的图 34相似的对话框。

图 34. NAT 激活

3. 您可以选择下列中的任意一个并单击**执行**:
   - 验证包含在指定的 NAT 配置文件中的网络地址转换项。

- 激活/更新配置以显示 NAT 模块当前使用的网络地址转换项。
- 释放 NAT 以禁用网络地址转换。
- 启用日志以启用网络地址转换记录。
- 禁用日志以禁用网络地址转换记录。

记录

假如同时启用了 NAT 记录和过滤器记录，NAT 将记录各种不同的错误条件。通过 **NAT 激活**面板或使用 **fwnat** 命令来启用 NAT 记录。通过**日志设施**面板或使用 **fwlog** 命令来启用过滤器记录。

下列活动将被记录到防火墙日志设施:

- 管理员所做的 NAT 表的更新(例如，静态项或 MAP 项)
- NAT 转换表的动态更新
- 错误信息
- 导致包被废弃的失败转换尝试
- 每次激活和释放 NAT

创建 NAT 的过滤器规则

当您已完成 NAT 配置后，必须为将使用 NAT 的连接创建过滤器规则。复查第39页的『第8章 控制通过 Firewall 的通信』，并使用用于直接连接的预定义服务。用于直接连接的预定义服务的实例为:

- HTTP direct out
- Telnet direct out

请参阅第40页的『使用预定义服务建立连接』以获取详细信息。

如果想要直接进入网络的服务，则必须创建一个。请参阅第60页的『使用配置客户程序创建服务』以获得详细信息。

附录. 注意事项

本出版物中对 IBM 产品、程序或服务的引用并不意味 IBM 打算在其运作的所有国家推出。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。根据 IBM 有效知识产权或其它受法律保护的权利，任何具有等价功能的产品、程序或服务均可以用来替代 IBM 的产品、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。

对于本文档中涉及的内容材料，IBM 可能拥有专利或未决专利的申请。本文档的提供并未给予您关于这些专利的任何许可。您可以以书面方式将许可查询发送至:

IBM Director of Licensing

IBM Corporation

500 Columbus Avenue

Thornwood, NY 10594

USA

本程序的许可证持有人，如欲获得有关的信息以能够: （i）在各自建立的程序与其它程序（包括本程序）之间交换信息以及 （ii）相互使用已交换的信息，请联系:

IBM Corporation
P.O. Box 12195
3039 Cornwallis
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。

本文档中描述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。

本文档不打算为生产使用，其供给不带任何形式的担保，因此我们拒绝一切保证，包括可销售性担保与对一个特定用途的适宜性。

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

下列术语为 IBM 公司在美国或其它国家的商标:

- 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。

Java 和 HotJava 是 Sun Microsystems 公司的商标。

其它可能由双星号表示的公司、产品和服务名称可能是其它公司的商标或服务标记。

文献目录

要得到 Internet 安全性的附加信息，访问 IBM eNetwork Firewall 主页，它在 **http://www.software.ibm.com/enetwork/firewall**

IBM 出版物信息

其它关于防火墙、Internet 安全性和常规安全性问题的 IBM 信息源都列出在这里。

防火墙主题

下列文档在 IBM Firewall CD-ROM 和 IBM eNetwork Firewall 主页上都可得到。

- *IBM eNetwork Firewall 用户指南*, GA31-1909
- *IBM eNetwork Firewall 参考大全*, SA31-1911
- *使用 IBM eNetwork Firewall NT 版本 3.2 防守门户（Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2）*, SG24-5209

Internet 和 World Wide Web 主题

- *Internet 连接服务器指南(A Guide to the Internet Connection Servers)*, SG24-4805
- *从 World Wide Web 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 的基础机构 (Building the Infrastructure for the Internet)*, SG24-4824
- *AS/400 和 Internet 流行主题(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 的示例(Examples of Using MQSeries on WWW)*, SG24-4882
- *如何保护 MVS/ESA 的 Internet 连接服务器(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
- *通过 Web 运行 CICS 事务: 到 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: 如何建立安全的 World Wide Web 连接 (Safe Surfing: How to Build a Secure World Wide Web Connection)*, SG24-4564
- *自学用 PERL 进行 CGI 编程七日通(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 访问 DB2 (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
- *安全性元素: AIX V4.1 (Elements of Security: AIX V4.1)*, GG24-4433
- *企业范围安全性体系结构和解决方案呈示指南 (Enterprise-Wide Security Architecture and Solutions Presentation Guide)*, SG24-4579
- *HACMP/6000 定制示例 (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: 保护开放的客户机/服务器分布企业(IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise)*, SC24-8135
- *IBM 系统监视器: 一个智能的代理结构 (IBM Systems Monitor: Anatomy of a Smart Agent)*, SG24-4398
- *开放系统联网的安全性概述 (Security Overview of Open Systems Networking)*, GG24-3815

- *AIX 系统监视器用户指南 (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

工业出版物信息

以下出版物都涉及到了 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）

词汇表

可 在 :
http://www.networking.ibm.com/nsg/nsgmain.htm
访问 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。

[M]

[P]

[Q]

[R]

[S]

[T]

[W]

[X]

[Y]

[Z]

读者意见表

IBM eNetwork Firewall Windows NT 版
用户指南
版本 3 发行版 2.1.1

GA31-1909-01

姓名

地址

单位及部门

电话号码

读者意见表

GA31-1909-01

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 公司
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

GA31-1909-01

请沿此线
撕下或折起

Printed in China

GA31-1909-01