瑞星防毒墙使用手册

——for RSW System 2.0 Version

We provide detailed guides about using RISING Antivirus gateway in this handbook. All operations and functionalities are involved. RISING assumes that you have read this manual carefully before running your devices.

北京瑞星信息技术有限公司

重 要 声 明

感谢您购买北京瑞星信息技术有限公司出品的瑞星防毒墙。请在安装本产品之前认真阅读配套的使用手册，本手册根据瑞星防毒墙软件版本号 2.0.16288 编写，适用于瑞星 RSW-1200、RSW-3200、RSW-9200、RSW-9300 防毒墙。当您开始使用本产品时，瑞星公司认为您已经阅读了本使用手册。

作为计算机病毒清除工具和网络安全防护工具，瑞星公司研制销售的防毒墙产品将不断地升级。无论是功能的增加、性能的提高，还是清除病毒种类的增加都关系到产品的实际使用效果。因此，您在使用本产品过程中应随时与瑞星公司保持联系，以便及时获得升级程序或更新换代产品。

随着产品不断升级，本手册内容将会有所修改，恕不另行通知。您可以从瑞星网站 http://www.rising.com.cn 下载到本使用手册的最新版本。

感谢您购买北京瑞星信息技术有限公司研制开发的网络安全产品！

北京瑞星信息技术有限公司

2008 年 5 月

公司简介

瑞星品牌诞生于 1991 年刚刚在经济改革中蹒跚起步的中关村，是中国最早的计算机反病毒标志。瑞星公司历史上几经重组，已形成一支中国最大的反病毒队伍。瑞星以研究、开发、生产及销售计算机反病毒产品、网络安全产品和反“黑客”防治产品为主，拥有全部自主知识产权和多项专利技术。

目前，瑞星公司已推出基于多种操作系统的瑞星杀毒软件单机版、网络版软件产品；以及企业防毒墙、防火墙、网络安全预警系统等硬件产品，是全球第三家、也是国内唯一一家可以提供全系列信息安全产品和服务的专业厂商。

在公安部组织的计算机病毒防治产品评测中，“瑞星杀毒软件”单机版、网络版曾双双荣获总分第一的殊荣，并连续 5 年蝉联至今。公司拥有国内最大、最具实力的反病毒和网络安全研发队伍，并且拥有国内安全行业唯一的“电信级”呼叫服务中心和“在线专家门诊”Online 服务系统。

瑞星和政府机构、商业伙伴以及媒体有着广泛而深入的合作关系，借助内外部各种资源，目前已建成五大安全网络体系——全球计算机病毒监测网、全球计算机病毒应急处理网、全国计算机病毒预报网、全国反病毒服务网以及全球病毒疫情监测网。

瑞星公司总部设立在北京，在全国各地设有分支机构。目前公司拥有国内最大的信息安全研发团队、国内最大的客户服务团队，以及销售、市场、网站等部门，并已经建成覆盖全国的庞大的销售和市场体系。

目前瑞星拥有 6000 万正版个人用户，7 万多家企业用户，主要软件产品以中（简、繁体）、英、俄、德、日五种语言版本推向全球市场，销售网络覆盖北美、欧洲、亚太等地区。作为在中关村成长起来的高科技企业，瑞星正逐步走向世界，实现公司的美好愿景——成为全球最具价值的信息安全产品和服务提供商。

目　录

前 言

为了防止病毒对网络的侵扰，瑞星公司将专业的基于应用层的安全技术引入到防毒墙当中，形成防毒、防火以及 IDS 一体化的综合安全网关产品。瑞星防毒墙的产品共分为 3 个系列（1 系列、3 系列和 9 系列），可分别适用于 SOHO 用户，小型、中型或大型企业的网络环境。关于瑞星防毒墙的更多信息，请访问：http://hardware.rising.com.cn。

建议您在使用瑞星防毒墙之前，仔细阅读本使用手册。通过本手册，您可以熟悉瑞星防毒墙的安装方法，并了解如何使用瑞星防毒墙对计算机病毒、黑客攻击等进行防范。

关于本使用手册中特殊标记及缩略语的说明：

- 本手册语言为中文，但一些专业术语可能会使用英文缩写。关于这些缩写的详细解释可参见瑞星防毒墙使用手册 APPENDIX2 专业术语表
- 本手册中“计算机病毒”简称为“病毒”
- 本手册中“单击”指单击鼠标左键
- 本手册中的“注意”表示为意外或可能引起重大损失的情况，请用户特别注意；“提示”则为一些帮助用户管理和使用防毒墙的经验

第一章 准备工作

安装瑞星防毒墙之前应做好下面两项准备工作：

- 企业网络规划：部署防毒墙前，对企业网络进行规划
- 网络参数确定：确定企业网络已经存在网络设备的具体情况

1.1 企业网络规划

用户在安装和使用瑞星防毒墙之前应该首先对本企业网络进行整体规划，确定网络拓扑结构，制定企业安全策略，便于日后进行更好的管理。

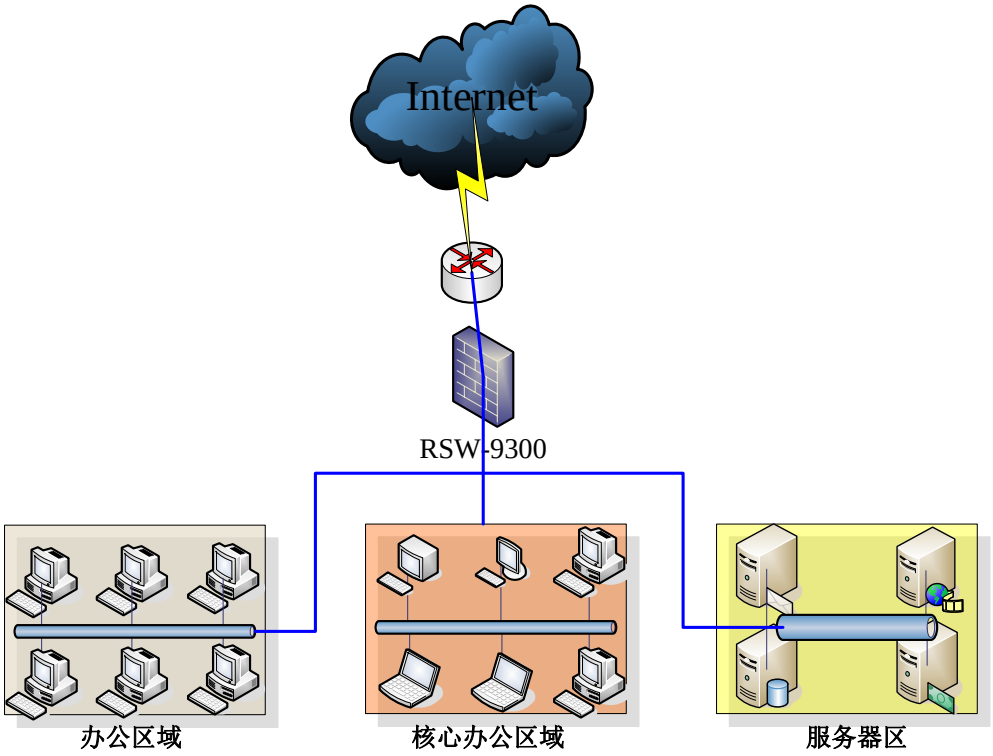


图 1.1 网络结构图

一般情况下，使用瑞星防毒墙的网络拓扑结构可以参照图 1.1 进行规划。这是我们在测试瑞星防毒墙时使用的实际网络结构。在图 1.1 中，Internet 为非安全区网络。实际应用中，任何应重点保护的子网与其他不信任网络相连时，都可以考虑使用防毒墙进行隔离。

之所以要将企业网络划分为内部安全区网络和 DMZ 区网络，是为了保证对外提供公开服务的服务器主机（如企业的 web 服务器、ftp 服务器、邮件服务器等）与其它不提供对外服务的主机分开。这样既便于集中管理，还可将风险隔离。由于对外提供服务的主机势必要比内部不提供对外服务的主机暴露给外面的信息要多，这就使这些对外主机更容易遭受外部黑客的攻击。如果将这些服务器集中放在 DMZ 区，即使它们遭到攻击，也不会危及内部安全区网络各主机的安全。内部安全区网络和 DMZ 区网络都是防毒墙保护的安全网络。

1.2 网络参数确定

规划好网络部署结构之后，还需要具体定义网络参数。如果选择网桥模式，只需为防毒墙分配一个用

于管理的 IP 地址；如果选择路由模式，则必须确定以下各项内容（可以从 3.1.1 接口模式及区域配置中获得关于防毒墙工作模式的详细信息）：

- 与外网连接的网关或路由器地址
- 防毒墙外网接口的域名、IP 地址、子网掩码、网络地址及广播地址
- 防毒墙内网接口的域名、IP 地址、子网掩码、网络地址及广播地址
- 防毒墙 DMZ 接口的域名、IP 地址、子网掩码、网络地址及广播地址
- 外部域名服务器地址及域名解析
- 内部域名服务器地址及域名解析
- 企业安全策略，如：网桥模式下是否允许跨网桥进行 Windows 登录；是否启用 DHCP；路由模式下是否允许从外网向内部网络进行 SSH 和 FTP；路由模式下，内部用户访问外网是否要求用户进行身份认证以及是否进行时间限制和内容限制；本企业必须使用的协议和服务等等

这些参数确定之后，就可以按照网络结构图部署瑞星防毒墙了。为使瑞星防毒墙能与企业网络协同工作，必须对其进行配置。其中包括防毒墙系统配置和企业安全策略的实施，这些将在下面的章节中陆续讲述。

第二章 登录防毒墙管理界面

瑞星防毒墙提供两种管理模式：串行接口模式和 Web 模式。本章介绍通过 Web 方式登录防毒墙的操作以及防毒墙的管理菜单。主要内容有：

- 登录防毒墙前的准备工作：登录防毒墙前需要进行的准备工作
- 登录防毒墙：如何登录瑞星防毒墙
- 防毒墙的管理菜单：了解瑞星防毒墙的功能项

2.1 登录防毒墙前的准备工作

建议用户使用 Internet Explorer 6.0 或更高版本浏览器。

为了创建一个到您的工作站的安全连接，瑞星防毒墙使用了安全套接层（SSL）协议（2.0 或 3.0 版本）。在防毒墙连接期间，所有的交换信息均被 SSL 加密，默认的访问端口为 443。

为了保证您能够访问瑞星防毒墙的管理界面，您的管理计算机必须有一个与防毒墙管理口（即和管理计算机相连的网口）在同一网段内的 IP 地址，并将管理计算机和防毒墙用随机附带的交叉线连接。

瑞星防毒墙 RSW-1200/3200 默认接口配置

接口	所属区域	接口模式	IP 地址/子网掩码
E0	WAN	网桥 1（br0）	1.1.1.1/32
E1	LAN	网桥 1（br0）	
E2	DMZ	静态 IP（Static）	192.168.100.244/24
E3	LAN	静态 IP（Static）	192.168.2.1/24

表 2.1 防毒墙出厂信息

瑞星防毒墙 RSW-9200 默认接口配置

接口	所属区域	接口模式	IP 地址/子网掩码
E0	WAN	网桥 1（br0）	1.1.1.1/32
E1	LAN	网桥 1（br0）	
E2	WAN	网桥 2（br1）	1.1.2.1/32
E3	DMZ	网桥 2（br1）	
E4		禁用（Disable）	
E5		禁用（Disable）	
E6	DMZ	静态 IP（Static）	192.168.100.244/24
E7	LAN	静态 IP（Static）	192.168.2.1/24

表 2.2 防毒墙出厂信息

瑞星防毒墙 RSW-9300 默认接口配置

接口	所属区域	接口模式	IP 地址/子网掩码
E0	WAN	网桥 1（br0）	1.1.1.1/32
E1	LAN	网桥 1（br0）	
E2	WAN	网桥 2（br1）	1.1.2.1/32

E3	DMZ	网桥 2（br1）	
E4	LAN	禁用（Disable）	
E5	LAN	禁用（Disable）	
E6	LAN	禁用（Disable）	
E7	LAN	禁用（Disable）	
E8	DMZ	静态 IP（Static）	192.168.100.244/24
E9	LAN	静态 IP（Static）	192.168.2.1/24

表 2.3 防毒墙出厂信息

默认情况下应将管理计算机 IP 地址设置为 192.168.2.*（*为 2~254 的任意数字，这里我们假设用户用 E3 口作为管理口，其地址为 192.168.2.1），子网掩码为 255.255.255.0，默认网关为 192.168.2.1。如图 2.1 所示。

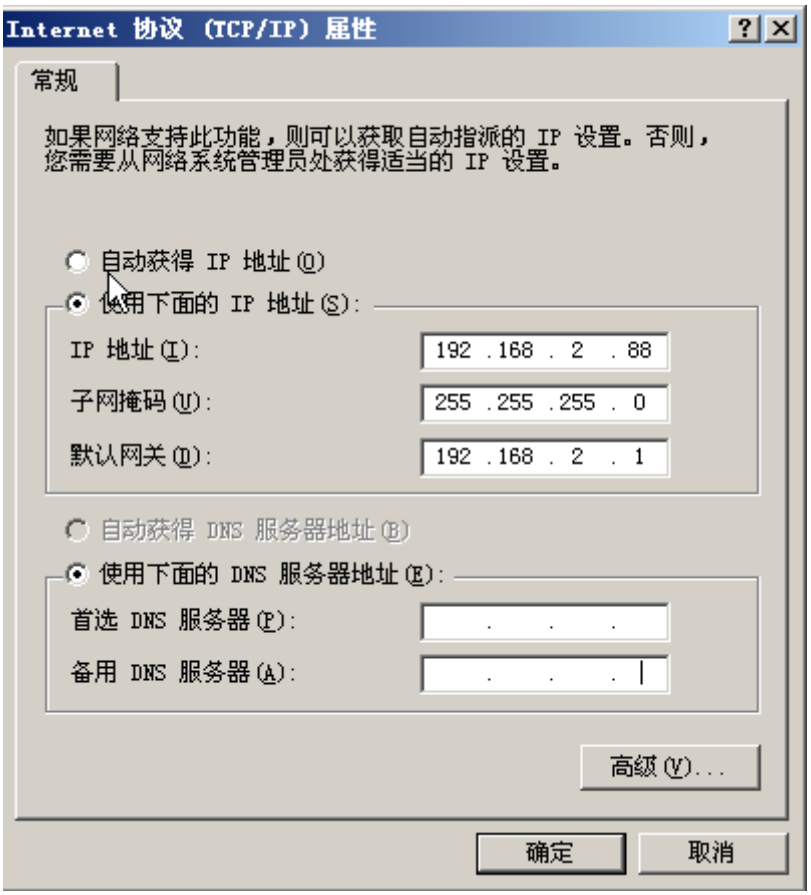


图 2.1 设置主机 IP 地址

2.2 登录防毒墙

当用户尝试登录管理界面时，会显示一个认证框。用户需要输入有效的用户名和密码以完成认证。有关如何在防毒墙中增加用户帐号请参阅本使用手册 5.1.1 帐号管理。

1. 在浏览器地址栏中，输入 https://192.168.2.1 （防毒墙管理口的地址），Web 浏览器会自动弹出一个安全警报，如图 2.2 所示

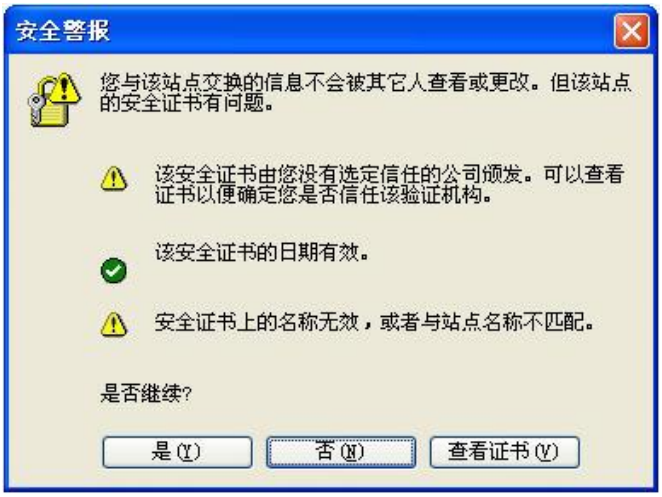


图 2.2 防毒墙证书

提示：当用户使用 IE7.0 或更高版本的浏览器时，会出现以下警告，如图 2.3 所示，此时，请单击继续浏览此网站(英文提示为：Continue to this website)，便可以看到防毒墙的登录界面了。

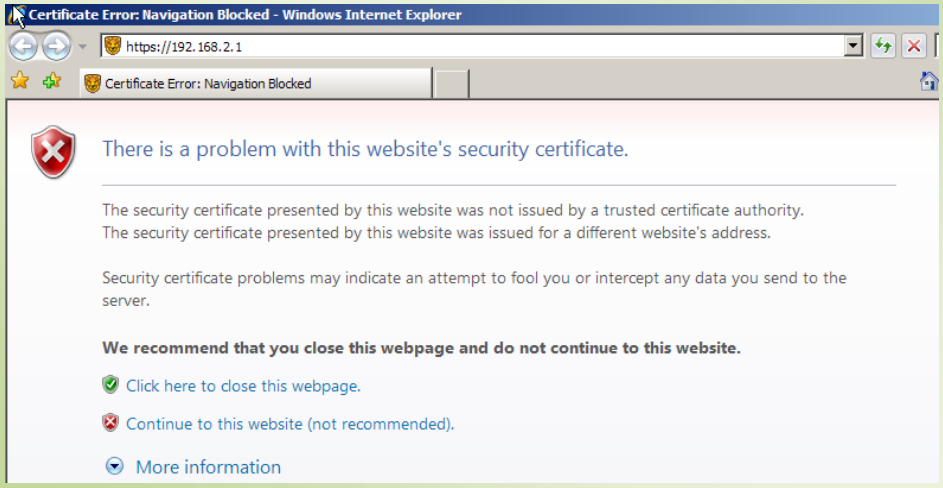


图 2.3 警告信息

2. 选择信任证书，进入防毒墙登录界面。如图 2.4 所示

图 2.4 防毒墙系统登录界面

3. 在用户名栏中，输入用户名：admin

4. 在密码栏中，输入默认密码：admin

5. 单击【登录】，进入瑞星防毒墙网页管理界面，并显示当前防毒墙系统运行的主要信息，如图 2.5 所示

注意：建议登录后立即修改默认密码。关于如何修改防毒墙的用户密码请参考 5.1.1 帐号管理。

图 2.5 防毒墙管理界面

防毒墙基本信息快速浏览		
系统资源	CPU 使用率	显示当前防毒墙系统 CPU 使用率
	内存使用率	显示当前防毒墙系统内存使用率
	硬盘占用率	显示当前防毒墙系统硬盘占用率
系统状态	设备编号	显示当前防毒墙设备编号
	设备名称	显示当前防毒墙设备名称，单击【更改】进入修改设备名称页面，如何修改请参见本手册
	联系 EMAIL	显示当前防毒墙设备联系人 Email 地址，单击【更改】进入修改联系人 Email 地址页面，如何修改请参见本手册
	系统时间	显示当前防毒墙系统时间，单击【更改】进入修改系统时间页面，如何修改请参见本手册
	运行时间	显示当前防毒墙系统无故障运行时间
	系统版本	显示当前防毒墙系统软件版本，单击【升级】进入防毒墙系统升级页面，如何进行防毒墙系统升级请参见本手册
	反病毒引擎	此处会显示当前防毒墙系统反病毒引擎正常工作的期限，如果超出服务时间，请重新购买反病毒服务并进行注册。在您使用瑞星防毒墙的各种升级服务之前，您必须进行服务激活，单击【激活】进行在线服务激活,具体的激活步骤请参见《快速使用指南》
	病毒库版本	显示当前反病毒引擎病毒库的版本，单击【升级】进入防毒墙病毒库升级页面，如何进行防毒墙病毒库升级请参见本手册 4.3 软件升级
	反垃圾引擎	该选项只有在您购买了反垃圾邮件授权后才显示，请在第一次登录防毒墙时输入购买的反垃圾引擎序列号，此处会显示当前防毒墙系统反垃圾引擎正常工作的期限，如果超出服务时间，请重新购买反垃圾服务并进行注册，单击【授权】输入反垃圾引擎序列号，产品激活流程参见《快速安装指南》
	连接数	显示当前客户端与防毒墙建立连接的数目
	在线管理员	显示当前防毒墙在线管理员的数目，单击【查看】进入在线用户管理页面，如何进行在线用户管理请参见本手册 5.1.2 在线用户管理
告警信息	显示防毒墙系统的告警信息	
接口配置信息	显示防毒墙各个网口的状态信息	
统计信息	显示防毒墙 Http、Ftp、Smtp、Pop3、Msn 和 Imap 过滤信息	
内网主机上传 Top5	显示防毒墙内主机一天中上传前五名客户端信息，单击【详细】链接到流量查看详细信息页面	
内网主机下载 Top5	显示防毒墙内主机一天中下载前五名客户端信息，单击【详细】链接到流量查看详细信息页面	
历史统计报告查看	管理员可以按照日报、周报和月报的汇总方式查看防毒墙运行的详细信息	
定时刷新	设定系统状态页面定时刷新的时间	

表 2.4 防毒墙基本信息快速浏览

提示：快速跳转至防毒墙基本信息页面

如果管理员正在浏览防毒墙其他配置页面，单击浏览器的刷新按钮能够快速返回到防毒墙基本信息页面。

2.3 防毒墙管理菜单

防毒墙管理分为十三项功能区域，每一项功能都由菜单区和相应的主页面构成：

- 主页面：显示各个功能模块的管理页面，可对防毒墙进行相关的配置和设置
- 菜单区：弹出式菜单。鼠标悬停在菜单栏上，右侧会弹出二级子菜单。如图 2.6 所示

图 2.6 防毒墙的功能菜单

各个菜单中包含的项目：

- **网络配置**：接口配置、出口配置、DNS 配置、网桥配置、路由配置、策略路由、DHCP 配置、网络诊断
- **系统管理**： 系统状态、系统时间、软件升级、系统维护、设备配置、DDNS 配置、DNS 代理、TCP/IP 选项
- **管理配置**：帐号配置、管理主机配置、SNMP 配置、集中管理、热备配置
- **防毒配置**：防病毒配置、HTTP 白名单、邮件白名单
- **垃圾邮件（可选模块）**：垃圾邮件判定和垃圾邮件摘要发送
- **对象管理**：地址、地址组、时间、时间组、服务、服务组
- **应用协议**：自动识别、预定义、识别结果

- **防火墙**：安全策略编辑、内容过滤规则、URL 过滤配置、URL 攻击防御、入侵防御、IP 黑名单、安全策略分析、连接信息管理、MAC 地址管理
- **地址转换**：包含源地址转换和目的地址转换的设置
- **VPN 配置**：SA 配置、VPN 通道、通道状态、L2TP 设置、PPTP 设置、SSL VPN 配置、用户设置
- **流量管理**：统计配置、控制配置、流量查看、流量分析、带宽管理
- **日志审计**：病毒日志、垃圾邮件、隔离文件、管理日志、系统日志、网络日志、URL 日志、可疑文件、入侵日志、告警配置
- **退出**：退出防毒墙的管理

第三章 网络配置

本章主要介绍和防毒墙接口相关的设置。主要由以下八个模块构成：

- 接口配置：定义接口工作模式、所属网络区域和接口配置信息
- 出口配置：进行防毒墙出口管理
- DNS 配置：配置防毒墙 DNS 解析服务器地址
- 网桥配置：进行防毒墙网桥管理
- 路由配置：定义防毒墙路由表
- 策略路由：定义特殊地址的路由表
- DHCP 配置：防毒墙为客户端提供 DHCP 服务的配置
- 网络诊断：进行防毒墙设备网络诊断

3.1 接口配置

在导航菜单中，单击【网络配置】➔【接口配置】进入配置页面，如图 3.1 所示。

图 3.1 防毒墙接口配置页面

3.1.1 接口模式及区域配置

将鼠标悬停在要设置的接口上，会弹出该接口的工作模式或区域菜单，如图 3.2 所示。

图 3.2 防毒墙接口拓扑和区域配置

这个菜单分为两部分：上面的一排网口图标用于设置网口的工作模式（并不对应真实的网口）。下面的红、绿和黄色的方块用于设置网口处于的网络区域。其中：

网口的工作模式	说明
网桥 1	用户可以选定一对防毒墙接口作为一个网桥，不需要任何其他配置就可以让防毒墙工作。当用户在不想改变现有网络拓扑结构的前提下使用防毒墙的各种功能时，可以选择该模式。防毒墙的这种工作模式也被称为“透明模式”。
网桥 2	防毒墙内置了两个独立的网桥。功能同“网桥 1”。
PPPoE	当用户通过 ADSL 连接到 Internet 时，可以把防毒墙的一个接口设置成 PPPoE 模式并将该接口与 ADSL modem 连接，这样防毒墙的其他网口可以通过防毒墙的地址转换服务与 Intenet 进行连接。
静态 IP	为防毒墙的网口配置一个静态的 IP。当用户需要： 1. 通过该网口管理防毒墙 2. 通过该网口提供网络服务（DHCP / NAT 等）时，需要把网口的工作模式设定成静态 IP 模式。这种工作模式也被称为“路由模式”。
DHCP	如果防毒墙的接口位于一个通过 DHCP 自动分配地址的网络中，可以把该接口配置成 DHCP 模式，让防毒墙自动获得 IP 地址，避免 IP 地址冲突（注：不要和防毒墙提供的 DHCP 服务混淆）。
禁用	如果不想使用防毒墙的某个接口，可以选择最后一项，禁用该接口

表 3.1 防毒墙网口的工作模式

网口的工作区域	说明
WAN	直接和 Internet 连接的网口，也被称为“外网口”。
LAN	和企业内部局域网相连的网口，也被称为“内网口”。
DMZ	如果企业有对外提供公开服务的服务器主机（如企业的 web 服务器、ftp 服务器、邮件服务器等），为了安全考虑，应该把他们与其它不提供对外服务的主机分开。连接这些对外提供服务的主机构成的网络的网口，称为 DMZ。

表 3.2 防毒墙网口的工作区域

用户可以根据自己实际的网络情况，对网口的工作模式和工作区域进行设置，只有把这两个内容都设置完后，网口才能正常工作。

提示：关于接口配置

- 当把防毒墙接口设置成网桥模式后，防毒墙在网络中是完全透明的。根据实际网络环境的不同，网桥设置有所不同。首先需要根据实际情况定义网桥模式下两个接口的工作区域，即一个接口工作在 WAN 区，另一个接口工作在 LAN 区或 DMZ 区。另外，网桥必须有一个 IP 地址，当网桥工作在二层透明模式下，网桥 IP 地址可以随意填写，只需为其增加一个可以到达的默认路由地址即可；当网桥工作在三层透明模式下，网桥 IP 地址必须为局域网内合法有效可路由的 IP 地址。
- 防毒墙接口的 PPPoE 以及 DHCP 模式只能工作在 WAN 区，当想把防毒墙的接口设置成这两种工作模式的时候，需要先把网口的区域设置成 WAN

例：内网用户通过 ADSL 上网的典型配置方法

网络拓扑结构

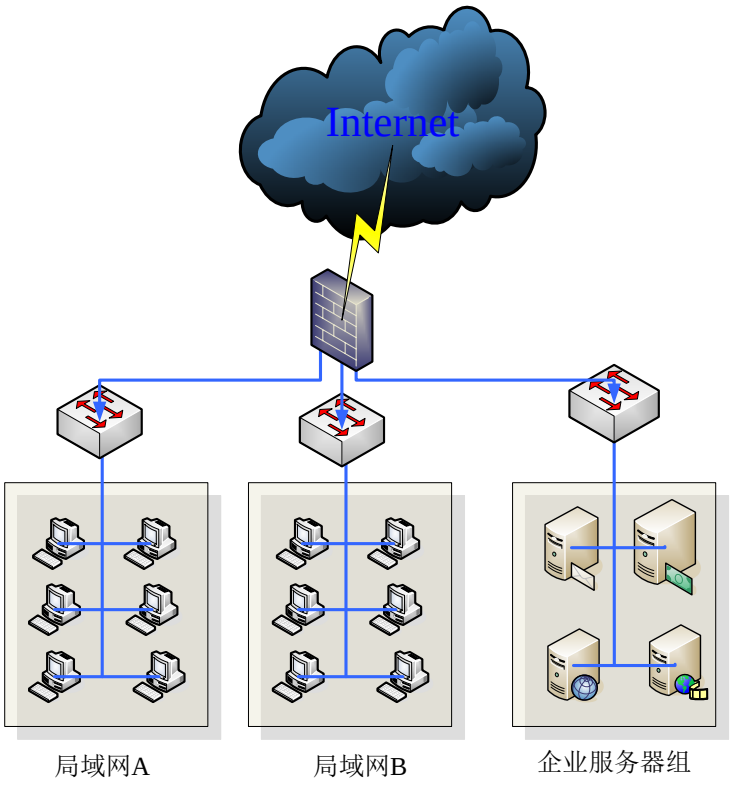


图 3.3 防毒墙 ADSL 工作模式拓扑结构

- 将 E0 接口设置为 PPPoE，区域为 WAN

1. 将鼠标悬停在 E0 接口上，选择该接口工作区域为 WAN

2. 在弹出的确认更改接口工作区域设置更改对话框中，单击【确定】按钮，如图 3.4 所示

图 3.4 确认接口区域设置更改

3. 将鼠标悬停在 E0 接口上，选择该接口工作模式为 PPPoE

4. 在弹出的确认接口工作模式更改对话框中，单击【确定】按钮，如图 3.5 所示

图 3.5 确认接口工作模式更改

- 按照上面相同的步骤将 E1 接口设置成静态 IP，区域为 LAN

提示：关于接口配置

我们这里只设置了接口的工作模式（PPPoE/静态 IP），为了让接口正常工作，还需要设置这两种模式的其他相关信息。对于 PPPoE 的更多设置，请参考 3.2 出口配置；对于静态 IP 的更多设置，请参考 3.1.3 接口配置。

3.1.2 接口列表

当配置好接口后，防毒墙会自动显示关于接口的详细信息。如图 3.6 所示。

接口列表

序号	接口	区域	模式	IP地址	物理地址	连接状态	自适应	带宽	全/半双工	MTU	操作
1	E0	WAN	BR0	-	00:90:fb:15:27:c8		on	1000	unknown	1500	
2	E1	LAN	BR0	-	00:90:fb:15:27:c9		on	1000	unknown	1500	
3	E2	WAN	BR1	-	00:90:fb:15:27:ca		on	1000	unknown	1500	
4	E3	DMZ	BR1	-	00:90:fb:15:27:cb		on	1000	unknown	1500	
5	E4	LAN	STATIC	-	00:90:fb:13:9f:70		on	1000	unknown	1500	
6	E5	LAN	DISABLE	-	00:90:fb:13:9f:71		on	1000	unknown	1500	-
7	E6	LAN	DISABLE	-	00:90:fb:13:9f:72		on	1000	unknown	1500	-
8	E7	LAN	DISABLE	-	00:90:fb:13:9f:73		on	1000	unknown	1500	-
9	E8	LAN	STATIC	193.168.20.215/24	00:90:fb:14:88:38		on	1000	Full	1500	
10	E9	LAN	STATIC	192.168.2.1/24	00:90:fb:14:88:39		on	1000	unknown	1500	

增加VLAN 删除VLAN

图 3.6 防毒墙接口列表

字段	说明

序号	该接口的顺序号
接口	接口的名称
区域	此接口的安全设置区域。WAN 对应非安全区域；LAN 对应安全区域；DMZ 对应中立区域
模式	该接口的工作模式。BR0 / BR1 对应网桥模式；STATIC 对应静态 IP 模式；DHCP 对应 DHCP 模式；PPPoE 对应 PPPoE 模式；DISABLE 为禁用模式，该接口不可用
IP 地址	该接口的 IP 地址
物理地址	网卡的 MAC 地址
连接状态	代表当前接口状态为连接； 代表当前接口状态为非连接
自适应	自动检测当前网络的连接带宽的大小
带宽	当前网络接口的带宽值
全/半双工	当前网络接口是否提供双通道模式。全双工即双通道模式；半双工即单通道模式
MTU	MTU 是 Maximum Transmission Unit 的缩写。意思是网络上传送的最大数据包，MTU 的单位是字节
操作	单击 图标可对当前网络接口的参数进行配置，详见 3.1.3 接口配置
增加 VLAN	在防毒墙的一个网口上增加 VLAN
删除 VLAN	删除某个网口的 VLAN

表 3.3 接口列表参数说明

3.1.2.1 增加一个 VLAN

单击【增加 VLAN】按钮，打开增加 VLAN 页面，如图 3.7 所示。

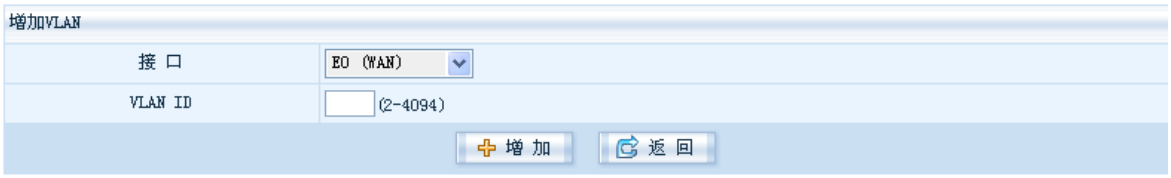


图 3.7 增加 VLAN

- 接口：VLAN 绑定的物理网口
- VLAN ID：标识 VLAN 的 ID

3.1.2.2 删除一个 VLAN

选定要删除的 VLAN，单击【删除 VLAN】按钮，如图 3.8 所示。

图 3.8 删除 VLAN

提示：关于 VLAN

利用 VLAN 可以有效的控制网络中的数据广播，用户可以在瑞星防毒墙的一个接口上设置多个 VLAN，之后防毒墙可以利用 VLAN Trunk 技术自动实现多个 VLAN 之间的路由。

3.1.2.3 修改已划分 VLAN 设置

单击图标可对当前网络接口的参数进行配置，详见 3.1.3 接口配置。

3.1.3 接口配置

单击接口列表中的图标，可以查看和修改相关的网口配置，如图 3.9 所示。

图 3.9 防毒墙网络接口配置

字段	说明
IP 地址列表	显示或管理当前接口的 IP 地址信息
接口信息	显示当前接口数据流量的详细信息
接口服务	设置接口提供的服务
接口防御	设置接口可以提供的攻击防御
链路设置	调整网卡的链路参数

表 3.4 接口配置功能说明

提示：关于网口的工作模式的影响

网口的工作模式会影响 IP 地址列表中的操作。

- **IP 地址列表**

这个 Tab 显示了网口当前的 IP 地址信息，当网口工作在 DHCP/网桥模式时，只能在这里显示网口的 IP 信息，如图 3.10 所示。

图 3.10 DHCP/PPPoE/网桥模式下的 IP 地址列表

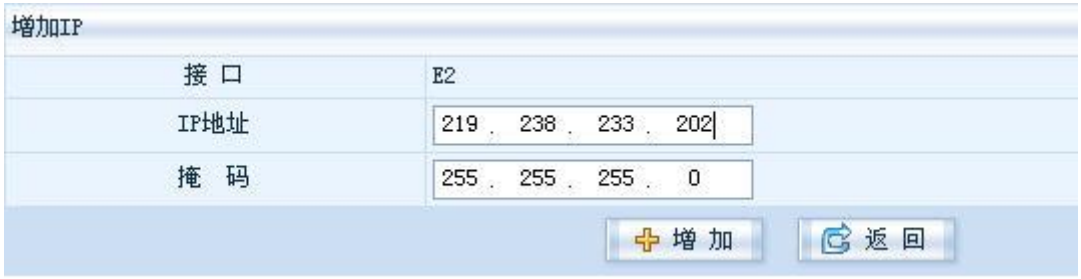
当网口工作在静态 IP 模式时，除了查看 IP 地址外，用户还可以通过单击【增加】/【删除】按钮修改网口的 IP 地址。

图 3.11 静态 IP 模式的 IP 地址列表 Tab

【增加】/【删除】按钮可以允许用户在一个网卡上绑定或删除多个 IP 地址。而每一个地址行右侧的图标则允许用户对当前网口的 IP 进行修改。

◆ 增加接口 IP 地址

在 IP 地址列表 Tab 中单击【增加】，设置当前接口的 IP 地址，如图 3.12 所示：



3.12 修改当前网络接口 IP 地址

1. 在 IP 地址处增加需要设置的 IP 地址
2. 设置子网掩码
3. 保存设置单击【确定】，取消操作单击【返回】

◆ 修改接口 IP 地址

在 IP 地址列表 Tab 中，单击图标，对当前存在的 IP 地址进行修改，如图 3.13 所示。

图 3.13 修改接口 IP 地址

在弹出的页面中：

1. 在 IP 地址处修改需要设置的 IP 地址
2. 修改子网掩码
3. 保存设置单击【确定】，取消操作单击【返回】

◆ 删除接口 IP 地址

要删除防毒墙接口某条 IP 地址记录，请选中该条记录前的复选框，单击【删除】。

当网口工作在 PPPoE 模式时，这部分内容为 PPPoE 管理，用户可以在这里设置 ADSL 拨号信息，如图 3.14 所示：

图 3.14 PPPoE 管理 TAB

图 3.14 各字段文字说明

项目	说明
用户名	进行 ADSL 拨号的用户名，一般由 ISP 提供
密码	进行 ADSL 拨号的密码，一般由 ISP 提供
重复密码	确认输入的 ADSL 拨号的密码
状态	分为未连接、连接中和已连接三种状态 ,未连接代表未进行 ADSL 连接、连接中表示正在进行 ADSL 连接、已连接表示已经建立 ADSL 连接
拨号模式	防毒墙 ADSL 拨号模式分为手动拨号和自动拨号两种模式。手动拨号通过管理员登录防毒墙，单

	击 连 接 进行 PPPoE 拨号，单击 断 开 断开 PPPoE 拨号；自动拨号功能通过防毒墙定时进行 PPPoE 拨号，节省计时付费客户的上网成本，根据客户的需要在特定的时间段进行 ADSL 连接，节约网络资源。

表 3.5 防毒墙 PPPoE 管理说明

用户填写完相关信息后，单击【应用】按钮保存配置，单击【连接】按钮连接 Internet，如图 3.15 所示。

图 3.15 启用 PPPoE 连接

当用户不需要使用 PPPoE 连接时，单击【断开】按钮断开 PPPoE 连接，如图 3.16 所示。

图 3.16 断开 PPPoE 连接

- **接口信息**

单击接口配置中的【接口信息】Tab，可以查看当前接口的数据流量，如图 3.17 所示：

图 3.17 防毒墙接口信息

- **接口服务**

> **提示：关于接口服务**
>
> 当防毒墙的接口工作在不同区域、不同模式时，接口可提供的服务是不同的。

单击接口配置中的【接口服务】Tab，可以查看并设置当前接口所处的工作模式下可以提供的服务。当选中相关服务时，防毒墙接口支持该项服务，反之则禁用该项服务。

◆ WAN 区：当防毒墙接口处于 WAN 时，防毒墙接口所提供的服务如图 3.18 所示：

图 3.18 WAN 区域接口服务

服务	说明
WEB	通过 Web 配置管理防毒墙
SSH	通过 SSH 配置管理防毒墙
SNMP	通过 SNMP 查看防毒墙信息
PING	响应 ping 命令
IPS	阻断恶意的网络通讯与防毒墙的连接
VPN	IPSEC VPN 远程接入
L2TP	通过第二层隧道协议在运行 Windows 操作系统的远程客户计算机和您的内部网络之间建立一个虚拟专用网络 VPN
PPTP	通过点对点隧道协议在运行 Windows 操作系统的远程客户计算机和您的内部网络之间建立一个虚拟专用网络 VPN
SSLVPN	基于安全套接层协议（Security Socket Layer）建立远程安全访问通道的 VPN 技术

表 3.6 WAN 区提供的服务列表

◆ LAN 区：当防毒墙接口处于 LAN 时，防毒墙接口所提供的服务如图 3.19 所示：

图 3.19 LAN 区域接口服务

字段	说明
WEB	通过 Web 配置管理防毒墙
SSH	通过 SSH 配置管理防毒墙
SNMP	通过 SNMP 查看防毒墙信息
PING	响应 Ping 命令
DHCPD	向该接口所在的网段内的计算机提供 DHCP 服务
DNSPROXY	向该接口所在的网段内的计算机提供 DNS 代理
IPS	阻断恶意的网络通讯与防毒墙的连接
默认 NAT	自动把该接口所在网段的地址，转换成 WAN 口的地址，提供内网的 Internet 访问

表 3.7 LAN 区提供的服务列表

◆ DMZ：通常该区域部署企业对外提供服务的服务器，该区域所提供的服务如图 3.20 所示：

图 3.20 DMZ 区域接口服务

字段	说明
WEB	通过 Web 配置管理防毒墙
SSH	通过 SSH 配置管理防毒墙
SNMP	通过 SNMP 查看防毒墙信息
PING	响应 ping 命令
DHCPD	向该接口所在的网段内的计算机提供 DHCP 服务
DNSPROXY	向该接口所在的网段内的计算机提供 DNS 代理
IPS	阻断恶意的网络通讯与防毒墙的连接
默认 NAT	自动把该接口所在网段的地址，转换成 WAN 口的地址，提供内网的 Internet 访问

表 3.8 DMZ 区提供的服务列表

- **接口防御**

单击接口配置中的【接口防御】Tab，可以为防毒墙配置接口防御，如图 3.21 所示：

图 3.21 接口防御配置

此处可启用 SYN FLOOD 防御、UDP FLOOD 防御、ICMP FLOOD 防御、每 IP 连接数限制和碎片攻击防御来防御来自于网络的攻击。

SYN FLOOD 防御、UDP FLOOD 防御、ICMP FLOOD 防御、每 IP 连接数限制和碎片攻击阈值，都以数据包每秒（PPS）为单位，可以根据客户的需要进行设定。SYN Flood、ICMP Flood、UDP Flood 和碎片攻击阈值的缺省值均为 1000 PPS，每 IP 连接数阈值缺省为 5 PPS。在给定的 IP 地址范围内，当通过的数据包值超过阈值时就会被认作是攻击，并被报告。SYN Flood、ICMP Flood、UDP Flood 突发值，以数据包个数为单位，限制一瞬间通过防毒墙数据包的个数，达到保护防毒墙正常工作的目的，突发值均为 100 个。用户可根据需要进行设定。

提示：关于 Flood 攻击，请参考 APPENDIX 3 SYN Flood 攻击介绍。

- **链路设置**

防毒墙可以配置最大传输单元 MTU 值以适应用户已有的网络设备，达到更好的网络传输效果。防毒墙网络带宽自动适应当前网络，无需用户另行操作。当遇到适应性较差的网络设备时，防毒墙系统提供 10M、100M 和 1000M 的全/半双工模式供用户选择适应当前的网络设备，达到更好的网络效果。如图 3.22 所示。

图 3.22 防毒墙链路设置

修改 MTU 设置和链路层设置后，单击【应用】，完成防毒墙链路设置的保存。

3.2 出口配置

提示：防毒墙出口管理功能只适用于企业拥有多个网络出口的情况下进行网络负载均衡，如果您的企业中只有一个网络接口，可不进行防毒墙出口的配置。

单击【网络配置】➔【出口配置】进行防毒墙出口管理，如图 3.23 所示。

图 3.23 防毒墙出口管理

字段	说明
序号	按阿拉伯数字排序出口的序号
名称	为出口自定义别名
接口	出口对应的物理接口
网关或帐号	该出口的网关地址
带宽权重	当网络拥有多出口时，网络流量会按带宽权重比例进行分配。带宽权重值越高所占比例越多；反之，值越小所占比例越小
状态	显示当前网络出口是否可用
操作	可修改当前出口配置

表 3.9 防毒墙出口管理说明

3.2.1 增加出口

提示：关于带宽权重

当企业拥有多个网络出口时，通过设置带宽权重可以合理分配网络出口的带宽资源。例如，企业有两条网络出口，分别为网通和电信宽带，将网通带宽权重设为 100，电信带宽权重设为 50，企业用户在访问网络时通过电信出口的数据流量比例就为 50/（100+50）=1/3。

单击【增加】按钮为防毒墙增加一个网络出口。

提示：关于网络出口

- 当防毒墙网口工作模式（静态 IP/DHCP/PPPoE）的时候，增加操作略有不同
- 只有工作区域处在 WAN 的网口才可以被增加成出口

- 当网口处于静态 IP 模式时

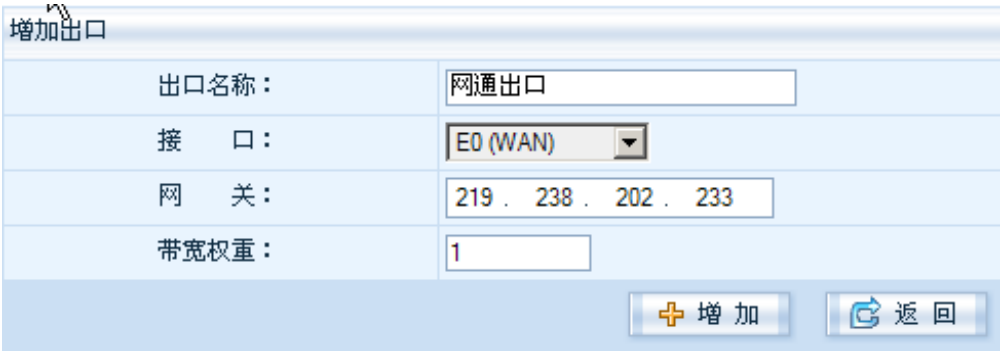


图 3.24 增加防毒墙出口地址

1. 出口名称：填写该出口的别名
2. 接口：选择防毒墙的出口

3. 网关：填写该接口的网关地址（即下一跳的地址）
4. 带宽权重：填写该接口的带宽权重值
5. 单击【增加】保存设置或单击【返回】取消操作

- 当网口处于 DHCP/PPPoE 模式时

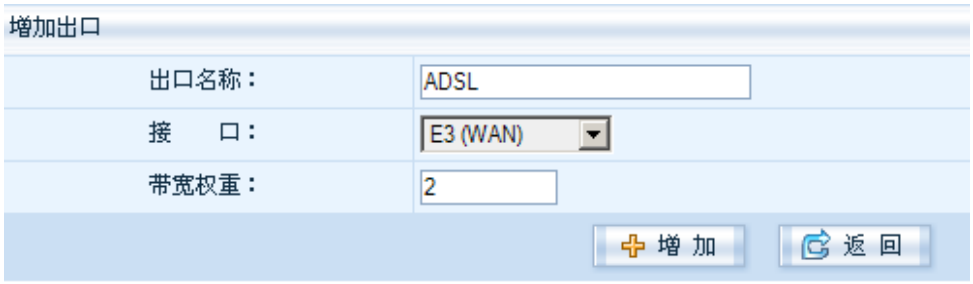


图 3.25 DHCP/PPPoE 模式下的增加出口对话框

1. 出口名称：填写该出口的别名
2. 接口：选择防毒墙的出口
3. 带宽权重：填写该接口的带宽权重值
4. 单击【增加】保存设置或单击【返回】取消操作

3.2.2 修改出口管理

要修改某一出口设置，请单击该条记录的按钮，根据网口工作模式的不同，相应的修改操作也不同。

- 当网口工作在静态 IP 模式下，用户可以修改网口的网关和带宽权重，如图 3.26 所示。

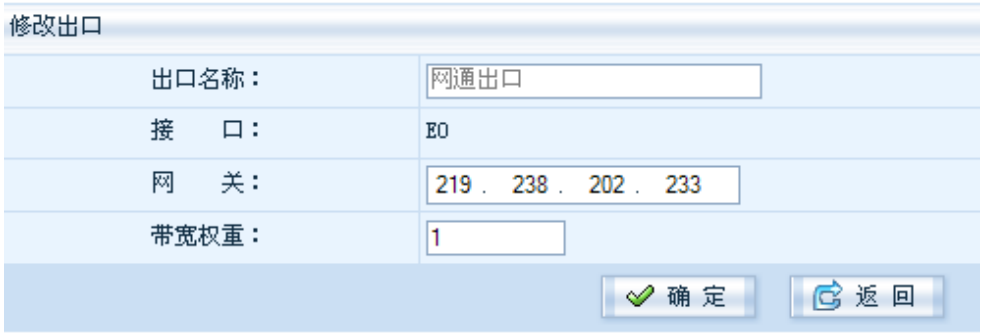


图 3.26 静态 IP 模式下的出口修改

- 当网口工作在 DHCP/PPPoE 模式下，用户只可以修改网口的带宽权重，如图 3.27 所示。

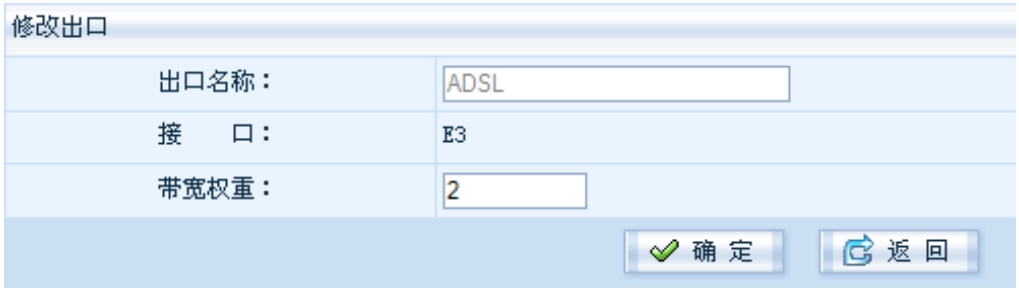


图 3.27 DHCP/PPPoE 模式下的出口修改

3.2.3 删除出口管理记录

要删除某条防毒墙出口记录，请选中该条记录前的复选框，单击【删除】。如图 3.28 所示。

图 3.28 删除出口配置记录

3.3 DNS 配置

防毒墙使用的首选、备用 DNS 服务器的 IP 地址。大多数情况下，这些 IP 地址由 Internet 服务提供商（ISP）提供。如果防毒墙的接口工作在 PPPoE 模式，将自动获取 DNS 的 IP 地址。

设定防毒墙的首选、备用 DNS 服务器：

1. 单击【网络配置】➔【DNS 配置】
2. 在首选 DNS 服务器栏中，输入首选 DNS 服务器的 IP 地址
3. 如果有备用 DNS 服务器，则在备用 DNS 服务器栏中输入备用 DNS 服务器的 IP 地址，如图 3.29 所示
4. 如果选中【通过 DHCP / PPPoE 自动获得 DNS 服务器地址】前单选框，则防毒墙自动从网络上获取 DNS 服务器地址无需用户手工输入

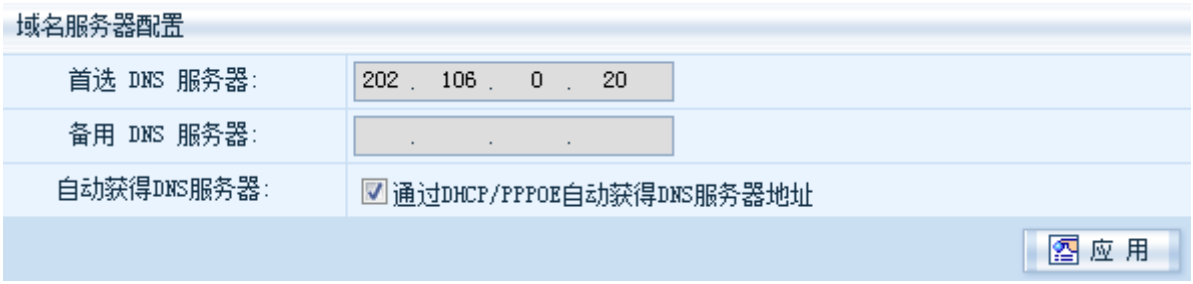


图 3.29 DNS 服务器设置

5. 单击【应用】保存所做的设置。如图 3.30 所示

图 3.30 DNS 设置成功

3.4 网桥配置

防毒墙内部提供两路网桥供用户使用。通过网桥模式，用户可以在不改变现有网络拓扑结构的情况下直接把防毒墙放置在网络中，从而使用防毒墙提供的各种服务。

> **提示：关于处于网桥模式的网口 IP 设置**
>
> 为了使防毒墙的杀毒功能正常工作，您需要为构成网桥的一对网口分别设置一个任意的 IP 地址。且网桥 IP 地址不要与内部网络已存在的 IP 地址相同。

单击【网络配置】➔【网桥配置】可以进入防毒墙网桥配置页面，如图 3.31 所示。

图 3.31 防毒墙网桥配置

3.4.1 设置网桥接口的 IP 地址

单击 IP 地址列表中的【增加】按钮，如图 3.32 所示。

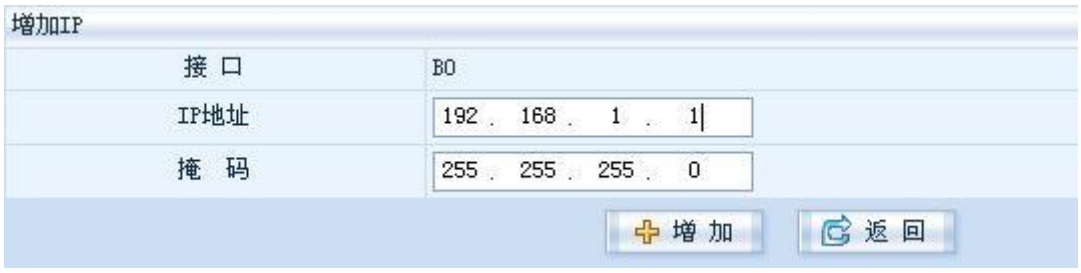


图 3.32 增加网桥 IP 地址

1. 填写网口 IP 地址
2. 填写网口的子网掩码
3. 单击【增加】保存设置，否则单击【返回】取消操作

3.4.2 修改网桥接口的 IP 地址

要修改某一网桥的 IP 地址，请单击该条记录的按钮，如图 3.33 所示。

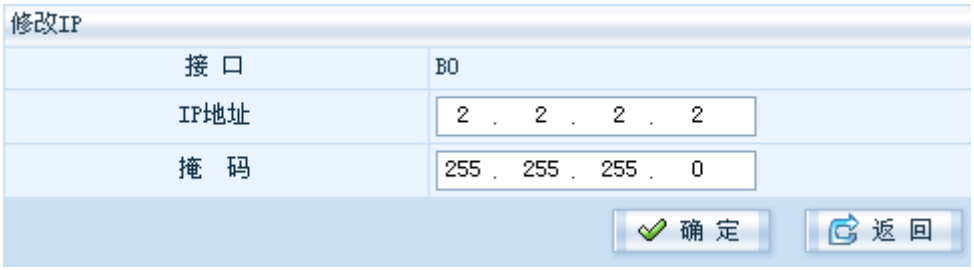


图 3.33 修改网桥端口的 IP 地址

1. 修改 IP 地址
2. 修改网口的子网掩码
3. 单击【确定】完成修改，单击 【返回】取消修改

3.4.3 删除网桥接口的 IP 地址

要删除某条网桥 IP 地址，请选中该条记录前的复选框，单击【删除】。如图 3.34 所示。

图 3.34 删除网桥 IP 地址

3.5 路由配置

瑞星防毒墙使用静态路由表确定转发数据包的目的接口。因此，在将数据包发送给防毒墙没有直接连接的特定网络或主机时，必须在路由表中增加静态路由条目。

提示：关于静态路由的配置

为了配置路由策略，防毒墙必须要有一个出口（即在 WAN 区的物理接口）

单击【网络配置】➔【路由配置】，您可以在静态路由配置页面查看并修改防毒墙当前的路由信息。如

图 3.35 所示。

静态路由配置

	序号	网络地址	网络掩码	网　关	网络接口	操作
□	1	193.168.20.0	255.255.255.0	0.0.0.0	E2	-
□	2	193.168.100.0	255.255.255.0	0.0.0.0	E3	-
□	3	3.3.3.0	255.255.255.0	0.0.0.0	E0	-
□	4	193.168.0.0	255.255.0.0	193.168.20.1	E2	✎

增 加　删 除

图 3.35 防毒墙的静态路由表

3.5.1 增加路由

当您要增加一个静态路由设置时，单击【增加】按钮，如图 3.36 填写静态路由配置。

静态路由配置

网络地址: 193 . 168 . 90 . 0

网络掩码: 255 . 255 . 255 . 0

网　关: ○ 指定

网络接口: ◉ 指定 E0 (WAN)

增 加　返 回

图 3.36 增加静态路由

- 网络地址：数据包转发的目的地址
- 网络掩码：目的地址所在网段的掩码，如果是到一特定计算机的路由，掩码为 255.255.255.255
- 网关：如果去往其他特定子网的路由表可以在其它机器上找到，则设置该机器的 IP
- 网络接口：此路由条目使用的网关，如果想使用防毒墙的接口作为网关，则直接在这里选择相应的接口

> **注意：网络接口和网关只能选择其中一种。**

3.5.2 修改路由

要修改某一条路由规则，请单击该条记录的✎按钮。如图 3.37 所示。

静态路由配置

网络地址: 193 . 168 . 90 . 0

网络掩码: 255 . 255 . 255 . 0

网　关: ○ 指定

网络接口: ◉ 指定 E0 (WAN)

确 定　返 回

图 3.37 修改静态路由配置

1. 修改子网地址
2. 修改子网掩码
3. 修改网络接口或指定网关
4. 单击【确定】保存设置，单击【返回】取消修改

3.5.3 删除路由

若要删除某条路由，请勾选该记录，单击【删除】直接删除该条路由。如图 3.38 所示。

静态路由配置

	序号	网络地址	网络掩码	网　关	网络接口	操作
☐	1	193.168.20.0	255.255.255.0	0.0.0.0	E2	-
☐	2	192.168.2.0	255.255.255.0	0.0.0.0	E3	-
☑	3	193.168.90.0	255.255.255.0	0.0.0.0	E0	
☐	4	3.3.3.0	255.255.255.0	0.0.0.0	E0	-
☐	5	3.3.3.0	255.255.255.0	0.0.0.0	E1.VPN	-
☐	6	193.168.0.0	255.255.0.0	193.168.20.1	E2	

增 加　删 除

图 3.38 删除静态路由

3.6 策略路由

策略路由是一种路由规划，它可以使数据包按照用户指定的策略进行转发。基于某些管理的需求，要求某些路由必须经过特定的路径，或者只能通过某些特定的协议和端口号进行通讯，此时就可以使用策略路由。

提示：当企业中拥有多个网络出口时，根据需要进行策略路由配置，当企业中只有一个网络出口时，可不进行策略路由的配置。

单击【网络配置】➔【策略路由】，进入策略路由设置页面，如图 3.39 所示。

策略路由配置

☐	序号	状态	规则名	出口	源地址	目的地址	服务	操作
您还没有设置规则，点击这里 **增加**								

图 3.39 防毒墙策略路由配置

3.6.1 增加策略路由

单击【增加】按钮，如图 3.40 所示。

图 3.40 增加新规则

- 规则名：规则的友好名称
- 出口：规则适用的出口
- 源地址
  - 类型 指定描述源地址的方法。用户可以通过三种方式定义源地址，分别为地址、地址组和自定义。其中地址和地址组在防毒墙中都是通过对象来表示的（要了解关于地址对象的更多设置，请参考 8.1 地址和 8.2 地址组）。而自定义则允许用户手工增加源地址的信息
  - 内容 指定具体的源地址内容。当用户选择地址或地址组这两种类型时，就可以在内容下拉列表中选择相应的对象作为源地址。当用户选择自定义的类型时，用户可以按照以下方式自定义源地址
    - 增加一个 IP 地址，例如：192.168.0.1
    - 增加一段地址，例如：192.168.0.1-192.168.0.2
    - 增加一个网段，例如：192.168.0.1/24
    - 增加一个 MAC 地址，例如：AA:AA:AA:AA:AA:AA
- 目的地址

  用户可以按照和指定源地址相同的方法来指定目的地址。但需要注意的是，当用户在目的地址中选择了自定义时，不能够通过 MAC 地址来指定，而只能够设置一个地址或网段
- 服务

  在瑞星防毒墙中，服务同样是用对象来表示的（要了解关于服务对象的更多设置，可以参看 8.5 服务和 8.6 服务组）
  - 类型 指定描述服务的方法。用户可以通过三种方式定义服务，分别为服务、服务组和自定义。其中服务和服务组在防毒墙中都是通过对象来表示的（要了解关于服务对象的更多设置，请参考 8.5 服务和 8.6 服务组）。而自定义则允许用户手工增加服务的信息。
  - 内容 指定具体的服务内容。当用户选择了服务或服务组这两种类型时，就可以在内容下拉列表中选择相应的对象作为服务了。当用户选择自定义的类型时，用户可以按照以下方式自定义服务
    - 增加一个已知协议和源、目的端口，例如：tcp:1-12 1-155 或 icmp:any 等

- 增加一个自定义的协议，例如：other:1-55

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条策略路由后，策略路由主页面上会显示出来。如图 3.41 所示。

3.41 防毒墙策略路由列表

字段	说明
序号	按照阿拉伯数字排序
状态	指示此规则的是否开启。绿色图标表示开启，红色图标表示停用状态
规则名	规则的代表名称。管理员自定义规则名称以方便管理
出口	所有流出此规则的数据流接口
源地址	显示此记录的来源 IP 地址
目的地址	显示此规则的数据目标地址
服务	采用何种服务
操作	提供设置、修改防毒墙 IP 地址转换的功能，可单击进入设置页面
设为启用	如果要开启某个被停用的规则，选中该规则前的复选框，单击【设为启用】按钮
设为停用	如果要停用某个被启用的规则，选中该规则前的复选框，单击【设为停用】按钮

表 3.10 防毒墙策略路由说明

3.6.2 修改策略路由

要修改某一条策略路由规则，请单击该条记录的按钮。如图 3.42 所示。

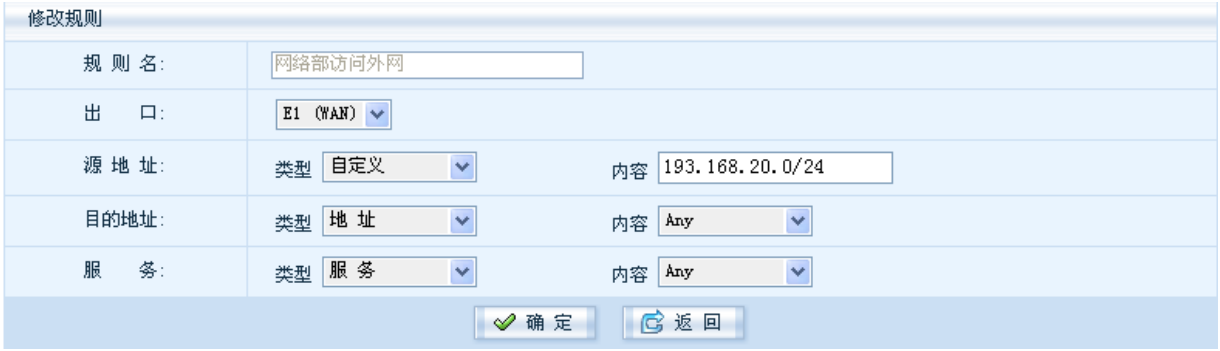


图 3.42 修改策略路由配置

1. 修改策略路由网络出口
2. 修改源地址和目的地址
3. 修改服务内容

4. 单击【确定】保存设置，单击【返回】取消修改

3.6.3 删除策略路由

若要删除某条策略路由，请勾选该记录，单击【删除】直接删除该条路由，如图 3.43 所示。

图 3.43 删除策略路由

3.7 DHCP 配置

您可以将瑞星防毒墙的某一个或多个接口配置为 DHCP 服务器，为多台主机动态分配 IP 地址。如果内部网络的 IP 地址十分紧缺，IP 地址可以根据需要来分配，提高 IP 地址的使用效率，简化网络管理。

在菜单栏单击【网络配置】➔【DHCP 配置】，将弹出 DHCP 配置页面，如图 3.44 所示。

图 3.44 防毒墙 DHCP 设置

3.7.1 允许 DHCP 服务

瑞星防毒墙默认不启用 DHCP 服务。启用该服务并经过配置后，防毒墙可以为不在同一个网络中的多个子网提供 DHCP 服务。关于如何启用 DHCP 服务请参考 3.1.3 接口配置。本节描述如何设置 DHCP 服务。

3.7.2 DHCP 管理

当启用 DHCP 时，防毒墙将根据指定的 IP 地址范围向内部网络上的每一个 DHCP 客户端分配地址。您可以设置多个地址段，应用于多个需要防毒墙 DHCP 服务的子网。

提示：不是网络中所有的计算机都适合使用 DHCP 服务

在您的网络中，提供服务的计算机不应在 DHCP 服务器那里获得 IP 地址。例如：邮件服务器、文件服务器和 DNS 服务器等。

3.7.2.1 增加一个动态地址段

创建一个 DHCP 的 IP 地址范围，单击 DHCP 动态地址分配列表页面的【增加】按钮。如图 3.45 所示。当设置成功后，防毒墙将自动为连接到该接口的计算机分配 IP 地址、网关和 DNS 地址。

图 3.45 创建 DHCP 地址段

1. 设定要提供 DHCP 服务的网口
2. 设置客户端默认网关 IP 地址
3. 输入动态分配 IP 地址范围起始 IP 地址
4. 输入动态分配 IP 地址范围终止 IP 地址

设定完成后，单击【增加】按钮保存设置。

3.7.2.2 修改动态地址段

如果需要修改已存在的记录，单击该记录的图标进入修改动态地址段页面。如图 3.46 所示。

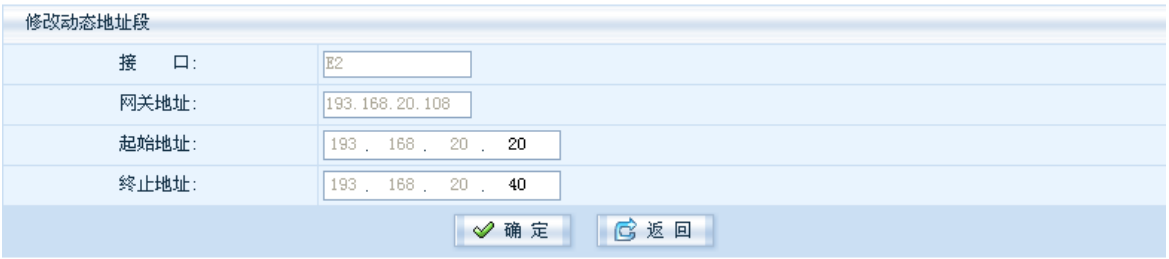


图 3.46 修改 DHCP 地址段

1. 修改动态分配 IP 地址范围起始 IP 地址
2. 修改动态分配 IP 地址范围终止 IP 地址

修改完成后，单击【确定】保存设置。

提示：关于 DHCP 的地址段

必须指定网络上的主机将要使用的 IP 地址范围。例如，如果输入 192.168.100.1 到 192.168.100.20，那么就有 20 个 IP 地址可以用来分配给客户端。而 192.168.100.21 到 192.168.100.254 的地址，客户端就不能通过防毒墙自动获取到。

3.7.2.3 删除动态地址段

若要删除某个记录，选中该记录前的复选框，单击【删除】按钮。

3.7.3 MAC 地址绑定分配列表

可以利用 MAC 地址绑定把 DHCP 自动地址列表中的 IP 地址自动分配给特定的某个 MAC 地址。

> **提示：关于 MAC 地址绑定**
>
> 增加 MAC 地址绑定记录首先要增加动态地址段，增加动态地址段参见 3.7.2 DHCP 管理

3.7.3.1 增加一个绑定

创建一个 MAC 地址和 IP 地址的关联，单击 MAC 绑定地址分配列表下的【增加】按钮，如图 3.47 所示。

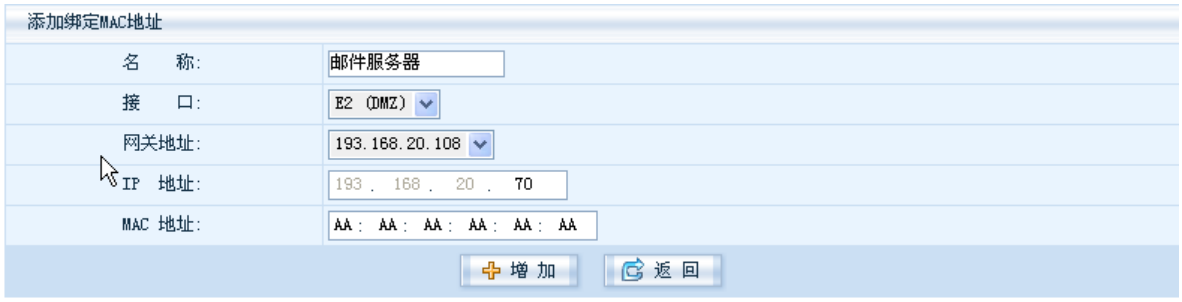


图 3.47 增加 MAC 地址绑定

1. 设定提供地址绑定服务的防毒墙网口
2. 网关地址：网关地址为该接口默认地址，如一个接口绑定多个 IP 地址，请管理员根据实际情况进行选择
3. IP 地址：输入要被绑定的 IP 地址
4. MAC 地址：输入该客户端网卡的 MAC 地址

设置完成后，单击【增加】按钮保存设置

3.7.3.2 修改一个绑定

如果需要修改已存在的记录，单击该记录的 图标进入修改页面，如图 3.48 所示。

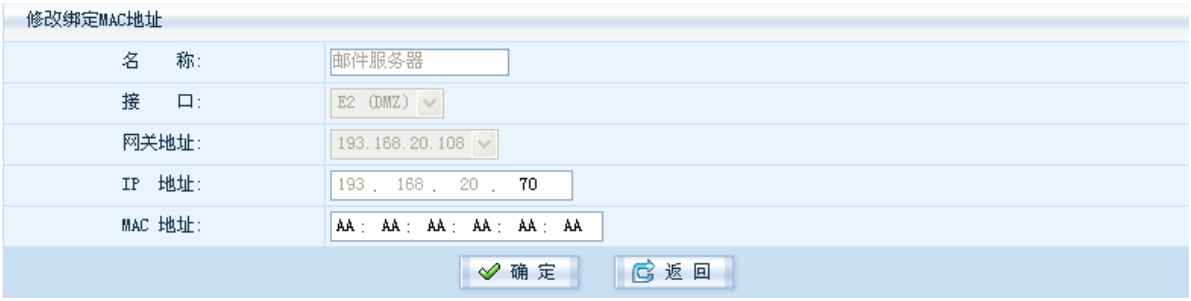


图 3.48 修改 DHCP 地址段

1. IP 地址：修改和 MAC 绑定的 IP 地址
2. MAC 地址：修改要绑定的 MAC 地址

修改完成后，单击【确定】按钮保存设置。

3.7.3.3 删除一个绑定

若要删除某个记录，选中该记录前的复选框，单击【删除】按钮。

3.8 网络诊断

该节主要介绍以下四个模块的功能以及使用方法。

- 远程协助：当瑞星防毒墙出现技术上的故障时，通过此设置获取瑞星工程师的技术支持
- 诊断信息发送：定期给瑞星技术支持人员发送防毒墙系统诊断信息，方便排障
- Ping：使用 ICMP 请求和应答协议，判断数据是否可以通过网络到达主机
- Trace Route：显示当前网络到达某个主机的路径

3.8.1 远程协助

当用户防毒墙出现技术上的故障时，瑞星防毒墙提供远程支持服务。单击【网络配置】➔【网络诊断】，进入远程支持页面，在调试 IP 和端口处填写由瑞星技术服务人员提供的 IP 地址和端口，单击【启动】，如图 3.49 所示。我们的工程师会在第一时间内通过互联网连接到您的防毒墙上，帮助您解决技术上的问题。

图 3.49 远程支持

3.8.2 诊断信息发送

在需要瑞星技术支持人员进行跟踪调试时打开该功能，防毒墙会在指定时间将防毒墙系统状态信息发送给瑞星技术支持人员，便于瑞星技术支持人员对客户的防毒墙产品进行故障跟踪和调试，避免因为防毒墙的工作不正常给用户造成损失。单击【网络配置】➔【网络诊断】，进入诊断信息发送页面，如图 3.50 所示。

图 3.50 防毒墙诊断信息发送页面

用户可以按照星期和发送时间的组合来定义发送诊断信息，对于发送时间的设置将应用到被选中的每

一个星期。如图 3.50 所示，防毒墙在每天的 12 点 30 分向瑞星技术支持人员发送诊断信息。设置好后，单击【应用】按钮保存。

3.8.3 诊断工具

- Ping

单击【网络配置】➔【网络诊断】，进入网络诊断页面。选择 Ping，进行当前网络诊断。Ping 的结果可以判断您正试图到达的主机是否打开并正在运行，以及防毒墙是否能够与该主机通信。

如果 Ping 的结果不通，则表示该远程主机已关闭或存在阻碍正常通信的其它问题。若要了解远程主机的具体状态，请使用其它方法进行检查。

1. 在目标字段中，输入将要被 Ping 的主机名称或 IP 地址

> **提示：**对于本地网络以外的请求，如果防毒墙上没有配置外部 DNS，域名是不能解析的，必须输入合法的 IP 地址。

2. 单击【执行】
3. Ping 测试的结果如图 3.51 所示

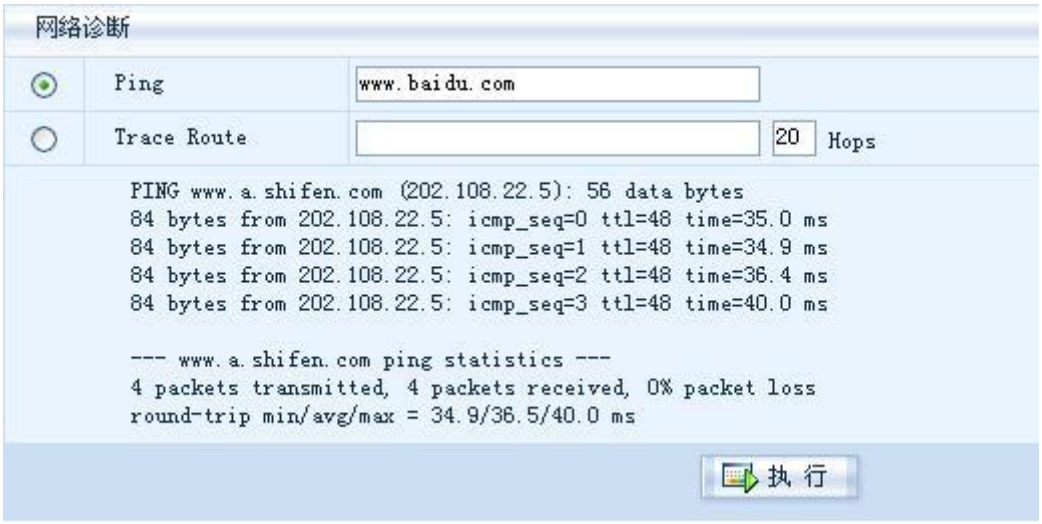


图 3.51 Ping 功能测试页面

- Trace Route

单击【网络配置】➔【网络诊断】，进入网络诊断页面。选择 Trace Route 功能，进行跟踪路由的诊断。

使用跟踪路由查看 IP 包在网络上的路径，根据不同的网络情况所消耗的时间有所差异，如遇等待时间较长，请耐心等候。

1. 输入远程主机的主机名称或 IP 地址。

提示：对于本地网络以外的请求，如果防毒墙上没有配置外部 DNS，域名是不能解析的，必须输入合法的 IP 地址。

2. 输入需要跟踪的地址（以 202.106.0.20 为例），单击【执行】，跟踪路由的结果如图 3.52 所示。

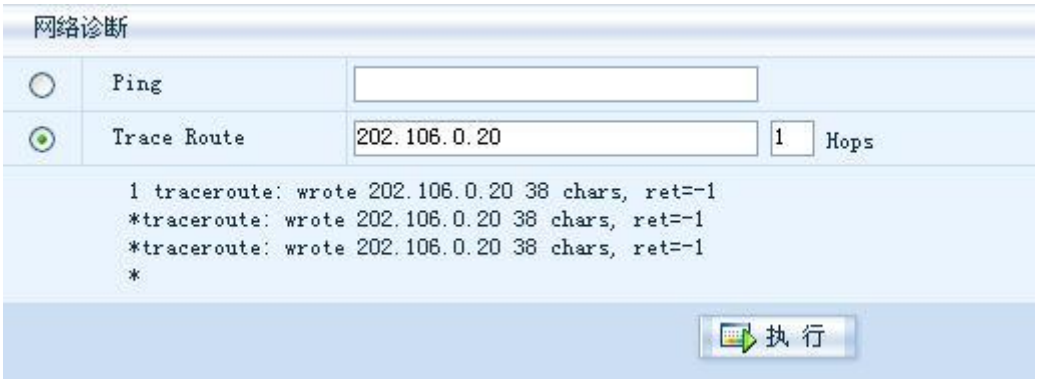


图 3.52 测试跟踪路由页面

第四章　系统配置的功能和使用

本章主要介绍以下八个模块的功能及使用方法。

- 系统状态：显示当前防毒墙运行的详细信息
- 系统时间：同步防毒墙和工作站上的系统时间与日期
- 软件升级：防毒墙系统及病毒库升级
- 系统维护：备份和恢复防毒墙系统配置
- 设备配置：设置防毒墙设备信息
- DDNS 配置：配置防毒墙某一接口获取固定的免费二级域名
- DNS 代理：设置域名解析代理功能
- TCP/IP 选项：设置防毒墙 TCP/IP 连接超时时间

4.1 系统状态

单击【系统管理】➔【系统状态】，进入防毒墙系统状态信息查看页面。如图 4.1 所示，通过系统资源、系统状态、统计信息、接口配置信息、告警信息和主机上传/下载前五名，简单扼要的表现出当前防毒墙系统的状态信息，有关此部分的详细说明请参见本手册 2.2 登录防毒墙。

图 4.1 防毒墙系统状态信息

4.2 系统时间

为了更好地对防毒墙进行监控和管理，应使防毒墙的系统时间与管理主机的时间相同。单击【系统管理】➔【系统时间】，如图 4.2 所示。

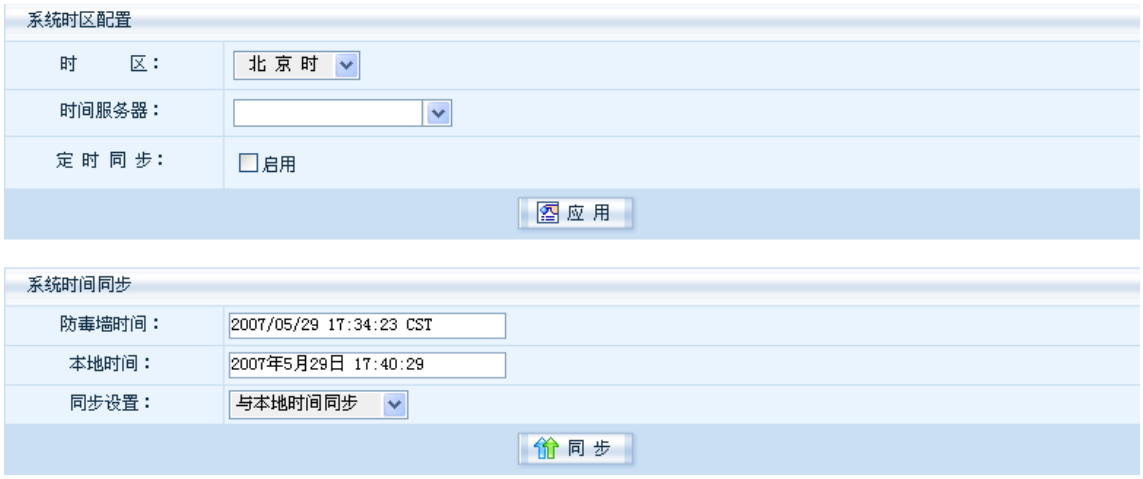


图 4.2 系统时间设置页面

4.2.1 系统时间配置

瑞星防毒墙支持网络时间服务器定时同步功能，单击【系统管理】➔【系统时间】，进入系统时间配置页面，如图 4.3 所示。

图 4.3 系统时间配置页面

1. 在时区处选择防毒墙使用的时区，分为北京时和世界时。
2. 选择使用定时同步时间的时间服务器，确保网络能够访问选择的时间服务器
3. 在定时同步处选中【启用】按钮，如图 4.4 所示

图 4.4 定时同步选项

4. 在时间处选择进行同步的时间，可根据年月/日/时/分、日/时/分、星期几/时/分、时/分进行同步
5. 单击【应用】按钮保存同步网络时间设置

4.2.2 系统时间同步

瑞星防毒墙提供了时间同步机制，该功能可为日志提供精确的时间。屏幕上分别显示了防毒墙时间和本地时间，如果两个时间相差较大，可在同步设置处选择与本地时间同步，单击【同步】按钮使防毒墙的系统时间与管理主机的时间相同，如图 4.5 所示。

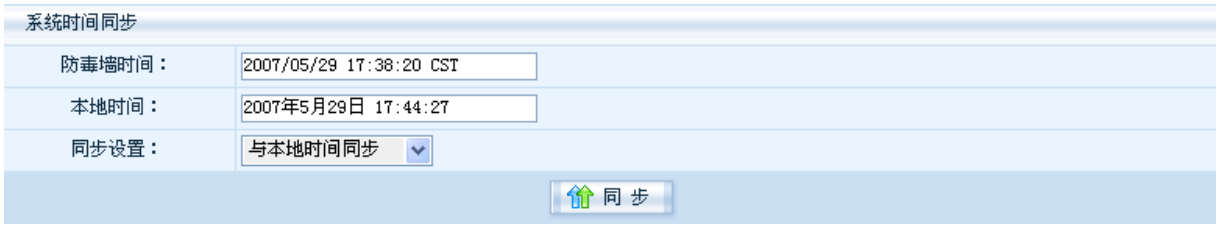


图 4.5 与本地时间同步

也可在同步设置处选择与时间服务器同步，单击【同步】按钮与时间服务器进行同步。如图 4.6 所示。

图 4.6 与时间服务器同步

注意：防毒墙的时间影响到系统日志和升级功能的准确性，请务必保证和本地时间同步。

4.3 软件升级

系统升级包含防毒墙基本系统升级和病毒库升级两部分内容。作为防毒网关，及时升级是保证设备正常工作的基础。请用户保证对此部分进行正确的设置。单击【系统管理】➔【软件升级】进入软件升级页面。

4.3.1 反病毒引擎

单击【系统管理】➔【软件升级】进入查看反病毒引擎页面，如图 4.7 所示。

图 4.7 查看防病毒引擎状态

字段	说明

注册状态	分为：有效序列号和未注册两种状态。用户购买防毒墙产品后，需要在首次升级起 30 天内进行服务激活，对于 30 天后仍未激活的产品将无法正常升级。病毒库更新关系到防毒墙产品的实际应用效果，请谨慎对待！用户可通过防毒墙基本信息页面进行防病毒引擎序列号的注册
有效日期	防病毒引擎的有效时间
病毒库版本	当前防毒墙病毒库版本
最后升级日期	显示防毒墙上一次病毒库升级的时间

表 4.1 病毒引擎状态说明

4.3.2 反垃圾邮件引擎

反垃圾邮件引擎能够有效的过滤通过防毒墙的垃圾邮件，其引擎状态如图 4.8 所示。

图 4.8 反垃圾邮件引擎状态

字段	说明
注册状态	分为：有效序列号和未注册两种状态。未注册的反垃圾邮件引擎不能正常工作，它关系到防毒墙反垃圾邮件的实际应用效果，用户可通过防毒墙基本信息页面进行反垃圾邮件引擎的注册
有效日期	反垃圾邮件引擎的有效时间，如果未购买反垃圾邮件授权，此处显示【未启用】状态
引擎版本	显示当前反垃圾邮件引擎的版本号
最后升级日期	显示防毒墙上一次反垃圾邮件引擎升级的时间

表 4.2 反垃圾邮件引擎状态说明

4.3.3 手动升级引擎

防毒墙病毒库升级分为：网站升级、局域网升级和本地升级三种方式，如图 4.9 所示。

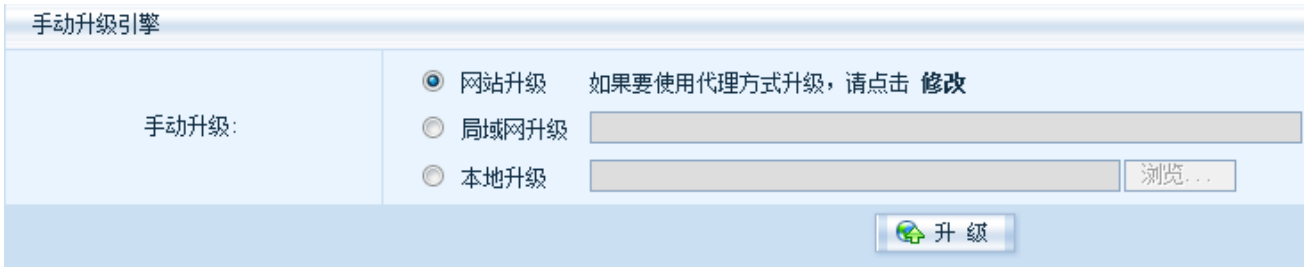


图 4.9 病毒库升级页面

- 网站升级：单击【升级】防毒墙将从瑞星网站自动下载病毒库升级包；单击【修改】进行代理方式升级设置
  - 通过代理方式进行病毒库升级

病毒库手动升级和定时升级代理服务器设置都通过此处进行修改，设置步骤如下：

1. 单击【修改】进入代理服务器设置页面，如图 4.10 所示

图 4.10 代理服务器设置页面

2. 选择【启用】则网站升级手动和定时两种升级方式将通过代理服务器访问瑞星病毒库升级服务器；选择【停用】则网站升级手动和定时两种升级方式将通过默认的网络连接访问瑞星病毒库升级服务器

3. 当选择【启用】时将显示代理服务器详细设置页面，如图 4.11 所示

图 4.11 代理服务器详细设置

a) 在地址和端口处输入代理服务器的地址和端口，单击【确认】完成代理服务器设置

b) 如需验证，单击【需要验证】前的单选框，如图 4.12 所示。输入验证信息后，单击【确认】完成代理服务器设置

图 4.12 代理服务器身份验证设置

- 局域网升级：选中该选项后，在局域网升级处输入升级服务器详细的 URL 地址，单击【升级】防毒墙从指定的局域网地址下载病毒库升级包
- 本地升级：将病毒库升级包下载到本地，通过【浏览】选择升级包，单击【升级】进行防毒墙病毒库的升级

4.3.4 定时升级引擎

防毒墙将自动下载升级包对病毒库进行升级。选中【定时升级】并单击【启用】，选择进行自动升级的时间和方式，单击【应用】保存设置，如图 4.13 所示

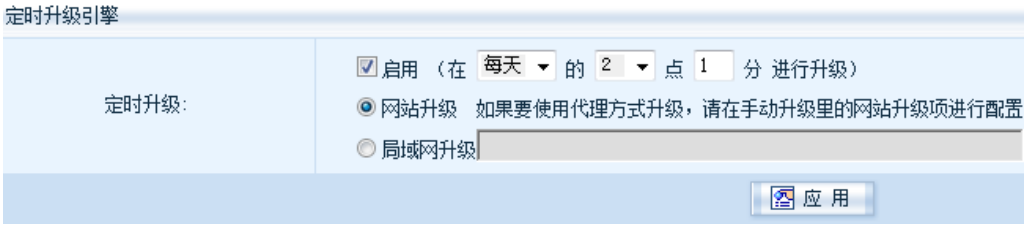


图 4.13 防毒墙定时升级引擎设置

4.3.5 系统升级

注意：防毒墙自身软件系统必须通过到瑞星主页下载升级包手动完成升级，升级完成后，通常需要重新启动系统。

为了升级您的防毒墙系统，请执行以下操作：

1. 在浏览器中输入 http://update.rising.com.cn/register/pcver/upgrade.htm，打开瑞星产品升级更新服务页面
2. 在页面上输入用户 ID（关于如何获得用户 ID，请参考《快速使用指南》）后，单击【登录】按钮，如图 4.14 所示

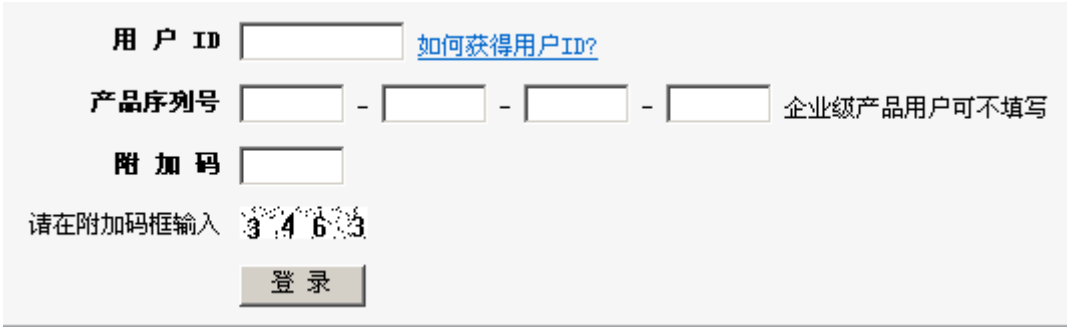


图 4.14 用户登录页面

3. 进入相应的产品升级包下载页面，选择系统升级包下载，将系统升级包下载到本地计算机
4. 在系统升级页面，单击【浏览】按钮，如图 4.15 所示

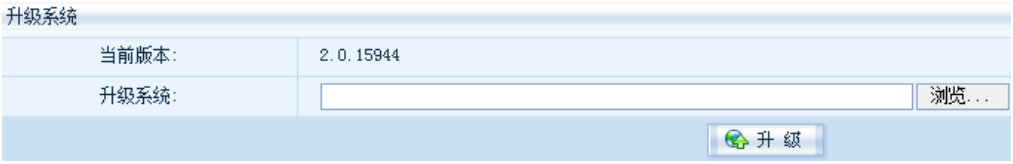


图 4.15 升级系统

5. 选择下载的升级文件
6. 单击【升级】按钮，开始系统升级

4.4 系统维护

4.4.1 备份当前配置

为了备份当前的系统配置，用于日后恢复系统，请执行以下操作：

1. 单击【系统管理】➔【系统维护】，在备份信息中填入为方便日后管理的相关备份信息
2. 在备份密码处输入备份文件的加密密码，并在重复密码处再次输入备份密码进行确认

图 4.16 创建备份

3. 单击【备份】按钮，系统将防毒墙的配置保存到一个文件中。如图 4.17 所示

图 4.17 防毒墙配置文件保存

4. 单击【确定】，返回到系统维护页面，将会出现【下载备份文件】按钮，如图 4.18 所示

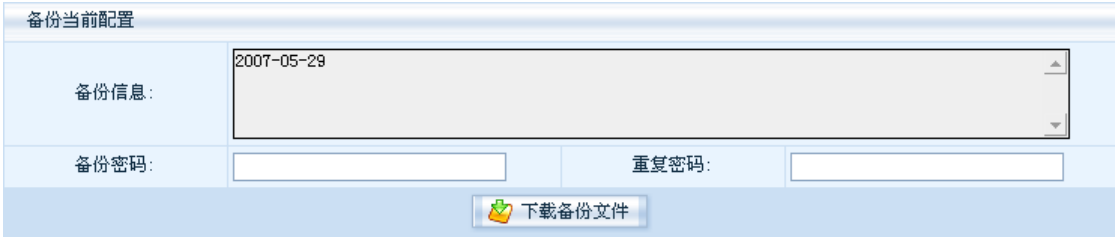


图 4.18 下载防毒墙备份文件

5. 单击【下载备份文件】系统提示保存备份文件，如图 4.19 所示。

图 4.19 确认保存备份文件

6. 单击【保存】将备份文件下载至本地计算机上保存。选择保存目录，如图 4.20 所示

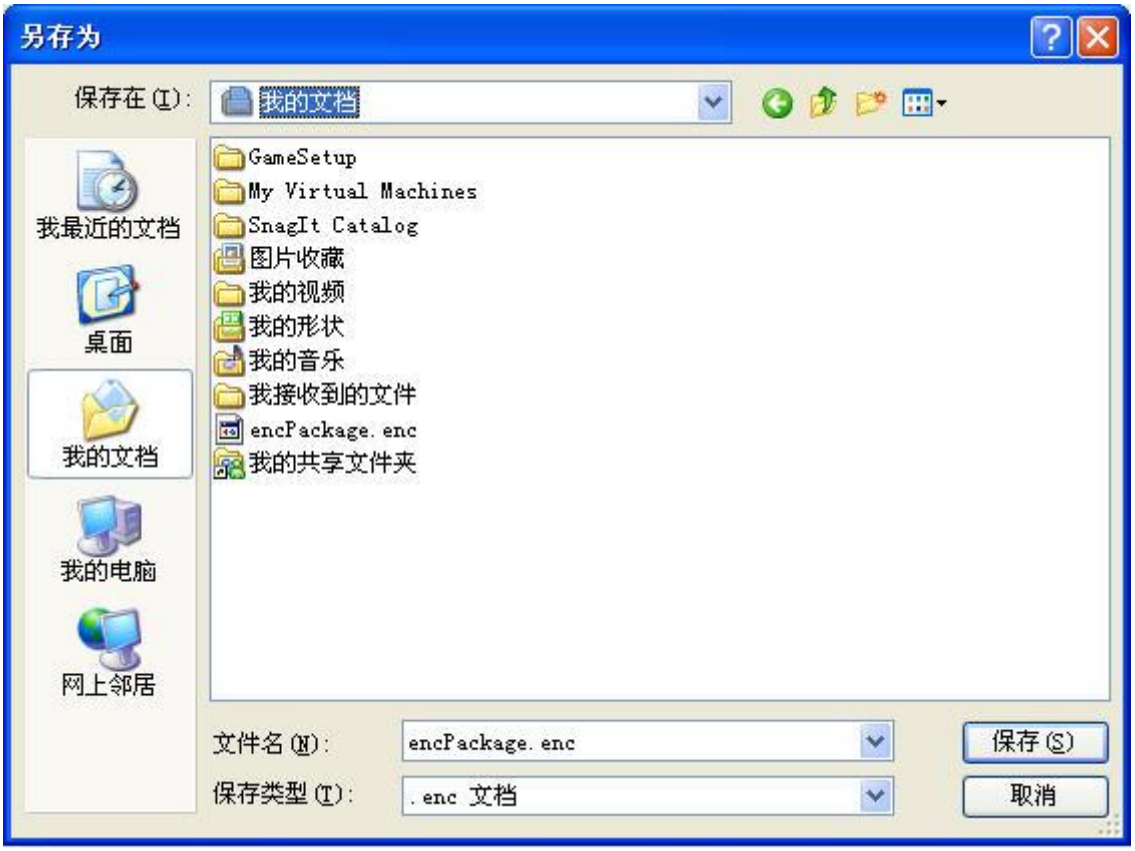


图 4.20 选择备份文件的存储位置

7. 单击【保存】按钮，保存备份文件

4.4.2 使用备份文件恢复

用户可以使用通过备份当前配置保存下来的备份文件恢复系统配置，为了进行系统配置恢复，请执行以下操作：

1. 单击【浏览】按钮，选择存放配置文件的目录，如图 4.21 所示

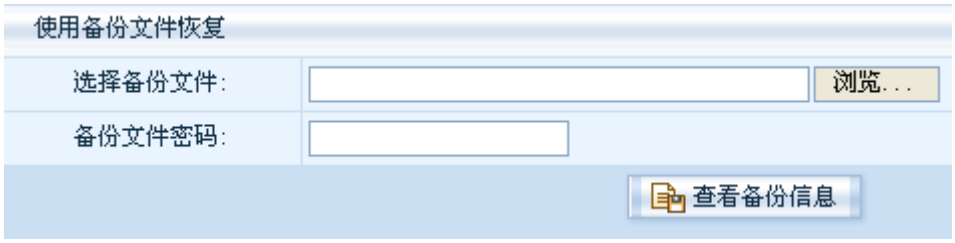


图 4.21 选择备份文件

2. 在备份文件密码处输入备份时进行加密的密码

3. 单击【查看备份信息】按钮，查看选择的备份文件的信息，确认选择的文件版本正确，如图 4.22 所示

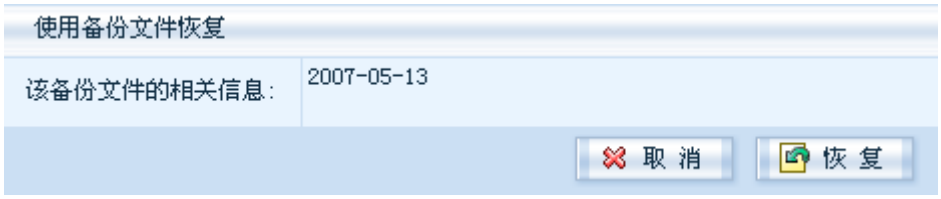


图 4.22 使用备份文件恢复系统设置

4. 单击【恢复】按钮进行恢复

注意：不同型号的防毒墙生成的备份文件不可以互相使用（例如：RSW-3200 的备份文件不能用在 RSW-1200 中），但是，同一型号的防毒墙生成的备份文件可以互相使用。

4.4.3 系统维护

单击【系统管理】➔【系统维护】，将进入系统维护页面。这里，用户可以进行恢复出厂设置、关闭系统、重启系统和自动关机的设置，如图 4.23 所示。

图 4.23 防毒墙系统维护

4.4.3.1 自动关机

瑞星防毒墙提供自动关机的功能。在自动关机下，勾选复选框启用防毒墙自动关机功能。您可以根据需要选择时间段关闭防毒墙，选择完自动关机的时间后单击【应用】按钮，保存设置。如图 4.24 所示。

图 4.24 定时关闭防毒墙系统

4.4.3.2 恢复出厂设置

单击【恢复出厂设置】图标，会出现一个对话框，询问是否将系统恢复到出厂状态，单击【确定】按钮，防毒墙系统将恢复到出厂状态，反之则单击【取消】按钮。

图 4.25 恢复防毒墙系统到出厂状态

提示：关于出厂设置

恢复出厂设置不会改变防毒墙的病毒库版本，只会把防毒墙系统配置恢复到出厂状态。

4.4.3.3 关闭系统

单击【关闭系统】图标，会出现一个对话框询问是否确定关闭系统，单击【确定】按钮防毒墙将关闭，反之则单击【取消】按钮。

图 4.26 关闭防毒墙系统

4.4.3.4 重启系统

单击【重启系统】图标  ，会出现一个对话框询问是否确定重启系统，单击【确定】按钮防毒墙将重新启动，反之则单击【取消】。

图 4.27 重启防毒墙系统

4.5 设备配置

4.5.1 系统名称

可以为防毒墙建立一个类似于计算机的主机名，联系人邮件处填写防毒墙管理员的邮件地址。防毒墙在对一些带毒文件的查杀时，可能会导致这些文件不可用。若用户需对这些文件做进一步处理，可以通过上述填写的信息快速联系到管理员。单击【系统管理】➔【设备配置】，如图 4.28 所示，在系统名称页面填写防毒墙主机名和联系人邮件地址。

图 4.28 防毒墙系统信息

4.5.2 设备 ID 维护

防毒墙拥有一个唯一的设备 ID 号，使用这个唯一的设备 ID 号在互联网上注册一个二级域名。当某个接口的 IP 地址使用 PPPoE 和 DHCP 模式时，每次获得的公网地址是不固定的，适用设备 ID 号的二级域名可以迅速解析到该接口的 IP 地址。单击【系统管理】➔【设备管理】，如图 4.29 所示，在设备 ID 维护页面启用设备 ID 维护，并选择对应的接口。

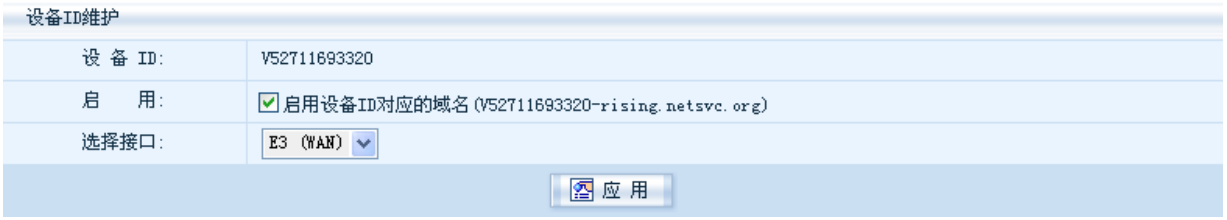


图 4.29 设备 ID 维护

提示：防毒墙设备 ID 功能只能解析接口区域为 WAN 区的地址，即启用此功能必须保证防毒墙能够正常访问 Internet。

4.5.3 SSL 证书管理

由于防毒墙的系统管理是通过 SSL 加密的 Web 方式进行访问，当管理员每次访问防毒墙时，都会弹出是否信任的对话框，这对经常访问防毒墙的管理员造成很大的困扰。通过防毒墙的 SSL 证书管理，可以将防毒墙的认证证书导入到管理主机本地，避免每次访问防毒墙时都需要确认证书可信。单击【系统管理】➔【设备管理】，SSL 证书管理如图 4.30 所示。

图 4.30 SSL 证书管理

1. 在证书通用名处输入防毒墙管理主机 IP 地址，如存在多个管理地址请在证书通用名处逐一输入
2. 单击【应用】按钮保存设置，系统弹出需要重新登录的对话框，如图 4.31 所示

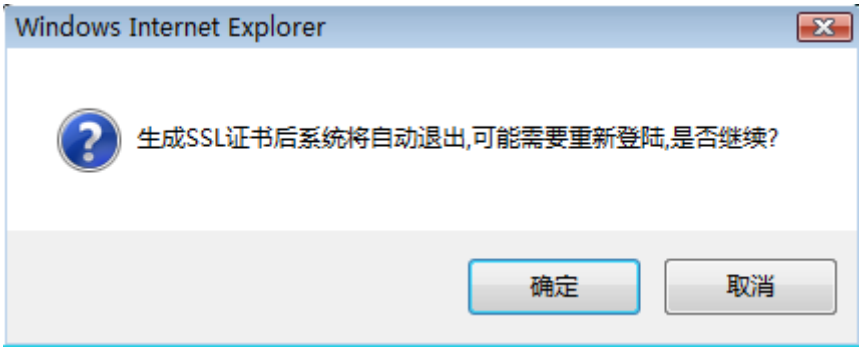


图 4.31 系统 SSL 生成证书

3. 单击图 4.31 中的【确定】按钮，系统返回重新登录界面，输入用户名和密码重新进行系统登录，进入系统后将页面定位到 SSL 证书管理页面，确认先前输入的证书通用名已经保存
4. 单击【下载并安装 SSL 根证书】，系统弹出将证书保存到管理主机的提示，如图 4.32 所示

图 4.32 证书下载提示框

5. 单击上图中的【保存】按钮，将证书存储到管理主机磁盘，存储完成后，双击该文件，系统弹出打开证书的提示，如图 4.33 所示

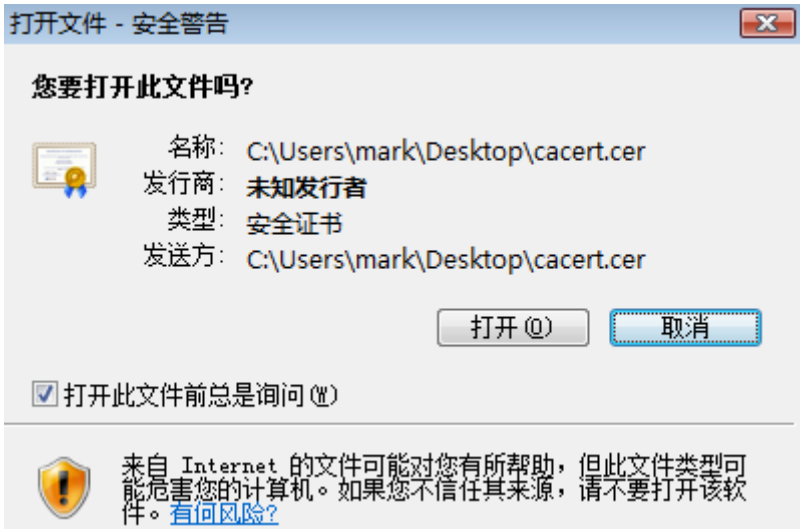


图 4.33 打开证书系统提示

6. 单击【打开】，如图 4.34 所示

图 4.34 防毒墙 SSL 证书

7. 选择【安装证书】，如图 4.35 所示

图 4.35 导入证书

8. 选择【下一步】，如图 4.36 所示

图 4.36 选择证书的存书类型

9. 选择【下一步】，如图 4.37 所示，单击【完成】按钮完成证书导入。

图 4.37 完成证书导入

10. 系统返回导入成功提示框，如图 4.38 所示

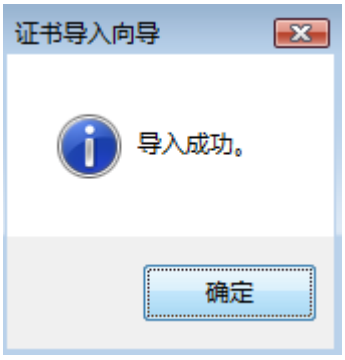


图 4.38 证书导入成功提示框

完成防毒墙证书在管理机上的导入后，在证书的有效期限内，管理机访问该防毒墙系统时将不会弹出系统警告信息。

4.6 DDNS 配置

如果您的企业使用免费域名系统，防毒墙 DDNS 功能可将某个接口获取的 IP 地址自动通过免费域名服务网站注册。单击【系统管理】➔【DDNS 配置】，进入 DDNS 配置页面，如图 4.39 所示。

图 4.39 防毒墙 DDNS 配置页面

4.6.1 增加 DDNS

在 DDNS 配置页面单击【增加】按钮，进入增加 DDNS 页面，如图 4.40 所示

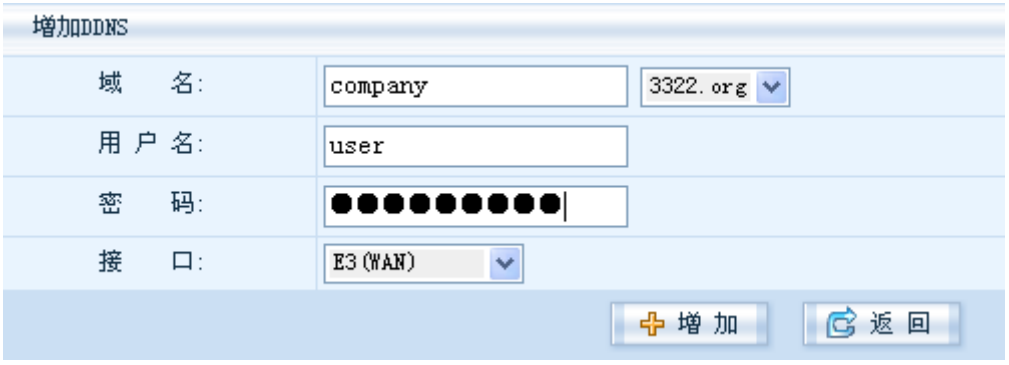


图 4.40 增加 DDNS 记录页面

1. 在域名处输入注册的域名
2. 输入登录免费域名网站的用户名
3. 输入登录免费域名网站的密码
4. 选择使用域名注册接口

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条 DDNS 记录后，DDNS 记录会在主页面上显示出来。如图 4.41 所示。

图 4.41 DDNS 配置列表

图 4.41 各字段文字说明

文字	说明
序号	按照阿拉伯数字排序规则

状态	代表该规则是否开启。绿色图标表示开启，红色图标表示停用状态。管理员可启用或停用规则
域名	在域名服务器上注册的域名全称
用户名	域名服务器登录的用户名
接口	防毒墙哪个接口进行域名注册
注册状态	分为成功和失败两种状态，如果在域名服务器上注册成功则显示成功状态，如果在域名服务器上注册失败则显示失败状态
操作	单击进入修改设置页面
设为启用	如果要启用某个被停用的规则，选中该规则前的复选框单击【设为启用】，则该规则被启用
设为停用	如果要停用某个被启用的规则，选中该规则前的复选框单击【设为停用】，则该规则被停用

表 4.3 防毒墙 DDNS 列表名词解释

4.6.2 修改 DDNS

在 DDNS 配置页面中选择需要修改的 DDNS 记录，单击该记录的图标，进入 DDNS 配置修改页面，如图 4.42 所示。

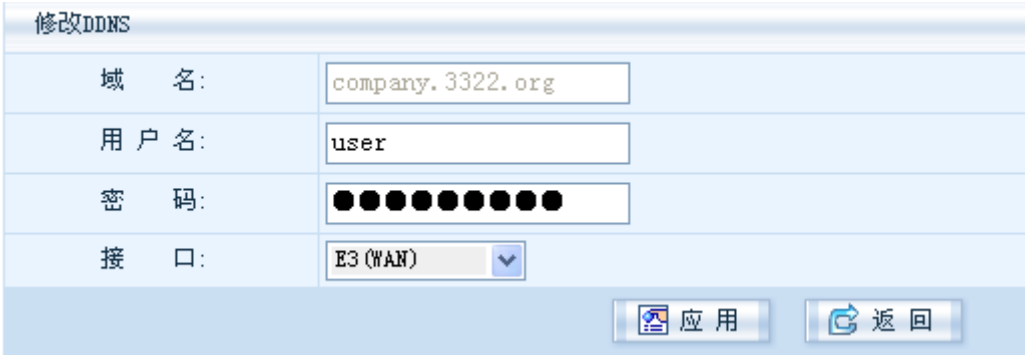


图 4.42 DDNS 配置修改页面

1. 输入登录免费域名网站的用户名
2. 输入登录免费域名网站的密码
3. 选择域名注册的接口

当填写好相关内容后，单击【应用】按钮确认修改，【返回】按钮取消修改。

4.6.3 删除 DDNS

在 DDNS 配置页面选中某条 DDNS 记录，单击【删除】按钮，则删除该条 DDNS 规则。

4.7 DNS 代理

瑞星防毒墙内置了 DNS 代理服务器，为防毒墙的内网计算机提供域名解析代理服务。防毒墙会缓存已知的域名-IP 地址纪录。当需要进行域名对应 IP 地址的解析时，DNS 代理服务器会检查是否有对应历史记录。如果没有才向上一级（如网络服务供应商）的 DNS 服务器查询。从而提高域名解析速度。而且，当上一级的 DNS 服务器 IP 地址更改时，内网计算机的 DNS 无需改动。瑞星防毒墙默认不启用 DNS 代理服务。

关于如何启用 DNS 代理服务，请参考 3.1 接口配置。本节描述如何设置 DNS 代理服务。

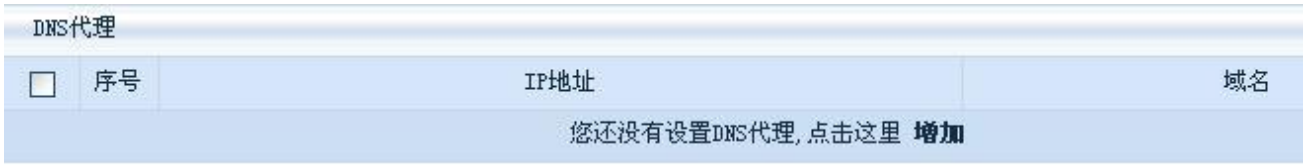


图 4.43 DNS 代理设置

4.7.1 增加 DNS 代理记录

如果想要手动增加一条域名-IP 地址的映射记录，单击 DNS 代理页面上的【增加】按钮，打开添加 DNS 代理页面，如图 4.44 所示。

图 4.44 添加 DNS 代理地址

1. 输入域名对应的 IP 地址
2. 输入要增加的域名
3. 单击【增加】按钮，保存设置

4.7.2 删除 DNS 代理记录

若要删除某个域名-IP 地址的映射记录，选中该记录前的复选框，单击【删除】按钮。如图 4.45 所示。

图 4.45 删除 DNS 代理列表记录

4.8 TCP/IP 选项

网络中很多无效的连接大量消耗网络资源，降低网络性能，并被很多黑客用于攻击企业网络的手段。利用防毒墙的网络超时功能将超时无效的连接予以丢弃，提高网络性能并阻断攻击。单击【系统管理】➔【TCP/IP 选项】，进入超时设置页面，如图 4.46 所示。

图 4.46 网络超时设置页面

图 4.43 各字段文字说明

字段	说明
一般超时	一般网络连接的超时时间
ICMP 超时	ICMP 包响应时间
TCP SYN-SENT	在发送连接请求后等待匹配的连接请求
TCP SYN-RECV	在收到和发送一个连接请求后等待对连接请求的确认
TCP ESTABLISED	表示已经建立了一个连接，可以传输数据
TCP FIN-WAIT	等待远程 TCP 连接的中断请求
TCP CLOSE-WAIT	等待本地网络发出的断开连接的请求
TCP LAST-ACK	等待原来发向远程 TCP 的连接中断请求的确认
TCP TIME-WAIT	等待足够的时间以确保远程 TCP 接收到连接中断请求的确认
TCP CLOSE	表示无 TCP 连接
UDP 超时	UDP 包响应时间
UDP Stream 超时	UDP 数据流超时时间设置

表 4.4 TCP/IP 选项名词解释

单击图 4.43 中的【高级设置】按钮，进行进一步的 TCP/IP 配置，如图 4.47 所示

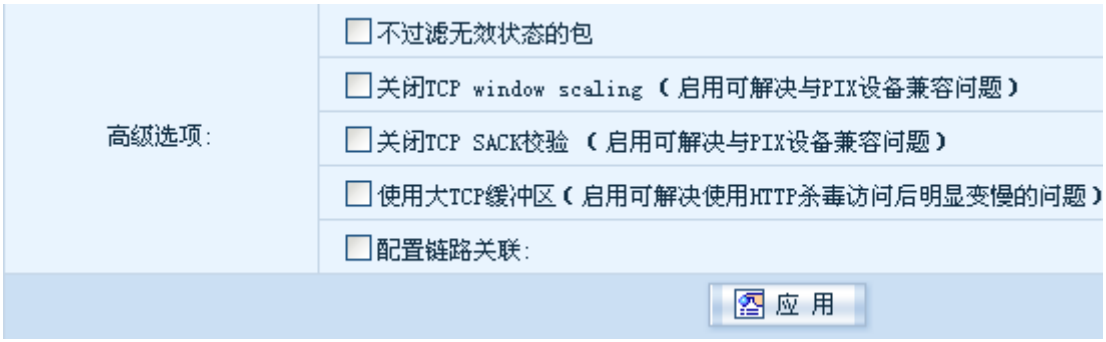


图 4.47 TCP/IP 选项高级设置

图 4.44 各字段文字说明

字段	说明
不过滤无效状态的包	启用此选项，对 TCP/IP 无效的包则不进行过滤
关闭 TCP Windows scaling	启用此选项，可解决与 PIX 设备兼容性的问题
关闭 TCP SACK 校验	启用此选项，可解决与 PIX 设备兼容性的问题
使用大 TCP 缓冲区	启用此选项，可提高 HTTP 杀毒后访问速度变慢的问题
配置链路关联	配置与上层或下层设备进行关联

表 4.5 网络超时名词解释

根据企业的实际网络状况，输入适当的网络超时时间，单击【应用】，保存网络超时设置。

第五章 管理配置

本章介绍防毒墙自身的管理方式以及用户管理机制，主要内容有：

- 帐号配置：防毒墙管理员帐号管理
- 管理主机配置：对远程登录防毒墙系统的工作站的登入点进行设置
- SNMP 配置：配置防毒墙可进行 SNMP 统一管理
- 集中管理：配置多台防毒墙集中统一管理
- 热备配置：配置两台防毒墙处于热备状态

5.1 帐号配置

5.1.1 帐号管理

单击【管理配置】➔【帐号配置】，进入帐号管理页面，防毒墙的超级管理员可对帐号进行管理（增加、删除及修改），如图 5.1 所示。

图 5.1 帐号管理

5.1.1.1 增加帐号

单击【增加】按钮进入增加管理员页面，如图 5.2 所示。

图 5.2 增加管理帐号

- 用户名：进行防毒墙系统登录的用户名
- 密码/重复密码：输入两次防毒墙系统登录的密码进行确认，系统会自动检查密码强度并给出相应

的提示

- 权限：为了防毒墙的管理安全，管理员权限共分为三级

管理员类型	说明
审计管理员	可以阅读部分防毒墙设置，但不可以修改
配置管理员	可以阅读全部防毒墙设置，可以进行部分设置的修改
超级管理员	可以阅读全部防毒墙设置，同时可以修改全部设置

表 5.1 管理员权限列表

- 有效期限：用户可以让管理员帐号只在某一特定的时间范围内有效
- 允许范围：用户可以制定让帐号只在特定的计算机上管理防毒墙，用户可以用三种方式指定 IP 地址
  - 增加一个 IP 地址，例如：192.168.0.1
  - 增加一个网段，例如：192.168.0.1/24
  - 增加一段地址，例如：192.168.0.1-192.168.0.2

系统预设的超级管理员帐号和密码都为 admin，只有超级管理员才可进行帐号的增删。设置完成后，单击【增加】按钮保存设置，【返回】按钮取消操作。同时，增加的管理员帐号会自动加入到管理员列表中。

5.1.1.2 修改帐号

如果需要修改已存在的用户名密码，单击该记录的 图标进入修改管理员页面。

图 5.3 修改系统帐号权限

可在修改页面修改密码、权限、有效期限和访问管理的源 IP 地址范围。

注意：不能修改帐号的用户名。

提示：关于帐号管理权限

只有超级管理员拥有全部帐号的修改和删除权限，而审计管理员和配置管理员对于帐号管理只有修改密码和源地址的权限。

5.1.1.3 删除帐号

若要删除某个帐号，选中该帐号，然后单击【删除】按钮（只有超级管理员具备该权限）。

5.1.2 在线用户管理

单击【管理设置】➔【帐号配置】，进入在线用户管理页面，如图 5.4 所示。

在线用户管理

	序号	管理员	类型	访问方式	访问IP	空闲时间(S)
☐	1	admin	超级管理员	web	192.168.100.111	0
☑	2	admin	超级管理员	web	192.168.100.88	7

踢 出

图 5.4 防毒墙在线用户

单击【踢出】按钮，超级管理员可以在这里将踢出不希望其继续管理防毒墙的帐号，如图 5.5 所示。

图 5.5 执行踢出操作

单击【确定】按钮，执行踢出操作或单击【取消】按钮取消操作。

5.2 管理主机配置

防毒墙的日常维护一般都是通过远程管理完成，请仔细设置相关的内容以保证防毒墙的管理安全。

5.2.1 远程管理选项

单击【管理配置】➔【管理主机配置】，进入防毒墙远程管理设置页面。设置远程管理防毒墙时的管理超时、自解锁时间和错误登录次数，如图 5.6 所示。

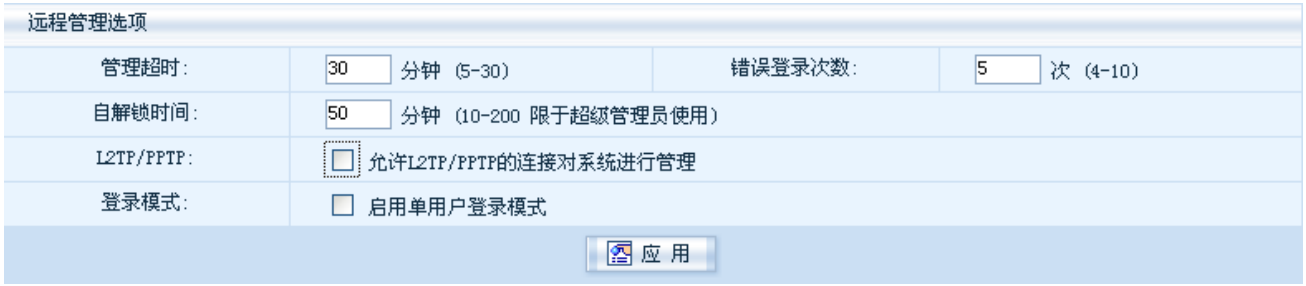


图 5.6 远程管理选项

- 管理超时：为了防止恶意修改防毒墙，当管理员在设置的时间内没有对防毒墙进行管理，则当管理员再次对防毒墙进行管理动作时，系统将退出管理页面,提示管理员重新登录。其默认配置时间为 30 分钟
- 错误登录次数：设置允许尝试登录的次数。如果某一帐号超过允许尝试登录的次数而没有正确登录，管理页面将弹出消息框提示“该用户被锁定”，只有防毒墙自解锁时间过后才能继续尝试登录。其默认配置为 5 次
- 自解锁时间：设置防毒墙帐号因为超过允许尝试登录次数而被锁定后系统自动解除锁定的间隔时间，其默认配置为 60 分钟
- L2TP/PPTP：启用此功能将允许用户通过 L2TP/PPTP 的方式连接到防毒墙并进行管理操作
- 登录模式：此功能将启用管理员单一登录模式，即一个管理员帐号只允许当前一个工作站登录管理防毒墙

设置完成后，单击【应用】按钮保存设置。

5.2.2 IP 访问控制

设置允许或禁用通过 Web 管理防毒墙的 IP 地址或地址段，如图 5.7 所示。

图 5.7 IP 访问控制

提示：关于 IP 访问控制

1. 防毒墙默认允许所有地址进行远程 Web 管理
2. 增加的 IP 范围必须和防毒墙的管理接口在同一网段才能生效
3. 一旦增加了 IP 访问控制，只有在控制列表中允许的地址才可以管理防毒墙，不在地址列表中的所有远程管理请求将被拒绝
4. 当在 IP 访问列表中拒绝某一网段的管理请求时，其他的地址仍然可以管理防毒墙

5.2.2.1 增加 IP 访问控制列表

单击 IP 访问控制页面中的【增加】按钮，增加一条访问控制记录，如图 5.8 所示。

图 5.8 增加 IP 访问控制地址

- 状态：选中启用框，表示该策略生效
- 策略：分为“允许”和“拒绝”两种策略。“允许”即该 IP 地址或网段可以访问防毒墙；“拒绝”则该 IP 地址或网段不能访问防毒墙
- 网段：填写 IP 地址或网段。如果为单一的 IP 地址，直接填写 IP 地址，否则需要填写 IP 地址/网段。例如：
  - 增加一个 IP 地址：192.168.0.1/32
  - 增加一个网段：192.168.0.1/24

设置完成后，单击【增加】按钮保存设置。

5.2.2.2 修改 IP 访问控制列表

如果需要修改已存在的列表，请单击该记录的图标进入修改页面进行修改。修改的内容见增加 IP 访问控制列表中的相关说明。

5.2.2.3 删除 IP 访问控制列表

如果需要删除已存在的列表，选中要删除策略，单击【删除】按钮。

5.2.2.4 启用/停用 IP 访问控制列表

当增加 IP 访问列表后，防毒墙会显示相关的内容，如图 5.9 所示。

图 5.9 IP 访问控制

其中状态栏中的红色图标表示该条策略为停用状态。如果需要这条策略生效，则选中该条策略，单击下面的【设为启用】按钮，系统会提示是否启用该条策略，如图 5.10 所示。

图 5.10 启用指定的策略

单击【确定】按钮启用该条策略，系统会返回该命令执行的结果，如图 5.11 所示。

5.11 启用 IP 访问控制策略执行成功

如果想放弃启用这条策略，单击【取消】取消启用该条策略的操作。

5.3 SNMP 配置

SNMP 即简单网络管理协议，通过 SNMP 管理软件可进行公司内部多台网络设备的统一管理，降低企业网络管理员的工作量，大大提高工作效率，目前大多数网络设备都支持 SNMP 功能。单击【管理配置】➔【SNMP 配置】，进入 SNMP 配置页面，如图 5.12 所示。

图 5.12 SNMP 配置页面

SNMP 配置分为：基本设置、查阅选项、TRAP 设置和基本信息四个部分，各部分配置无依存关系，可独立进行配置。

5.3.1 基本设置

用户设置部分为进行 SNMP 统一管理时的认证信息，通过设置此部分内容建立防毒墙与 SNMP 管理软件之间的信任连接。SNMP 共分为三个版本 V1、V2C 和 V3，此部分的公共体相当于口令，V1 和 V2C 都是使用公共体进行 SNMP 连接。其设置步骤如下：

1. 选择 SNMP 的版本
2. 在版本处选择 V1 或 V2C 时，在下面输入公共体信息，如图 5.13 所示。

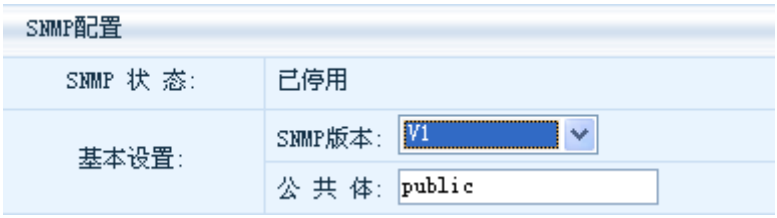


图 5.13 SNMP V1 和 V2C 设置

3. 当选择 V3 时，其设置如下：
   a) 在用户名处输入认证的用户名，长度不小于 6 位
   b) 在密码处输入认证的密码，长度不小于 8 位
   c) 在加密密码处输入加密传输时使用的密钥信息，长度不小于 8 位
   d) 勾选【可写】复选框则通过 SNMP 管理软件可读-写防毒墙设置，否则只能读取防毒墙设置

图 5.14 SNMP V3 版本设置

4. 单击【应用】，保存 SNMP 配置信息。如图 5.15 所示

图 5.15 保存 SNMP 配置

5. 单击【启用】启用防毒墙 SNMP 功能，如图 5.16 所示

图 5.16 启用防毒墙 SNMP 功能

6. 如需停止防毒墙 SNMP 功能，单击【停用】按钮，如图 5.17 所示

图 5.17 停用防毒墙 SNMP 功能

5.3.2 查阅选项

查阅选项分为：CPU 信息、内存信息、磁盘信息和病毒信息四个部分，勾选需要查看的防毒墙信息，如图 5.18 所示。

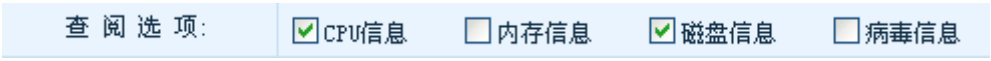


图 5.18 SNMP 查阅选项

单击【应用】，保存 SNMP 配置信息。如图 5.19 所示

图 5.19 保存 SNMP 配置

5.3.3TRAP 设置

通过配置 TRAP 功能，可向 SNMP 管理中心发送信息，例如：登录提示、离线提示等。其设置步骤如下：

1. 在版本处选择 V1 或 V2C
2. 在主机 IP 处输入 SNMP 管理中心的 IP 地址，并保证防毒墙能与 SNMP 管理中心正常通讯
3. 输入公共体名称
4. 单击【应用】，保存 SNMP 配置信息。如图 5.20 所示

图 5.20 保存 SNMP 配置

5. 单击【启用】启用防毒墙 SNMP 功能，如图 5.21 所示

图 5.21 启用防毒墙 SNMP 功能

6. 如需停止防毒墙 SNMP 功能，单击【停用】按钮，如图 5.22 所示

图 5.22 停用防毒墙 SNMP 功能

5.3.4 基本信息

基本信息部分可输入防毒墙的详细信息，方便管理员在管理多台网络设备时迅速定位需要查找的设备。其设置步骤如下：

1. 在设备名称处输入设备的制造厂商或型号
2. 在联系人处输入该设备的管理员信息
3. 在联系地址处输入该管理员的联系信息，如：邮件、电话、地址等等
4. 单击【应用】，保存 SNMP 配置信息。如图 5.23 所示

图 5.23 保存 SNMP 配置

5.4 集中管理

瑞星防毒墙支持三级分层结构，分别为总中心防毒墙、分中心防毒墙和子防毒墙。其分层结构可由一个总的节点控制，当您的企业中拥有多台防毒墙时，您可以根据防毒墙所处的网络位置确定其身份，简化管理工作。

5.4.1 创建防毒墙身份

单击【管理设置】➔【集中管理】，进入集中管理配置页面，如图 5.24 所示。

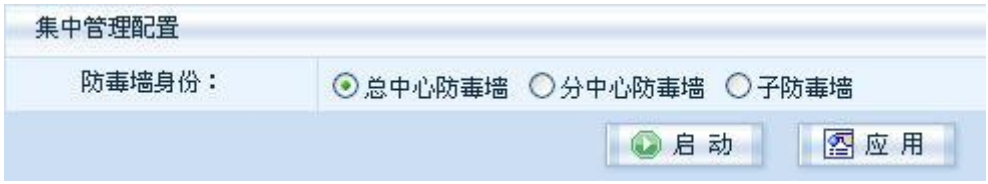


图 5.24 防毒墙集中管理配置页面

- 创建总中心防毒墙

1. 在防毒墙身份处选择总中心防毒墙，单击【应用】按钮，如图 5.25 所示

图 5.25 确认防毒墙身份设置

2. 单击图 5.25【确定】按钮，返回集中管理配置页面，单击【启动】，如图 5.26 所示

图 5.26 确认启动集中管理

3. 单击图 5.26【确定】按钮，返回集中管理配置页面，如图 5.27 所示

图 5.27 启动总中心集中管理页面

- 创建分中心防毒墙

1. 在防毒墙身份处选择分中心防毒墙，如图 5.28 所示

图 5.28 分中心防毒墙设置页面

2. 在允许管理 IP 处输入用于管理分中心防毒墙的总中心防毒墙 IP 地址，便于总中心进行管理
3. 在密码处输入防毒墙集中管理的验证密码
4. 单击【应用】按钮，如图 5.29 所示

图 5.29 确认防毒墙身份设置

5. 单击图 5.29【确定】按钮，返回集中管理配置页面，单击【启动】，如图 5.30 所示

图 5.30 确认启动集中管理

6. 单击图 5.30【确定】按钮，返回集中管理配置页面，如图 5.31 所示

图 5.31 启动分中心防毒墙集中管理页面

- 创建子防毒墙

1. 在防毒墙身份处选择子防毒墙，如图 5.32 所示

图 5.32 子防毒墙设置页面

2. 在允许管理 IP 处输入用于管理子防毒墙的分中心防毒墙 IP 地址，便于分中心防毒墙进行管理

3. 在密码处输入防毒墙集中管理的验证密码

4. 单击【应用】按钮，如图 5.33 所示

图 5.33 确认防毒墙身份设置

5. 单击图 5.33【确定】按钮，返回集中管理配置页面，如图 5.34 所示

图 5.34 子防毒墙集中管理启动页面

5.4.2 停止防毒墙集中管理

当防毒墙身份为总中心防毒墙或分中心防毒墙时，单击图 5.35 中的【停止】按钮，取消防毒墙集中管理功能。

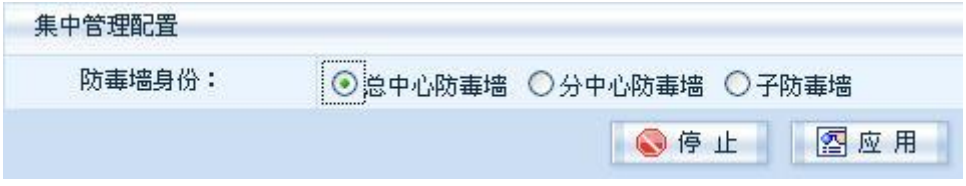


图 5.35 防毒墙集中管理状态

5.4.3 可管理 IP 列表

可管理 IP 列表显示当前防毒墙可进行集中管理的防毒墙列表，如图 5.36 所示。

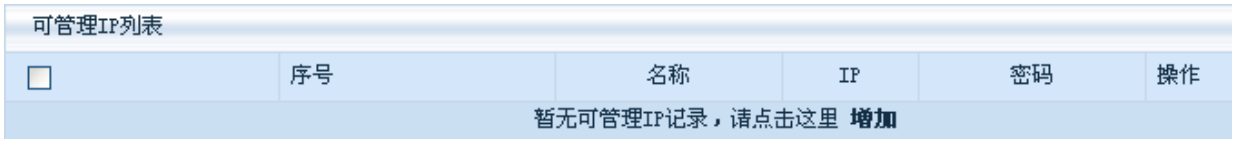


图 5.36 防毒墙集中管理列表

5.4.3.1 增加集中管理 IP 地址

在可管理 IP 列表中单击【增加】按钮，进入增加可管理 IP 页面，如图 5.37 所示。

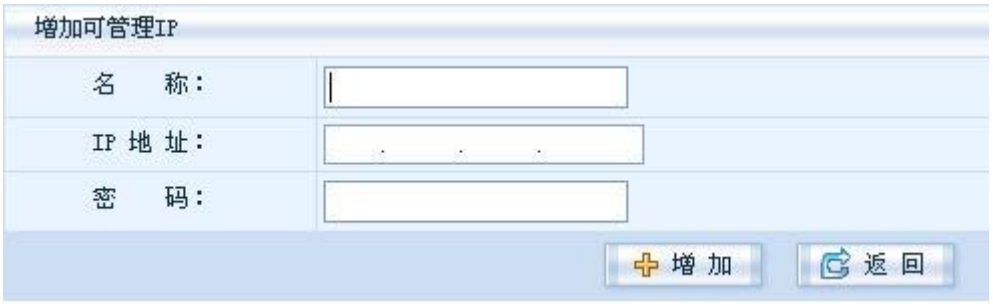


图 5.37 增加防毒墙可管理 IP

1. 在名称处输入需要进行管理的防毒墙的名称
2. 在 IP 地址处输入总中心或分中心下各个防毒墙节点的管理 IP 地址
3. 在密码处输入防毒墙集中管理的密码

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条管理 IP 记录后，集中管理 IP 记录会在主页面上显示出来。如图 5.38 所示。

图 5.38 可集中管理 IP 列表

5.4.3.2 修改集中管理 IP 地址

单击可管理 IP 列表的某条记录的 图标，进入防毒墙可集中管理 IP 地址修改页面，如图 5.39 所示。

图 5.39 修改防毒墙可管理 IP 地址

1. 在 IP 地址处修改总中心或分中心下各个防毒墙节点的管理 IP 地址
2. 在密码处修改防毒墙集中管理的密码

当填写好相关内容后，单击【确定】按钮确认修改，【返回】按钮取消修改。

5.4.3.3 删除集中管理 IP 地址

如果需要删除已存在的记录，选中要删除记录，单击【删除】按钮。

5.4.4 进行管理

单击上层防毒墙任何管理界面右侧的  图标，如图 5.40 所示。

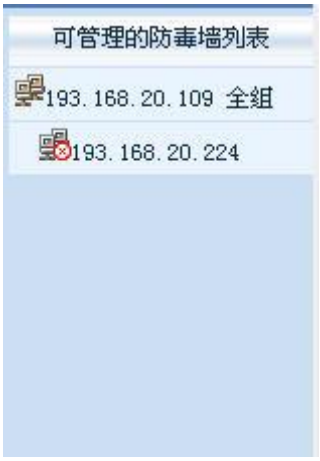


图 5.40 防毒墙可管理列表

单击下级防毒墙的 IP 地址，进入下级防毒墙管理界面进行防毒墙的系统管理。

5.5 热备配置

瑞星防毒墙支持双机热备功能，为用户提供不间断网络服务，当主防毒墙因故障原因无法运行时，另一台备用防毒墙会马上接管其所有工作，保证网络的安全畅通，单击【管理配置】➔【热备配置】，进入热备配置页面。

5.5.1 主机配置

当用户在热备身份中选择主机时，会显示主机的相关配置。如图 5.41 所示。

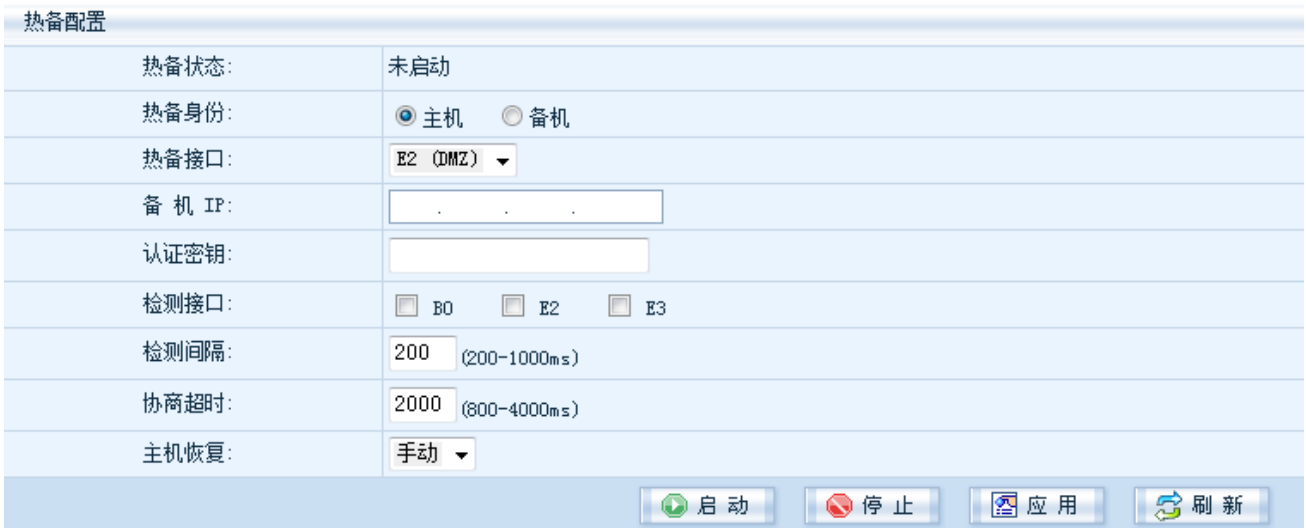


图 5.41 防毒墙热备主机配置

字段	说明
热备状态	显示防毒墙热备状态，分为已启动和未启动两种状态
热备身份	选择该防毒墙为主机还是备机
热备接口	与备机相连的网口
备机 IP	实现与备机间高速数据传输。当防毒墙身份为主机时，备机 IP 应为与之相连的防毒墙备机热备接口的 IP 地址
认证密钥	两台防毒墙进行协商的密钥
检测接口	选择热备协商时进行检测的防毒墙正在工作的接口
协商间隔	设置两台防毒墙进行协商的间隔时间
协商超时	设置两台防毒墙协商超时时间
主机恢复	当主机从故障中恢复正常，从备机接管工作。分为手动和自动，当选择自动时，主机在协商时间内自动接管备机的工作；当选择手动时，主机不接管备机工作，需管理员在需要主机进行接管时，将主机恢复改为自动，单击【应用】，主机才会在协商时间内自动接管备机的工作

表 5.2 防毒墙热备主机配置说明

5.5.2 备机配置

当用户选择备机时，会显示备机的相关配置，如图 5.42 所示。

图 5.42 防毒墙热备备机配置

字段	说明
热备状态	显示防毒墙热备状态，分为已启动和未启动两种状态
热备身份	选择该防毒墙为主机还是备机
热备接口	与主机相连的网口
主机 IP	实现与主机间高速数据传输。当防毒墙身份为备机时，主机 IP 应为与之相连的防毒墙主机热备接口的 IP 地址
认证密钥	两台防毒墙进行协商的密钥

表 5.3 防毒墙热备备机配置说明

第六章 防毒配置

防毒墙的一个重要作用就是进行病毒扫描。它支持邮局协议（POP3）、简单邮件传输协议（SMTP）、文件传输协议（FTP）、超文本传输协议（HTTP）、MSN 协议和 IMAP 协议。通过病毒扫描功能，可以实现查杀邮件附件、传输文件和网页内容中的病毒。

将上述协议的病毒扫描启用后，防毒墙就自动扫描使用该协议传输的数据，并进行病毒检测。为确保瑞星防毒墙能够检测最新的病毒，请您及时升级其病毒库文件。有关病毒库更新，请参阅本用户手册软件升级。

用户可以从以下三个方面配置防毒墙的病毒处理行为：

- 防毒配置：防毒墙防毒策略配置
- HTTP 白名单：设置某些安全的站点不进行杀毒，提高网站浏览速度
- 邮件白名单：设置某些安全的联系人和邮件域不进行杀毒，提高邮件的收发速度

提示：关于杀毒

1. 受邮件代理所限，防毒墙邮件扫描暂不支持 Unicode 编码。但由于目前绝大多数的邮件用户都设定成使用多目的因特网邮件扩展(MIME)编码，因此不支持 Unicode 编码几乎不会给您带来安全问题
2. 瑞星防毒墙可对 MSN，Hotmail 和 Yahoo 等基于网页的邮件系统进行有效地扫描
3. 防毒墙支持对最大为 100 层压缩的文件进行扫描
4. 防毒墙可扫描大部分压缩文件格式（.rar 和.ace 文件必须是由 WinRAR 3.0 或更高版本生成的）。当同时有大量的压缩文件附件到达时，可能会造成网络性能的下降
5. 防毒墙不能扫描带有密码保护的压缩文件

6.1 防毒配置

6.1.1 病毒查杀配置

单击【防毒配置】➔【防病毒配置】，进入病毒查杀配置页面，如图 6.1 所示。

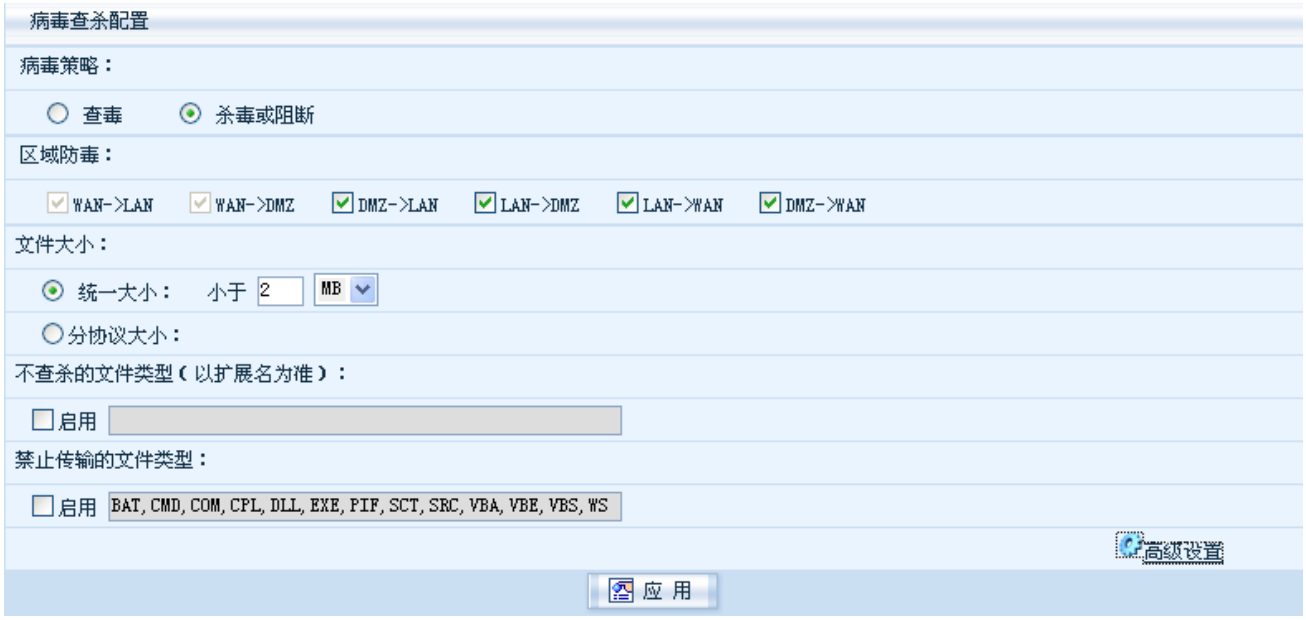


图 6.1 病毒查杀配置页面

6.1.1.1 病毒策略

可以选择“查毒”或“杀毒或阻断”操作。若设置为查毒，发现病毒后不做删除等处理，只在日志中记录。若设置为杀毒或阻断，则发现病毒后会进行清除，并在日志中记录。如图 6.2 所示。

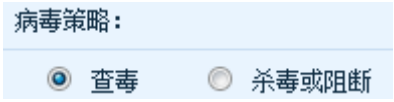


图 6.2 防毒墙病毒策略

6.1.1.2 区域防毒

这里，用户可以选择只对特定流向的数据进行杀毒操作。其中 WAN ➔ LAN 和 WAN ➔ DMZ 为不可修改选项，瑞星防毒墙强制对非安全区域到安全区域和中立区的数据进行杀毒。其它区域之间传输数据时是否进行杀毒操作，可根据企业网络情况有选择的启用。在局域网和 DMZ 之间设立有效的安全杀毒屏障，阻断病毒在内部区域内传播，如图 6.3 所示。

图 6.3 防毒墙区域防毒

6.1.1.3 查杀文件大小设置

为了保证系统正常工作，防毒墙不会对过大的文件进行病毒查杀。用户可以通过如下两种方式指定查杀文件的大小。如果不进行任何设置，防毒墙默认统一指定查杀文件的大小为 2MB。

- 统一指定查杀文件的大小，若数据文件超过指定的大小将不做查杀，如图 6.4 所示

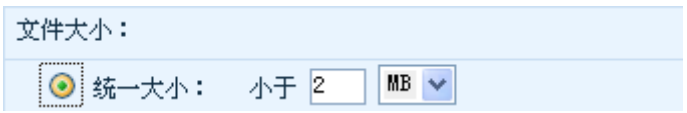


图 6.4 设置统一查杀文件的大小

- 分协议指定杀毒文件大小：对通过 HTTP、FTP、SMTP、POP3 和 MSN 五种协议传输的数据分别指定查杀文件的大小，若文件超过设置的大小将不做查杀，如图 6.5 所示。

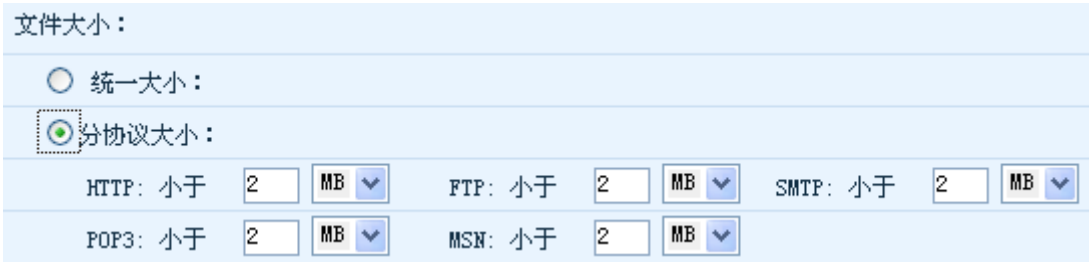


图 6.5 分别指定查杀文件大小

提示：关于杀毒

查杀文件的大小以 MB 和 KB 为单位。当以 MB 为单位时：范围是 1-10 之间；当以 KB 为单位时，范围是 1-999 之间。

6.1.1.4 查杀类型

这里用户可以选择防毒墙查杀文件的类型。防毒墙默认查杀常用的文件类型，另外用户还可以向防毒墙中增加自定义的文件类型。如图 6.6 所示。

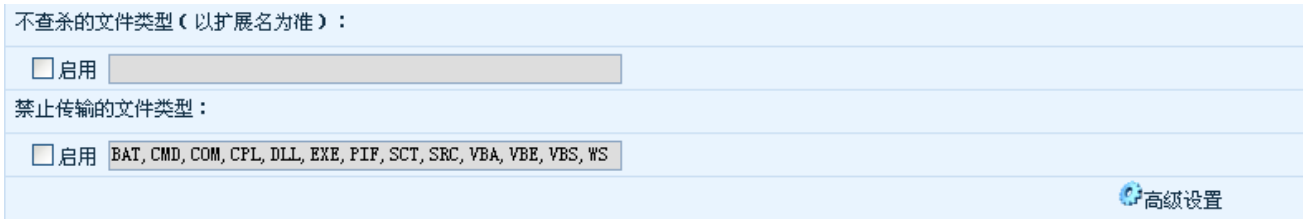


图 6.6 病毒查杀设置页面

- 不查杀的文件类型：单击【启用】输入文件类型使防毒墙不进行查杀，例如：iso,
- 禁止传输的文件类型：防毒墙系统默认将 BAT、CMD、COM、CPL、DLL、EXE、PIF、SCT、SRC、VBA、VBE、VBS、WS 这些会给用户网络带来危险的文件类型归纳到禁止传输的文件类型中，启用它会使您的网络更加安全

另外，当用户需要进一步定制引擎的行为时，可以单击【高级设置】按钮。如图 6.7 所示。

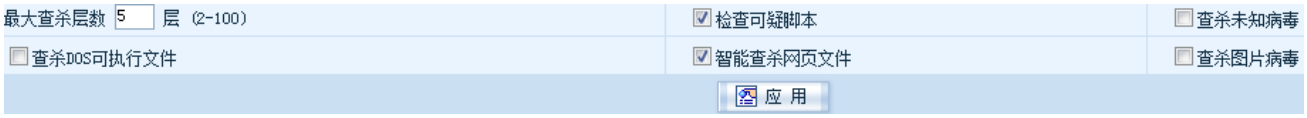


图 6.7 查杀类型的高级设置

- 最大查杀层数：当文件被压缩时，指定防毒墙可以识别的压缩层数（系统默认查杀 5 层压缩文件，最多可以解压缩 100 层，但不建议用户设置太多的压缩层数）；

- 检查可疑脚本：对可疑脚本进行检测并阻断；
- 查杀未知病毒：利用防毒引擎的未知病毒查杀功能对病毒进行识别；
- 查杀 DOS 可执行文件：对 DOS 下的可执行文件进行查杀；
- 智能查杀网页文件：当客户端访问某些包含安全威胁网页时，防毒墙根据网页包含的病毒特征决定是否阻断此次连接，如不满足阻断条件则在防毒墙日志中进行记录；
- 查杀图片病毒：利用防毒引擎的图片查杀功能对病毒进行识别；

6.1.2 协议设置

用户在这里可以对 HTTP 和 FTP 协议做更进一步的设定，如图 6.8 所示。

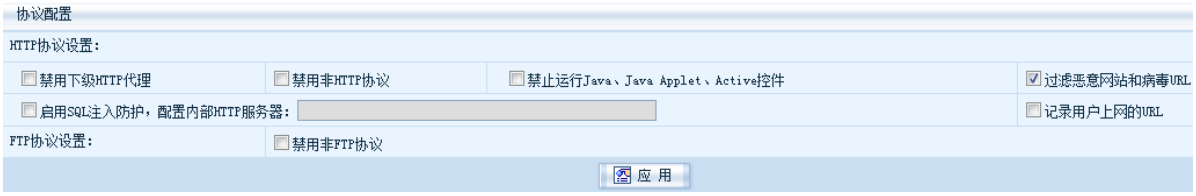


图 6.8 协议配置

- HTTP 协议设置
  - 禁用下级代理：通过防毒墙后的数据不能是指向一个代理服务器的数据
  - 禁用非 HTTP 协议：防毒墙进行 HTTP 协议杀毒操作时，指定杀毒的端口如果进行非 HTTP 协议数据的传输，防毒墙将丢弃这些数据
  - 禁止运行 Java、Java Applet、Active 控件：启用此功能，防毒墙将限制用户访问 Web 页面时运行 Java、Java Applet、Active 控件
  - 过滤恶意网站和病毒 URL：启用此功能将过滤已经分析出来的恶意网站和病毒 URL 地址，此列表将不断更新
  - 启用 SQL 注入防护：启用此功能可防止内部的数据库服务器被注入攻击，勾选启用后将内部的服务器地址输入到文本框中
  - 记录用户上网的 URL：记录用户通过防毒墙上网的 url 地址，并在日志中记录
- FTP 协议设置
  - 禁用非 FTP 协议：防毒墙进行 FTP 协议杀毒操作时，指定杀毒的端口如果进行非 FTP 协议数据的传输，防毒墙将丢弃这些数据

6.2 HTTP 白名单

通过设置瑞星防毒墙 HTTP 白名单，可让一些经常访问的安全站点跳过防毒墙的 HTTP 协议检查，提高页面的访问速度，减少防毒墙的系统开销。单击菜单【防毒配置】➔【HTTP 白名单】，进入 HTTP 协议访问不查杀站点名单页面，如图 6.9 所示。

图 6.9 防毒墙白名单设置

6.2.1 增加白名单记录

单击【增加】按钮，进入增加白名单对象页面，如图 6.10 所示。

图 6.10 增加白名单对象

在网址处输入想要增加到白名单的网址，例如 www.rising.com.cn，单击【增加】按钮保存配置。如图 6.11 所示。

图 6.11 白名单列表

这样，所有通过防毒墙访问 www.rising.com.cn 的 HTTP 数据将不再进行检查。

6.2.2 删除 HTTP 白名单记录

当管理员确定白名单中某条记录为不安全站点时，可选中该条记录，单击【删除】按钮删除白名单记录，防毒墙将重新检查这个站点。

6.3 邮件白名单

通过设置瑞星防毒墙邮件白名单，让一些安全的邮件服务器进行邮件传输时跳过防毒墙的检查，减少防毒墙的性能开销。单击菜单【防毒配置】➔【邮件白名单】，进入邮件地址白名单页面，如图 6.12 所示。

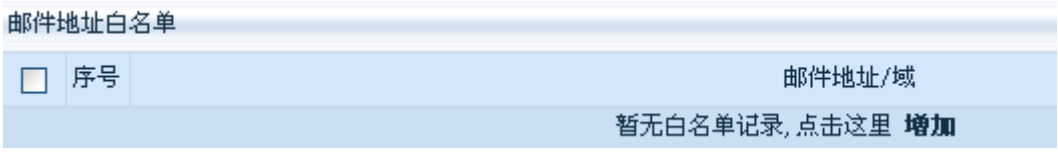


图 6.12 防毒墙邮件白名单设置

6.3.1 增加白名单记录

单击【增加】按钮，进入增加白名单对象页面，如图 6.13 所示。

图 6.13 增加邮件白名单域

在邮件地址/域输入想要增加的邮件地址/域，例如@163.com，单击【增加】按钮保存配置。如图 6.14 所示。

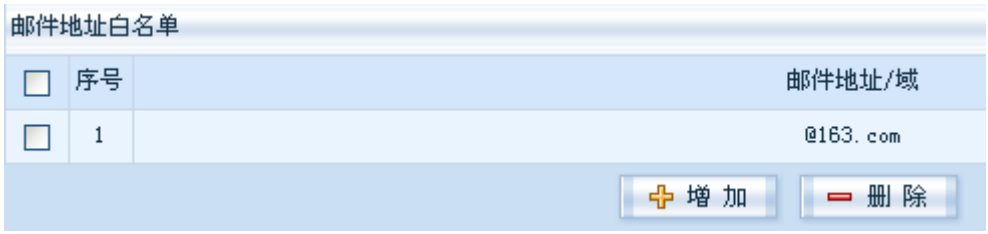


图 6.14 邮件地址白名单列表

这样，所有通过防毒墙的 163 邮件域的邮件将不进行检查。

6.3.2 删除邮件白名单记录

当管理员确定白名单中某条记录不安全时，可选中该条记录，单击【删除】按钮删除白名单记录，防毒墙将重新检查这个邮件地址/域。

第七章　垃圾邮件（可选模块）

瑞星反垃圾邮件引擎结合了传统的基于关键字的检测以及先进的集中判别技术，采用了分布式设计，可以实时更新垃圾邮件数据库，在用户不做任何设置的情况下，垃圾邮件的识别率可以达到 90%以上。从而在网关处有效帮助用户过滤垃圾邮件，避免垃圾邮件发送到企业内部邮件服务器，减少因为处理垃圾邮件而耽误的工作时间。同时也支持与局域网内邮件客户端自定义标识，从而提高垃圾邮件的分捡效率和垃圾邮件识别率，简化管理员的管理工作。本章介绍瑞星反垃圾邮件引擎的配置和使用。

- 垃圾邮件判定：设置防毒墙反垃圾邮件引擎的过滤规则
- 邮件摘要发送：将防毒墙过滤的垃圾邮件信息发送给相关人员

提示：关于防毒墙反垃圾模块

瑞星防毒墙“反垃圾邮件”功能为可选功能组件模块，如需应用需另行购买。

7.1 垃圾邮件的判定

瑞星反垃圾邮件引擎一方面可以利用集中判别技术自动根据邮件发送行为自动对垃圾邮件进行识别，同时，出于效率方面的考虑，用户也可以自行指定黑白名单以及过滤关键字。

7.1.1 反垃圾邮件功能配置

单击菜单【垃圾邮件】➔【垃圾邮件判定】，进入反垃圾邮件功能配置页面，如图 7.1 所示。

图 7.1 反垃圾邮件功能配置

选中【启用垃圾邮件过滤】复选框单击【应用】按钮，则防毒墙反垃圾邮件功能开启；反之，则关闭防毒墙反垃圾邮件功能。

7.1.2 反垃圾邮件基本配置

单击菜单【垃圾邮件】➔【垃圾邮件判定】，进入反垃圾邮件基本设置页面，如图 7.2 所示。

图 7.2 垃圾邮件判定

- 启用发件人白名单：选中反垃圾邮件基本配置页面中的【启用发件人白名单】复选框启用这项功能，在下面的文本框中输入不希望防毒墙反垃圾功能过滤的邮件地址，单击【应用】按钮保存设置
- 启用发件人黑名单：选中反垃圾邮件基本配置页面中的【启用发件人黑名单】复选框启用这项功能，在下面的文本框中输入希望防毒墙直接判定为垃圾邮件的邮件地址，单击【应用】保存设置
- 关键字过滤：选中反垃圾邮件基本配置页面中的【启用邮件标题中的广告关键词过滤】复选框启用这项功能，在下面的文本框中列表增加一些常用明显带有骚扰性质的内容，例如：推销、发票等信息，防毒墙将邮件标题中带有这些信息的邮件直接过滤

提示：关于黑白名单以及关键字的增加和删除

在增加多条关键字以及黑白名单时，按 Enter 键换行输入即可。需要取消某些黑白名单或关键字时，只需要选中要删除的内容，按 Delete 键后，单击【应用】按钮即可。

7.1.3 反垃圾邮件详细设置

- SMTP 反垃圾邮件设置

单击【垃圾邮件】➔【垃圾邮件判定】，进入 SMTP 内部邮件域校验页面，如图 7.3 所示。

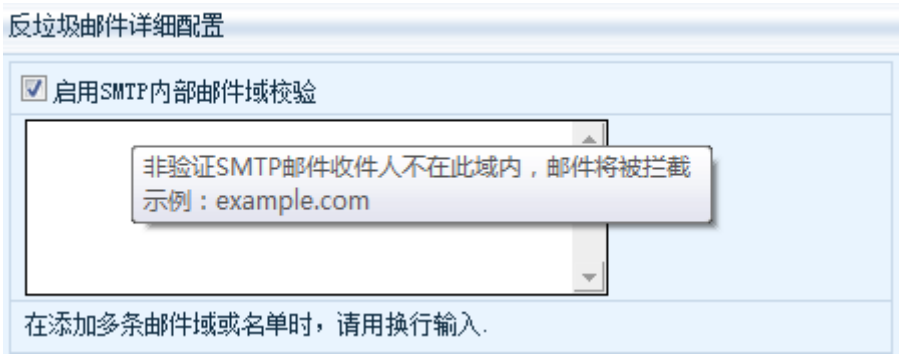


图 7.3 SMTP 内部邮件域校验配置页面

选中 SMTP 反垃圾邮件配置页面中的【启用 SMTP 内部邮件域校验】复选框启用这项功能。当启用该功能时，防毒墙会把经过的邮件的目的邮件域和内部邮件域校验列表中的邮件域进行比对，当没有找到匹配时，防毒墙将直接过滤掉邮件。此项功能可以有效的防止垃圾邮件的传播，避免邮件服务器被当作垃圾邮件中继服务器，被非法分子利用。

选中 SMTP 反垃圾邮件配置页面中的【使用内部域宽校验】复选框启用这项功能。当启用该功能时，防毒墙将以更为宽松校验方式对发件人和收件人的邮件地址进行检查。

提示：关于邮件域的增加和删除

在增加多条内部邮件域时，按 Enter 键换行输入即可。需要取消某些邮件域时，只需要选中要删除的内容，按 Delete 键后，单击【应用】按钮即可。

7.1.4 POP3 反垃圾邮件标识

单击【垃圾邮件】➔【垃圾邮件判定】，进入 POP3 自定义邮件分类标识页面，如图 7.4 所示。

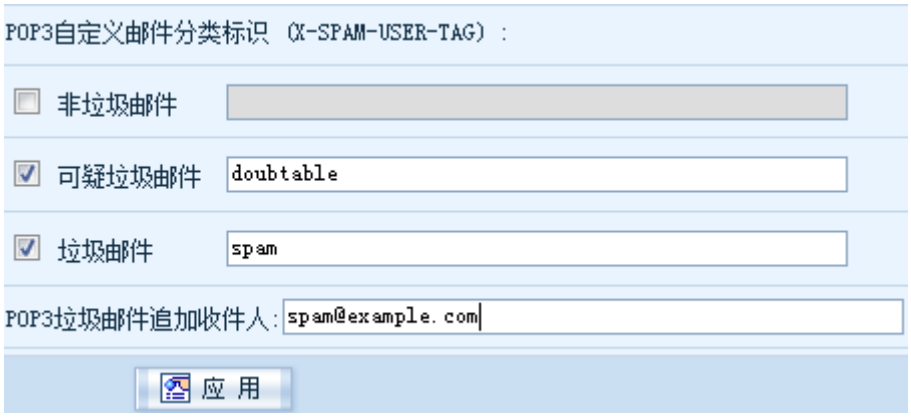


图 7.4 POP3 反垃圾邮件标识

瑞星防毒墙反垃圾邮件功能支持用户分类标识，当用户收取一些企业外部公网邮箱的邮件时，由于邮件已经到达公网邮件服务器，防毒墙此时不对已经到达邮件服务器的邮件进行拦截。当用户进行 pop 下载时，瑞星防毒墙反垃圾引擎对邮件进行扫描后添加标记，通过用户邮件客户端的分拣机制对邮件进行分类。

- 非垃圾邮件：输入非垃圾邮件的标记信息
- 可疑垃圾邮件：输入可疑垃圾邮件的标记信息
- 垃圾邮件：输入垃圾邮件的标记信息
- Pop3 垃圾邮件追加收件人：按照标准邮件格式输入一个邮件地址，反垃圾引擎会将检测到的垃圾邮件加入该邮件地址标记，通过邮件客户端的分拣机制将该邮件扔入邮件客户端的垃圾邮箱

单击【应用】，当防毒墙下载邮件时会根据所提供的信息进行判定，进一步提高了垃圾邮件的识别率。

如果要删除自定义邮件分类标识下的某条信息或取消某项功能，可取消“非垃圾邮件”、“可疑垃圾邮件”和“垃圾邮件”选项，单击【应用】，防毒墙接收邮件时将不对邮件进行标记。

7.2 邮件摘要发送

防毒墙可以定期把拦截到的邮件的摘要信息发送给这些邮件的收件人，防止由于误报给用户带来损失。

7.2.1 垃圾邮件摘要发送计划

单击【垃圾邮件】➔【邮件摘要发送】，进入垃圾邮件摘要发送计划页面，如图 7.5 所示。

图 7.5 垃圾邮件摘要发送时间

用户可以按照星期和发送时间的组合来定义发送计划，对于发送时间的设置将应用到被选中的每一个星期。如图 7.5 所示，防毒墙在工作日的 8 点、12 点和 16 点向用户发送摘要。设置好后，单击【应用】按钮保存。

7.2.2 垃圾邮件摘要主题

单击【垃圾邮件】➔【邮件摘要发送】，进入垃圾邮件摘要主题页面，如图 7.6 所示。

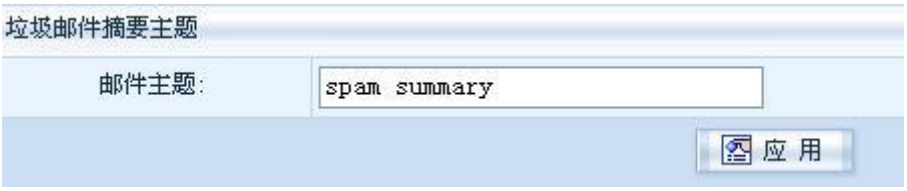


图 7.6 垃圾邮件摘要主题

管理员可以指定防毒墙发送的垃圾邮件摘要的主题，从而方便用户查找确认。填写适当的主题后，单击【应用】按钮，保存设置。

第八章 对象配置

对象是防毒墙管理配置中的一个基本概念，用来描述管理策略中的一个基本元素。瑞星防毒墙中的所有策略都由这些元素组合而成。这些基本元素由以下七个方面构成：

- 地址：设置防毒墙地址对象与实际环境中的客户端一一对应
- 地址组：将防毒墙中的地址对象一个或多个进行组合，构成地址组
- 时间：定义防毒墙策略执行的时间
- 时间组：将防毒墙中的时间对象一个或多个进行组合，构成时间组
- 服务：定义防毒墙服务对象
- 服务组：将防毒墙中的服务对象一个或多个进行组合，构成服务组

8.1 地址

地址对象在防毒墙中可以代表单个地址、一个网段或一段地址。单击【对象配置】➔【地址】进入地址管理页面，如图 8.1 所示。

图 8.1 地址管理

8.1.1 增加地址对象

单击【增加】按钮，进入增加地址页面，如图 8.2 所示。

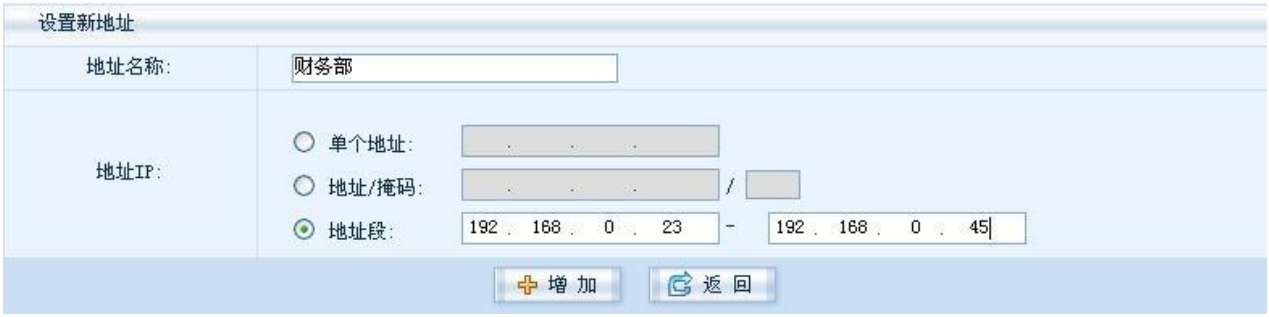


图 8.2 增加地址页面

- 地址名称：用来表示该地址对象的友好名称
- 地址 IP：用户可以用三种方式来定义地址对象代表的内容
  - 增加一个 IP 地址，例如：192.188.0.1
  - 增加一个网段，例如：192.188.0.1/24
  - 增加一段地址，例如：192.188.0.1-192.188.0.2

设置完成后，单击【增加】按钮保存设置，【返回】按钮取消操作。

8.1.2 修改地址对象

如果需要修改某个地址对象，单击该地址对象的图标进入修改地址页面，如图 8.3 所示。

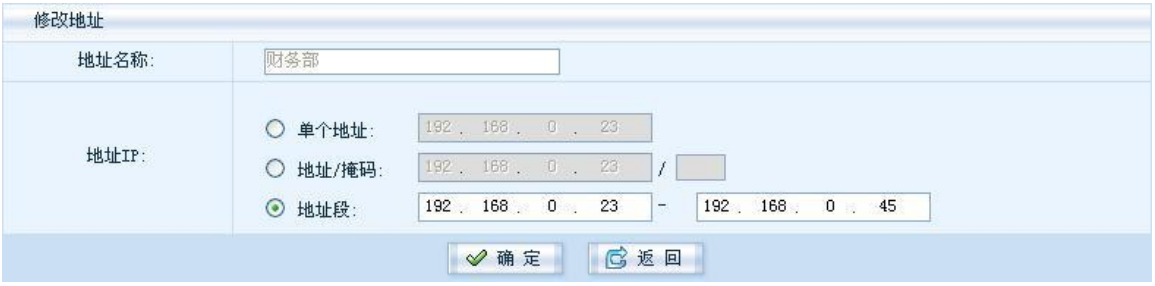


图 8.3 修改地址

修改方式见 8.1.1 增加地址对象中的说明。

8.1.3 删除地址对象

若要删除某个地址对象，在地址管理页面选中相应的地址对象（可以多选），单击【删除】按钮。如果选中最上方的复选框则代表选择全部的地址对象。

8.2 地址组

地址组对象用来统一管理地址对象。当管理员需要对多个地址对象施加同一条策略的时候，可以使用地址组简化管理。单击菜单【对象配置】➔【地址组】进入地址组管理页面，如图 8.4 所示。

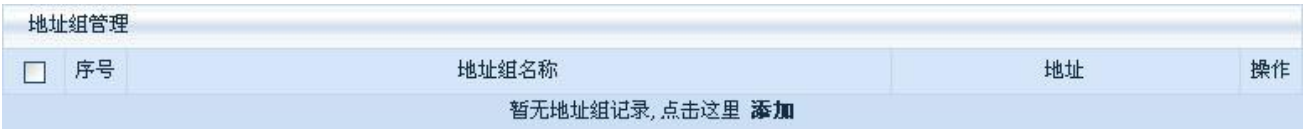


图 8.4 地址组对象

8.2.1 增加地址组对象

单击【增加】按钮进入设置新地址组页面，如图 8.5 所示。

图 8.5 增加地址组

- 地址组名称：用于表示该地址组对象的友好名称
- 可用地址：这里会列出当前防毒墙中所有的地址对象，用户可以选择需要增加的地址对象左边的复选框，把地址对象增加到地址组对象中来

设置好后，单击【增加】按钮进行保存，【返回】按钮取消操作。

8.2.2 修改地址组对象

如果需要修改某个地址组对象，单击该地址组对象的图标进入修改地址组页面，如图 8.6 所示。

图 8.6 修改地址组

修改方式见 8.2.1 增加地址组对象中的说明。

8.2.3 删除地址组对象

若要删除某个地址组对象，在地址组管理页面选择相应的地址组对象（可以多选），单击【删除】按钮。如果选中最上方的复选框则代表选择全部的地址组对象。

8.3 时间

时间对象用来表达和时间有关的概念。用户可以在安全策略的设置中引用这里的时间对象来约束策略的时间范围。单击菜单【对象配置】➔【时间】进入时间对象管理页面，如图 8.7 所示。

图 8.7 时间对象管理

瑞星防毒墙将最常见的工作时间进行预设置，用户可根据自己的需要进行选择、修改和增加来适应本企业的需要。

8.3.1 增加时间对象

单击【增加】按钮，进入自定义时间页面，如图 8.8 所示。

图 8.8 时间对象设置

1. 时间对象名称：用来表示该时间对象的友好名称
2. 时间段：每天的起始和结束时间段
3. 星期：时间段生效的星期范围

设置完成后，单击【确定】按钮保存设置，【返回】按钮取消操作。

8.3.2 修改时间对象

如果需要修改某个时间对象，单击该时间对象的图标进入修改时间对象页面，如图 8.9 所示。

图 8.9 修改时间对象

修改方式见 8.3.1 增加时间对象中的说明。

8.3.3 删除时间对象

若要删除某个时间对象，在时间对象管理页面选择相应的时间对象（可以多选），单击【删除】按钮。如果选中最上方的复选框则代表选择全部的地址组对象。

8.4 时间组

时间组对象用来统一管理时间对象。当管理员需要对多个时间对象施加同一条策略的时候，可以使用时间组简化管理。单击菜单【对象配置】➔【时间组】进入时间组管理页面，如图 8.10 所示。瑞星防毒墙将最常见的工作时间进行预设置，用户可根据自己的需要进行选择、修改和增加来适应本企业的需要。

图 8.10 时间组对象

8.4.1 增加时间组对象

单击【增加】按钮进入设置时间组页面，如图 8.11 所示。

图 8.11 增加时间组

1. 时间组名称：用来表示该时间组对象的友好名称
2. 可用时间对象：这里会列出当前防毒墙中所有的时间对象，用户可以选择需要增加的时间对象左边的复选框，把时间对象增加到时间组对象中来

设置好后，单击【增加】按钮进行保存，【返回】按钮取消操作。

8.4.2 修改时间组

如果需要修改某个时间组对象，单击该时间组对象的 图标进入修改时间组页面进行修改。如图 8.12 所示。

图 8.12 修改时间组

修改方式见 8.4.1 增加时间组对象中的说明。

8.4.3 删除时间组

若要删除某个时间组对象，选中该记录前的复选框进行选择（可以多选），单击【删除】按钮。如果选中最上方的复选框则代表选择全部的时间组对象。

8.5 服务

服务对象用来表达各种不同类型的协议。瑞星防毒墙提供自定义服务设置，这是瑞星防毒墙比较有特色的功能。传统防毒墙一般只提供固定的几种服务，管理员因此只能迁就设备所提供的功能，而即便有些传统防毒墙虽然提供了增加服务的功能，也只能分析 IP、ICMP 等三层以下的通讯协议，对于七层应用程序则无法有效的检测。而网络常会在毫无防备的情况下遭受攻击。另外，传统防毒墙所提供的服务状态检测都是以通讯端口为基础的，且防毒墙不允许用户自定义服务采用的端口号，当服务使用的端口号改变了之后，原有的服务检测就会在自定义规则中失去原本具有的功能。从而给系统带来安全隐患。

针对上述问题，瑞星防毒墙的状态检测功能是完全以服务为基础的，用户可以自定义服务以及服务使用的端口号。并把这些服务应用在安全策略规则中。极大的增加了管理员管理的灵活性，有效的保护了系统安全。单击菜单【对象配置】➔【服务】进入服务管理页面，如图 8.13 所示。瑞星防毒墙将常用的服务进行归纳总结，用户可根据自己的需要进行选择、修改和增加服务对象。

服务管理

	序号	名 称	服务内容	操 作
☐	1	DHCP_Relay	UDP/67	
☐	2	DNS_tcp	TCP/53	
☐	3	DNS_udp	UDP/53	
☐	4	FTP	TCP/21	
☐	5	FTP_data	TCP/20	
☐	6	HTTP	TCP/80	
☐	7	HTTPS	TCP/443	
☐	8	ICMP	ICMP: any	
☐	9	IKE	UDP/500	
☐	10	IMAP	TCP/143	
☐	11	L2TP	TCP/1701	
☐	12	LDAP	TCP/389	
☐	13	MSN	TCP/1863	
☐	14	NTP_tcp	TCP/123	
☐	15	NTP_udp	TCP/123	
☐	16	POP3	TCP/110	
☐	17	PPTP	TCP/1723	
☐	18	QQ_4000	UDP/4000	

图 8.13 防毒墙预定义服务列表

瑞星防毒墙将最常见的服务进行预设置，用户可根据自己的需要进行选择、修改和增加来适应本企业的需要。

8.5.1 增加服务对象

单击【增加】按钮，进入设置新服务对象页面，如图 8.14 所示。

图 8.14 设置新服务对象

- 服务名称：用来表示该服务对象的友好名称
- 协议：服务使用的协议，防毒墙提供了 4 种定义协议的方式
  - ✓ TCP/UDP 对于这两种常用的 3 层协议，用户可以指定协议使用的源端口和目的端口号的范围，如

图 8.15 所示

图 8.15 TCP/UPD 的设置

✓ ICMP 用户可以指定 ICMP 协议的类型域，如图 8.16 所示

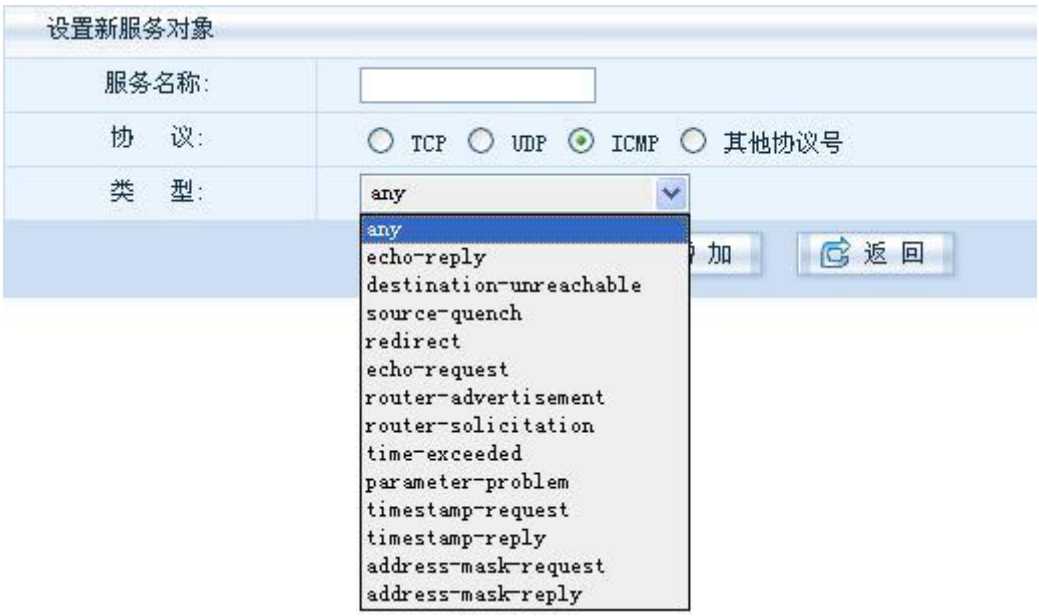


图 8.16 ICMP 的配置

其中：

ICMP 类型	说明
Any	所有的 ICMP 类型
Echo-reply	对 ping 的回应
Destination-unreachable	由主机或路由器返回的消息，一些包不可到达
Source-quench	当数据报在路由的过程中网关没有足够的缓存存放该数据报的时候，网关会丢弃该数据报，并向源地址发送 source-quench 消息
Redirect	当网关 1 在路由表中查到数据报的下一个网关（网关 2）时，如果数据报的源地址和网关 2 属于同一个网段，则网关 1 会向发送数据报的主机发送 redirect 消息，告诉它直接去连接网关 2
Echo-request	通常是我们使用的 ping 命令发送的消息
Router-advertisement	邻机公告
Router-solicitation	邻机请求

Time-exceeded	超时差错报文
Parameter-problem	参数差错报文
Timestamp-request	发送消息的时候使用的时间戳
Timestamp-reply	确认回复的时候使用的时间戳
Address-mask-request	地址掩码请求
Address-mask-reply	地址掩码应答

表 8.1 ICMP 协议的类型域

提示：关于 ICMP

用户可以从 http://www.faqs.org/rfcs/rfc792.html 了解到关于 ICMP 消息类型的详细描述。

- 其他协议号 用户可以通过协议号来定义未在防毒墙上列出的协议，如图 8.17 所示

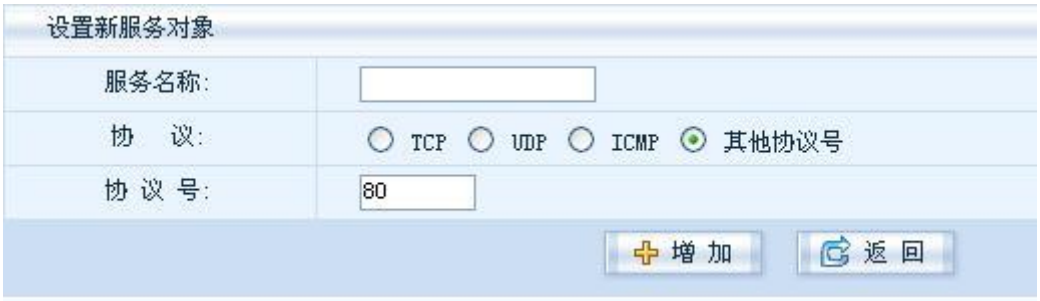


图 8.17 自定义协议号

提示：常用协议号

TCP、UDP、AH 的协议号分别为 6、17 和 51。

设置完成后，单击【确定】按钮保存设置，【返回】按钮取消操作。

8.5.2 修改服务

如果需要修改某个服务对象，单击该对象的 图标进入修改服务对象页面进行修改。如图 8.18 所示。

图 8.18 修改服务对象

修改方式见 8.5.1 增加服务对象中的说明。

8.5.3 删除服务

若要删除某个服务对象，选中该记录前的复选框进行选择（可以多选），单击【删除】按钮。如果选中最上方的复选框则代表选择全部的服务对象。

8.6 服务组

服务组对象用来统一管理服务对象。当管理员需要把多个服务对象应用于一条策略的时候，可以使用服务组简化管理。单击菜单【对象配置】➔【服务组】进入服务组管理页面，如图 8.19 所示。

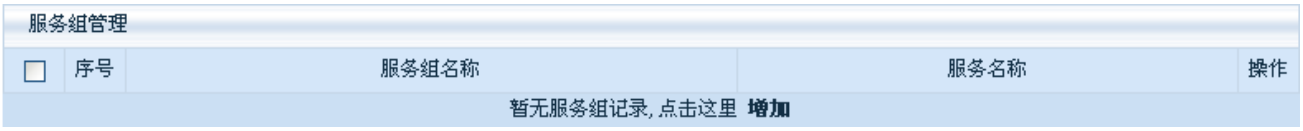


图 8.19 服务组对象

8.6.1 增加服务组

单击【增加】按钮进入页面，如图 8.20 所示。

图 8.20 增加服务组

1. 服务组名称：用来表示该服务组对象的友好名称
2. 可用服务：这里会列出当前防毒墙中所有的服务对象，用户可以选择需要增加的服务对象左边的复选框，把服务对象增加到服务组对象中来

设置好后，单击【增加】按钮进行保存，【返回】按钮取消操作。

8.6.2 修改服务组

如果需要修改某个服务组对象，单击该服务组对象的图标进入修改服务组页面进行修改。如图 8.21 所示。

图 8.21 修改服务组

修改方式见 8.6.1 增加服务组中的说明。

8.6.3 删除服务组

若要删除某个服务组对象，选中该记录前的复选框进行选择（可以多选），单击【删除】按钮。如果选中最上方的复选框则代表选择全部的服务组对象。

第九章 应用协议

传统防火墙只能对应用程序进行包过滤，当被控制的客户端增加代理或实施一些欺骗行为时，防火墙就不能有效的进行控制。瑞星通过多年对网络安全的深入研究，通过对常用应用协议的分析，利用防毒墙有效对协议进行识别并实施阻断。

- 自动识别：对选择的协议自动识别
- 预定义：列出一些常见协议所使用的默认通讯端口，可根据实际需求自行增加
- 识别结果：记录防毒墙的协议识别结果

9.1 自动识别

如果防毒墙没有识别出传输的数据使用的协议，会自动对以下选中的协议做自动识别。如果想让防毒墙自动识别某些协议，则在这里选中它们。如图 9.1 所示。

图 9.1 应用协议自识别配置

选中相应的协议后，单击【应用】按钮保存设置。

类别	协议	说明
通用协议	FTP	文件传输协议
	HTTP	超文本传输协议
	IMAP	一种在服务器上管理邮件的协议
	POP3	一种从服务器上收取邮件的协议
	SMTP	简单邮件传输协议。
	SOCKS5	一种代理协议
多媒体协议	H323	由国际电信联盟（ITU-T）制定的协议族，大部分网络会议软件和网

		络电话软件均使用该协议
	RTSP	由 RealNetworks 和 Netscape 共同提出的，该协议定义了一对多应用程序如何有效地通过 IP 网络传送多媒体数据
IM 协议	Jabber/g-talk	g-talk 使用的通讯协议
	MSN 文件传输协议	MSN 传输文件时使用的协议
	MSN 协议	MSN 的通讯协议
	QQ	QQ 使用的协议
	Skype to phone	Skype 电话使用的协议
	Skype	Skype IM 通讯协议
	Yahoo	Yahoo 通使用的协议
远程控制协议	vnc	帮助内网的 2 台计算机透明通信使用的协议
P2P 协议	BT	BT 使用的协议
	Edonkey/ Emule	Emule 使用的协议
	迅雷	迅雷使用的协议
股票软件	大智慧	大智慧使用的协议
	大智慧新一代	大智慧新一代使用的协议
	盘口王	盘口王使用的协议
	钱龙金典版	钱龙金典版使用的协议
	钱龙旗舰版	钱龙旗舰版使用的协议
	通达信	通达信使用的协议
	同花顺	同花顺使用的协议
	证券之星	证券之星使用的协议
网络游戏	边锋网络游戏	边锋网络游戏使用的协议
	传奇世界	传奇世界使用的协议
	浩方对战平台	浩方对战平台使用的协议
	联众游戏	联众游戏使用的协议
	热血传奇	热血传奇使用的协议

表 9.1 瑞星防毒墙可以自动匹配的协议

9.2 预定义

防毒墙将 HTTP、FTP、POP3、SMTP、MSN、IMAP 协议默认使用端口写入应用协议规则中，供用户直接使用，但有些站点或服务器使用一些特殊的端口进行数据传输，为了能够识别这些使用标准协议而非标准端口的协议，瑞星防毒墙提供用户自定义设置，单击菜单【应用协议】➔【预定义】进入应用预定义配置页面，如图 9.2 所示。

图 9.2 防毒墙应用预定义配置页面

9.2.1 增加应用协议规则

在应用预定义配置页面单击【增加】按钮，如图 9.3 所示。

图 9.3 增加预定义规则

1. 在协议名称处选择需要增加的协议，如图 9.4 所示

图 9.4 预定义协议选项

2. 在服务 IP 输入进行检查的 IP 地址，如果不确定 IP 地址，可选择“Any”选项，代表对所有地址都进行检查

3. 在协议处选择通过 TCP 或 UDP 进行数据传输

4. 输入该协议的端口

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条应用协议预定义规则后，该记录会在主页面上显示出来，如图 9.5 所示。

应用预定义配置

序号	应用协议名	服务器IP	协议	端口	操作	移动
1	HTTP	Any	tcp	80	-	
2	FTP	Any	tcp	21	-	
3	POP3	Any	tcp	110	-	
4	SMTP	Any	tcp	25	-	
5	MSN协议	Any	tcp	1863	-	
6	IMAP	Any	tcp	143	-	
7	FTP	Any	tcp	23		

增 加 删 除

图 9.5 防毒墙应用预定义配置列表

9.2.2 移动应用协议规则顺序

瑞星防毒墙应用协议规则是有顺序性的，所以为了达到良好的效能，适时的调整规则的次序是必要的。如果要调整已定义的规则顺序，只要单击该规则移动栏内“”图标，即可进入顺序修改状态，如图 9.6 所示。单击第三条规则的操作按钮，选择要移动到的位置序号，即可移动该规则的顺序。

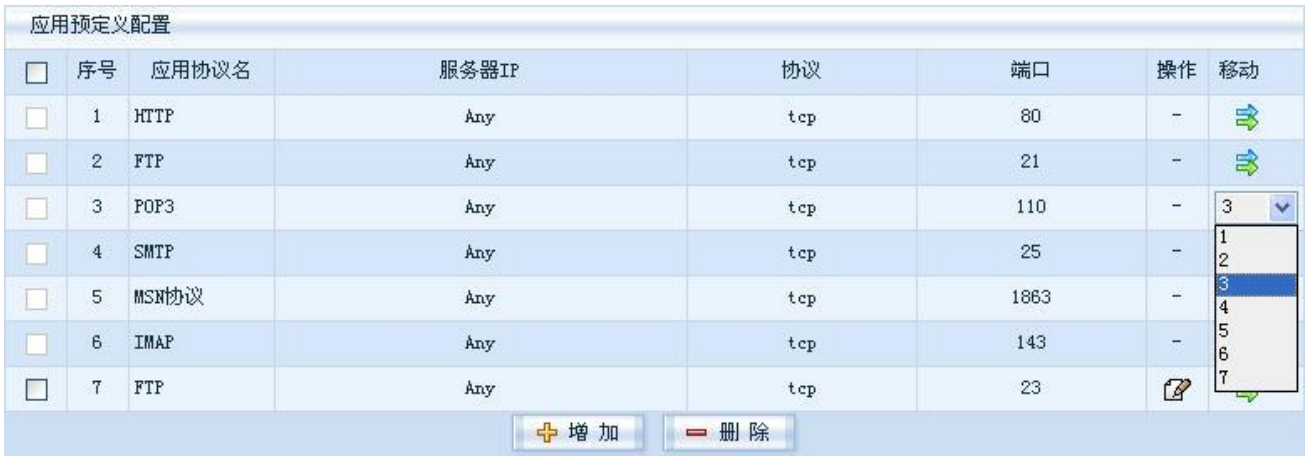


图 9.6 移动应用预定义协议顺序

9.2.3 修改应用协议规则

HTTP、FTP、POP3、SMTP、MSN、IMAP 协议默认使用端口是不允许用户更改的，用户只能够修改自定义增加的应用协议规则。单击应用协议列表中某记录的图标，进入预定义规则修改页面，如图 9.7 所示。

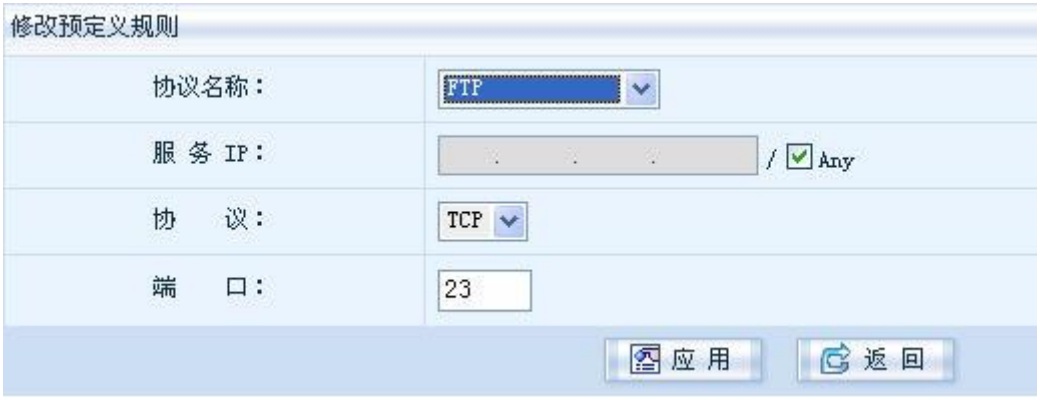


图 9.7 修改应用协议规则

关于应用协议规则修改操作请参阅本文档 9.2.1 增加应用协议规则部分内容。

9.2.4 删除应用协议规则

选中某条应用协议规则记录，单击【删除】按钮，则删除该条应用协议规则。

9.3 识别结果

防毒墙将管理员选择识别协议的识别结果分类显示，如图 9.8 所示。

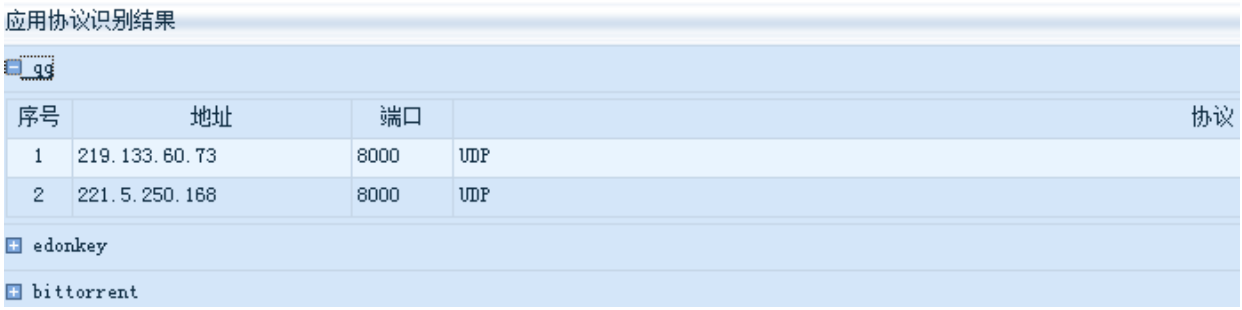


图 9.8 应用协议识别结果

图 9.8 各字段说明

字段	说明
应用协议	识别结果按照应用协议进行分类，单击协议名称展开详细信息，再次单击收起。
序号	按照阿拉伯数字排序
地址	该应用协议连接的ip地址
端口	该应用协议所使用的端口
协议	该应用协议进行数据传输时使用的协议

表 9.2 应用协议识别结果说明

第十章 防火墙

本章从以下九个方面介绍防毒墙的安全策略：

- 安全策略编辑：设置防火墙安全策略
- 内容过滤规则：定义防毒墙内容过滤策略，包含：病毒过滤和垃圾邮件过滤
- URL 过滤配置：进行防毒墙 URL 过滤设置
- URL 攻击防御：配置防毒墙对内部服务器实施保护
- 入侵防御：进行防毒墙入侵防御设置
- IP 黑名单：对一些经常制造网络威胁的地址进行过滤
- 安全策略分析：对已经建立的安全策略进行分析
- 连接信息管理：查看通过防毒墙建立的连接信息
- MAC 地址管理：管理防毒墙下客户端的 MAC 与 IP 地址的关联

防毒墙安全策略的主要功能是检验所有通过防毒墙的数据，根据制定的防毒墙规则判定数据通过还是丢弃，防止未经允许数据通过防毒墙。防毒墙可以检查任何接口进入的所有数据，不但如此，还可以根据规则的定义进行数据的流向检查。例如，通过接口的数据传输可分二个方向，一个是由因特网流向企业内部网络，另一个是由企业内部送往因特网。因此，管理员必需在设置防毒墙时指定防毒策略规则。图 10.1 是防毒墙的入侵防范示意图。

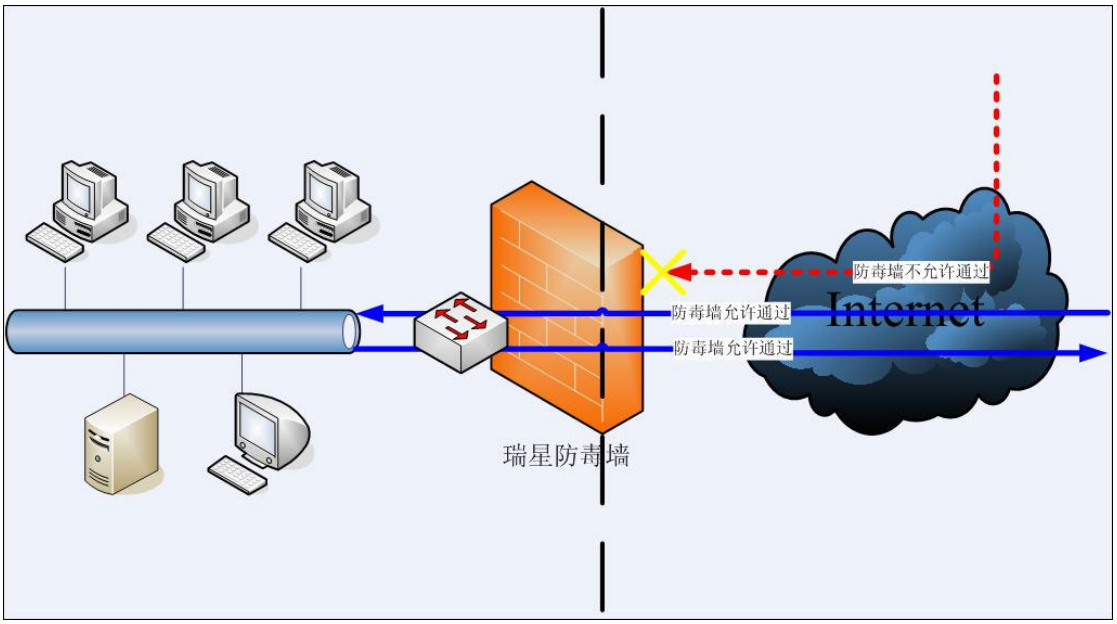


图 10.1 防毒墙的入侵防范示意图

瑞星防毒墙默认的规则允许所有网络连接，默认对进入 E1 接口的数据进行杀毒。如果需要高安全的通讯模式，可以通过增加防毒规则来满足企业的需要。

10.1 安全策略编辑

瑞星防毒墙集成了防火墙功能，对请求建立连接的数据包进行检查，如果符合策略要求才可建立连接，否则予以丢弃，大大提高了网络的安全性。单击【防火墙】➔【安全策略编辑】，进入安全策略编辑页面，如图 10.2 所示。

图 10.2 安全策略编辑页面

10.1.1 增加安全策略

在安全策略编辑页面，单击【增加】进入增加新策略页面，如图 10.3 所示。

图 10.3 增加新安全策略

1. 策略名处输入唯一的策略名称，方便管理员进行识别
2. 在方向处选择数据流的入口和出口
3. 在源地址处选择地址类型和内容，此部分内容参阅 8.1 地址和 8.2 地址组的设置。也可选择自定义地址类型，手工输入地址、地址区间、网段和 MAC 地址，输入格式参阅表 10.1

类型	格式
地址	192.168.0.1
地址区间	192.168.0.1-192.168.0.3
网段	192.168.1.0/24
MAC 地址	AA：AA：AA：AA：AA：AA

表 10.1 自定义地址输入格式

4. 在目的地址处选择地址类型和内容，此部分内容参阅 8.1 地址和 8.2 地址组的设置。也可选择自定义地址，手工输入地址、地址区间、网段，输入格式参阅表 10.1

5. 在服务处选择服务类型和内容，此部分内容参阅 8.5 服务和 8.6 服务组的设置。也可选择自定义服务，手工输入协议的源端口和目的端口号、其他协议号输入格式参阅表 10.2

类型	格式
TCP 源端口和目的端口	tcp:1-135 1-135
UDP 源端口和目的端口	udp:1-135 1-135
ICMP	icmp:any
其他协议号	other:51

表 10.2 自定义服务的输入格式

6. 在时间处选择时间类型和内容，此部分内容参阅 8.3 时间和 8.4 时间组的设置。也可选择自定义时间，手工输入时间范围输入格式参阅表 10.3

类型	格式
时间 星期	12：00-13：00 Mon，Tue

表 10.3 自定义时间输入格式

7. 在策略处选择允许或拒绝。允许为允许此策略建立连接；拒绝为拒绝此策略建立连接

8. 进行日志记录则在日志处勾选【启用记录】单选按钮，如果不进行日志记录则不勾选此按钮

9. 单击增加新策略页面的【高级选项】按钮，如图 10.4 所示

图 10.4 安全策略应用协议选项

10. 勾选需要进行检查的协议，有关此部分内容请参阅应用协议部分

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条安全

策略后，安全策略记录会在主页面上显示出来，如图 10.5 所示。

图 10.5 防毒墙安全策略

图 10.5 上各字段的说明如下：

字段	说明
序号	按照阿拉伯数字排序，数字越小说明策略优先级越高
状态	代表该策略是否开启。绿色图标表示开启，红色图标表示停用状态。管理员可启用或停用规则
策略名	策略的代表名称。管理员自定义策略名称以方便管理
入口	所有进入此策略的数据流
出口	所有流出此策略的数据流
源地址	定义该策略的数据来源地址
目的地址	定义该策略的数据目标地址
时间	定义该策略适用时间
服务	该策略要检查何种服务内容
策略	定义该策略的行为模式。在防毒墙策略上共有两种行为模式：允许或拒绝。绿色图标表示允许，红色图标为拒绝
日志	显示该策略下是否启用日志记录。绿色对勾图标表示启用日志记录状态。红色的图标表示不进行日志记录
高级	所启用的高级选项中的应用协议
操作	单击进入设置页面
移动	移动调整定义的策略规则顺序
设为启用	如果要启用某个被停用的策略，选中该策略前的复选框单击【设为启用】，则该策略被启用并开始过滤
设为停用	如果要停用某个被启用的策略，选中该策略前的复选框单击【设为停用】，则该策略被停用并停止过滤

表 10.4 安全策略名词解释

10.1.2 移动安全策略顺序

瑞星防毒墙安全策略是有顺序性的，所以为了达到良好的效能，适时的调整策略的次序是必要的。如果要调整已定义的策略顺序，只要单击该策略移动栏内“”图标，即可进入顺序修改状态，如图 10.6 所示。单击第二条策略的操作按钮，选择要移动到的位置序号，即可移动该策略的顺序。

图 10.6 移动防毒墙安全策略

10.1.3 修改安全策略

单击安全策略记录的图标，进入安全策略修改页面，如图 10.7 所示。

图 10.7 修改安全策略页面

1. 在方向处选择数据流的入口和出口

2. 在源地址处选择地址类型和内容，此部分内容参阅 8.1 地址和 8.2 地址组的设置。也可选择自定义地址类型，手工输入地址、地址区间、网段和 MAC 地址，输入格式参阅表 10.1

3. 在目的地址处选择地址类型和内容，此部分内容参阅 8.1 地址和 8.2 地址组的设置。也可选择自定义地址，手工输入地址、地址区间、网段，输入格式参阅表 10.1

4. 在服务处选择服务类型和内容，此部分内容参阅 8.5 服务和 8.6 服务组的设置。也可选择自定义服务，手工输入协议的源端口和目的端口号、其他协议号输入格式参阅表 10.2

5. 在时间处选择时间类型和内容，此部分内容参阅 8.3 时间和 8.4 时间组的设置。也可选择自定义时间，手工输入时间范围输入格式参阅表 10.3

6. 在策略处选择允许或拒绝

7. 是否启用日志记录

8. 单击修改策略页面的【高级选项】按钮，勾选需要进行检查的协议

9. 单击【确定】按钮确认修改，【返回】按钮取消修改

10.1.4 删除安全策略

选中某条安全策略记录，单击【删除】按钮，则删除该条安全策略。

10.2 内容过滤规则

通过设置内容过滤规则，才可进行病毒查杀和垃圾邮件过滤。单击【防火墙】➔【内容过滤规则】，进入内容过滤规则编辑页面，如图 10.8 所示。

图 10.8 过滤规则编辑页面

10.2.1 增加内容过滤规则

在过滤规则编辑页面单击【增加】，进入增加新规则页面，如图 10.9 所示。

图 10.9 增加内容过滤规则

1. 在规则名处输入唯一的规则名称，方便管理员进行识别

2. 在入口处选择此策略的数据流入口

3. 在源地址处选择地址类型和内容，此部分内容参阅 8.1 地址和 8.2 地址组的设置。也可选择自定义地址类型，手工输入地址、地址区间、网段和 MAC 地址，输入格式参阅表 10.1

4. 在目的地址处选择地址类型和内容，此部分内容参阅 8.1 地址和 8.2 地址组的设置。也可选择自定义地址类型，手工输入地址、地址区间、网段，输入格式参阅表 10.1

5. 在服务处勾选需要进行过滤的服务，默认设置为自动识别这些服务。如果某个协议采用特殊

的端口号，请选中该协议的自定义选项，输入所采用的特殊端口号（如需输入多个端口，请以逗号分隔），如图 10.10 所示

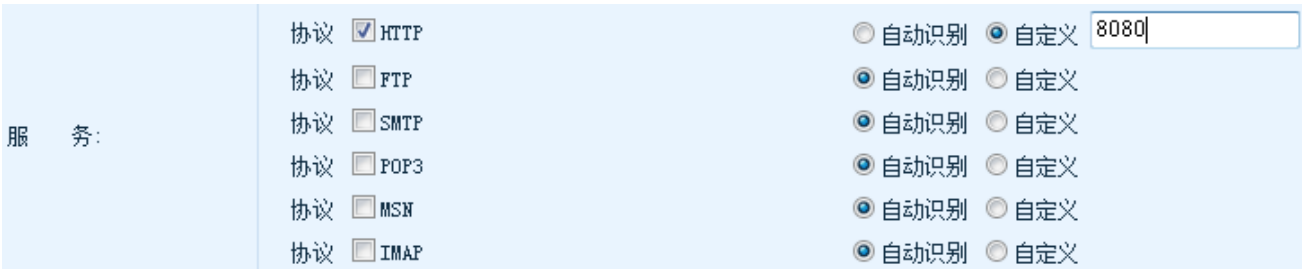


图 10.10 自定义协议端口号

6. 在策略处选择是否进行过滤

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条内容过滤规则后，内容过滤规则记录会在主页面上显示出来。如图 10.11 所示。

图 10.11 内容过滤规则

图 10.11 上文字说明

字段	说明
序号	按照阿拉伯数字排序，数字越小说明策略优先级越高
状态	代表该策略是否开启。绿色图标表示开启，红色图标表示停用状态。管理员可启用或停用规则
规则名	规则的代表名称
入口	所有进入此策略的数据流
源地址	定义该策略的数据来源地址
目的地址	定义该策略的数据目标地址
服务	该策略要检查何种服务内容
过滤	定义该规则的行为模式。防毒墙内容过滤共有两种行为模式：过滤或不过滤。绿色图标表示过滤，红色图标为不过滤
操作	单击进入修改过滤规则页面
移动	移动调整定义的策略规则顺序
设为启用	如果要启用某个被停用的规则，选中该规则前的复选框单击【设为启用】，则该规则被启用并开始过滤
设为停用	如果要停用某个被启用的规则，选中该规则前的复选框单击【设为停用】，则该规则被停用并停止过滤

表 10.5 内容过滤规则说明

10.2.2 移动内容过滤规则顺序

瑞星防毒墙内容过滤规则是有顺序性的，所以为了达到良好的效能，适时的调整规则的次序是必要的。如果要调整已定义的规则顺序，只要单击该规则移动栏内“”图标，即可进入顺序修改状态，如图 10.12 所示。单击第二条规则的操作按钮，选择要移动到的位置序号，即可移动该规则的顺序。

图 10.12 移动防毒墙内容过滤规则顺序

10.2.3 修改内容过滤规则

单击内容过滤规则记录的图标，进入内容过滤规则修改页面，如图 10.13 所示。

图 10.13 修改内容过滤规则

1. 在入口处修改此策略的数据流入口

2. 在源地址处修改地址类型和内容，此部分内容参阅 8.1 地址和 8.2 地址组的设置。也可选择自定义地址类型，手工输入地址、地址区间、网段和 MAC 地址，输入格式参阅表 10.1

3. 在目的地址处修改地址类型和内容，此部分内容参阅 8.1 地址和 8.2 地址组的设置。也可选

择自定义地址类型，手工输入地址、地址区间、网段，输入格式参阅表 10.1

4. 在服务处勾选需要进行过滤的服务，默认设置为自动识别这些服务。如果某个协议采用特殊的端口号，请选中该协议的自定义选项，输入所采用的特殊端口号（如需输入多个端口，请以逗号分隔）

5. 在策略处选择是否进行过滤

6. 单击【确定】按钮确认修改，【返回】按钮取消修改

10.2.4 删除内容过滤规则

选中某条内容过滤规则记录，单击【删除】按钮，则删除该条内容过滤规则。

10.3 URL 过滤配置

URL 过滤功能可以阻止用户访问非法、色情和工作无关的站点，控制网络资源的使用和提高网络性能。管理员可根据需要进行配置，过滤有害的网站和控制下载内容。单击【防火墙】➔【URL 过滤配置】进入 URL 过滤页面，如图 10.14 所示。

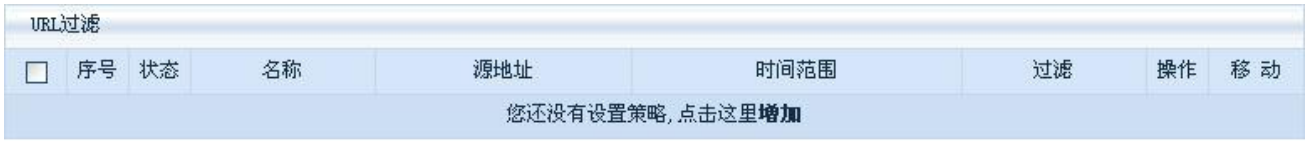


图 10.14 防毒墙 URL 过滤列表

10.3.1 增加 URL 过滤规则

单击【增加】，进入增加新策略页面，如图 10.15 所示。

图 10.15 增加 URL 过滤策略

1. 在策略名处输入 URL 过滤策略的名称

2. 在源地址处修改地址类型和内容，此部分内容参阅 8.1 地址和 8.2 地址组的设置。也可选择自定义地址类型，手工输入地址、地址区间、网段和 MAC 地址，输入格式参阅表 10.1

3. 在时间处选择时间类型和内容，此部分内容参阅 8.3 时间和 8.4 时间组的设置。也可选择自定义时间，手工输入时间范围输入格式参阅表 10.3

4. 选择过滤的类型并输入过滤内容

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条 URL 过滤规则后，URL 过滤规则记录会在主页面上显示出来。如图 10.16 所示。

图 10.16 URL 过滤规则列表

图 10.16 各字段文字说明

字段	说明
序号	按照阿拉伯数字排序，数字越小说明规则优先级越高。
状态	代表该过滤规则是否开启。绿色图标表示开启，红色图标表示停用状态。管理员可启用或停用规则
名称	规则的代表名称。管理员自定义规则名称以方便管理
时间范围	该规则在什么时间段生效
源地址	定义该规则的数据来源地址
过滤	进行过滤的网站名、网站地址或文件类型
操作	单击进入修改过滤规则页面
移动	移动规则排列顺序
设为启用	如果要启用某个被停用的规则，选中该规则前的复选框单击【设为启用】，则该规则被启用并开始过滤
设为停用	如果要停用某个被启用的规则，选中该规则前的复选框单击【设为停用】，则该规则被停用并停止过滤

表 10.6 URL 过滤规则列表名词解释

10.3.2 修改 URL 过滤规则

单击 URL 过滤规则记录的图标，进入 URL 过滤规则修改页面，如图 10.17 所示。

图 10.17 修改 URL 过滤策略

1. 在源地址处修改地址类型和内容
2. 在时间处修改时间的类型和内容
3. 修改过滤的类型并输入过滤内容
4. 单击【确定】按钮确认修改，【返回】按钮取消修改

10.3.3 删除 URL 过滤规则

选中某条 URL 过滤规则记录，单击【删除】按钮，则删除该条 URL 过滤规则。

10.4 URL 攻击防御

企业服务器常常因网络攻击而不能够正常提供服务，利用防毒墙 URL 攻击防御功能，可以对企业服务器提供全方位的保护。单击【防火墙】➔【URL 攻击防御】，进入防毒墙 URL 攻击防御配置页面，如图 10.18 所示。

图 10.18 URL 攻击防御列表

10.4.1 增加 URL 攻击防御规则

单击【增加】，进入增加 URL 攻击防御页面，如图 10.19 所示。

图 10.19 增加 URL 攻击规则

1. 在服务器 IP 处填写提供对外服务的服务器 IP 地址
2. 输入服务器的 URL 地址
3. 输入统计时间，防毒墙以统计时间为周期进行访问统计
4. 输入在统计时间周期内允许的访问次数。如果在统计周期内超出允许的访问次数，则连接被阻断
5. 在阻断时间栏填写阻断连接的时间

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条 URL 攻击防御规则后，URL 攻击防御规则记录会在主页面上显示出来。如图 10.20 所示。

图 10.20 URL 攻击防御列表

设为启用：如果要开启某个被停用的规则，选中该规则前的复选框单击【设为启用】，则该规则被启用。

设为停用：选中该规则前的复选框单击【设为停用】，则停止该规则。

10.4.2 修改 URL 攻击防御规则

单击 URL 防御规则记录的图标，进入 URL 攻击防御规则修改页面，如图 10.21 所示。

图 10.21 URL 攻击防御规则修改页面

1. 在服务器 IP 处修改提供对外服务的服务器 IP 地址
2. 修改服务器的 URL 地址
3. 修改统计时间
4. 修改在统计时间内允许的访问次数
5. 修改阻断时间

单击【确定】完成修改，单击 【返回】取消修改

10.4.3 删除 URL 攻击防御规则

选中某条 URL 防御规则记录，单击【删除】按钮，则删除该条 URL 防御规则。

10.5 入侵防御

把已经发现计算机系统漏洞和常见的入侵手段加入防毒墙安全策略规则中，通过应用这些规则，帮助管理员快速抵御来自互联网的恶意入侵。当外部试图与企业内部某个工作站建立连接时，防毒墙首先进行入侵防御规则匹配，发现符合入侵防御规则设置后，立即阻断连接，达到保护用户网络的目的。防毒墙将这些入侵防御手段进行分类，以便管理员进行管理。单击【防火墙】➔【入侵防御】，进入入侵防御设置页面，如图 10.22 所示。

图 10.22 防毒墙入侵防御规则

提示：瑞星防毒墙默认不启用这些策略，管理员可根据实际情况有选择性的启用这些策略。随着入侵手段和系统漏洞的不断增加，瑞星防毒墙也会在随后的升级版本中陆续增加这些策略。

10.5.1 启用入侵防御规则

我们以启用蠕虫类的入侵防御规则举例：

1. 单击蠕虫类，如图 10.23 所示

图 10.23 蠕虫入侵防御规则列表

2. 勾选蠕虫类列表下规则记录前的复选框（可多选），也可选择最上面的复选框，选中所有蠕虫类下的入侵防御规则，如图 10.24 所示

蠕虫类

	序号	状态	内容
☑	1		MswinRPCdcom溢出漏洞ms03-026此漏洞是冲击波/冲击波杀手/高波/sdbot等病毒传播的途径之一
☑	2		MsLSA服务RPC远程缓冲区溢出漏洞MS04011震荡波等病毒利用此漏洞进行传播
☑	3		MSIE的iFrame系统溢出漏洞此漏洞会做为求职信/坏透了/尼姆达等病毒传播的途径之一
☑	4		apache-worm
☑	5		sql-worm
☑	6		MscanWorm.sanftp
☑	7		MscanWorm.CheckSTATUS

图 10.24 选择蠕虫类入侵防御规则

3. 单击【设为启用】，弹出确认操作对话框，如图 10.25 所示

图 10.25 启用指定的策略

4. 单击【确定】启用这些策略，单击【取消】放弃启用这些策略。

5. 单击【确定】后，系统返回策略执行成功提示，单击【确定】，则这些策略被启用，如图 10.26 所示。

蠕虫类

	序号	状态	内容
☐	1		MswinRPCdcom溢出漏洞ms03-026此漏洞是冲击波/冲击波杀手/高波/sdbot等病毒传播的途径之一
☐	2		MsLSA服务RPC远程缓冲区溢出漏洞MS04011震荡波等病毒利用此漏洞进行传播
☐	3		MSIE的iFrame系统溢出漏洞此漏洞会做为求职信/坏透了/尼姆达等病毒传播的途径之一
☐	4		apache-worm
☐	5		sql-worm
☐	6		MscanWorm.sanftp
☐	7		MscanWorm.CheckSTATUS

图 10.26 蠕虫入侵防御规则启用状态

10.5.2 停用入侵防御策略

勾选需要停用的入侵防御策略规则，单击【设为停用】。

10.5.3 自定义入侵防御规则

瑞星防毒墙入侵防御规则针对目前已知的漏洞和流行的入侵手段能够积极地做出响应，当一个新的漏洞和入侵手段出现时，由于防毒墙入侵防御策略中没有相应的记录会导致该功能失效。为了能让防毒墙在网络出现问题时第一时间做出响应，网络管理员可以通过添加自定义规则快速阻断发现的漏洞攻击等等。单击【防火墙】➔【入侵防御】，进入入侵防御设置页面，如图 10.27 所示。

图 10.27 防毒墙入侵防御规则

- 增加自定义入侵防御规则

单击【增加】按钮增加自定义入侵防御规则，如图 10.28 所示

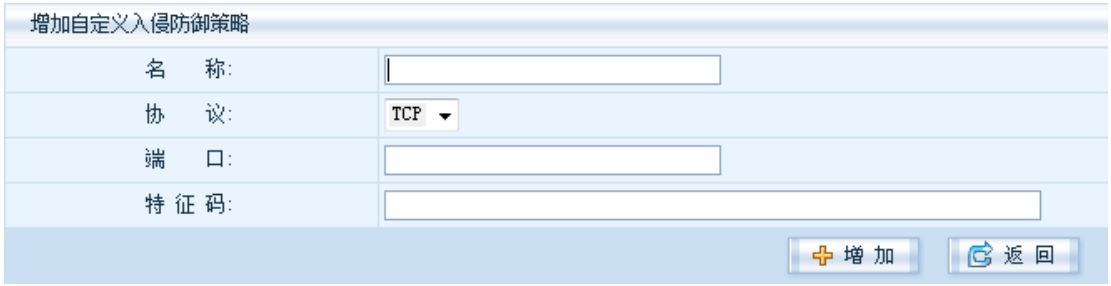


图 10.28 增加自定义入侵防御规则

1. 在名称处输入该规则的友好名称
2. 选择协议
3. 输入进行传输的端口，如果输入多个端口请用逗号分隔
4. 输入该漏洞或入侵手段的特征码

单击【增加】完成入侵防御策略，单击【返回】放弃增加策略。如图 10.29 所示。

图 10.29 入侵防御规则自定义类列表

- 删除自定义入侵防御规则

  勾选需要删除的自定义入侵防御策略规则，单击【删除】按钮进行删除；如需删除单个策略请单击该策略同一行的图标。

- 修改自定义入侵防御规则

  如需修改自定义入侵防御规则，请单击该策略同一行的图标进入修改页面，如图 10.30 所示。

图 10.30 修改自定义入侵防御规则

1. 输入修改的协议
2. 输入修改的端口，如果输入多个端口请用逗号分隔
3. 输入修改的特征码

单击【确定】完成修改，单击【返回】放弃修改。

10.6 IP 黑名单

瑞星防毒墙支持 IP 地址黑名单功能，将一些恶意 IP 地址或 IP 地址段加入到黑名单中，当这些地址试图进行网络连接时，防毒墙会自动拒绝这些连接。单击【防火墙】➔【IP 黑名单】，进入 IP 黑名单页面，如图 10.31 所示。

图 10.31 IP 黑名单列表

单击【增加】，增加一个 IP 黑名单地址，如图 10.32 所示。

图 10.32 增加 IP 黑名单地址

输入已经确认是恶意 IP 的地址或地址段，单击【增加】保存设置，单击【返回】取消操作。单个地址格式为“1.1.1.1”；地址段格式为“1.1.1.0/24”。分别增加以上两个 IP 地址，则 IP 黑名单列表如图 10.33

所示。

图 10.33 IP 地址黑名单列表

如果要删除 IP 黑名单记录，请勾选该条记录前的复选框，单击【删除】按钮。

10.7 安全策略分析

当企业内部存在多条安全策略记录时，通过安全策略分析功能进行安全策略的查找，单击【防火墙】➔【安全策略分析】，进入安全策略分析页面，如图 10.34 所示。

图 10.34 安全策略分析页面

输入查询条件：

1. 在方向处选择入口和出口
2. 选择源地址
3. 选择目的地址
4. 选择服务
5. 选择时间，如图 10.35 所示

图 10.35 查询条件

6. 单击【搜索】进行查询，如图 10.36 所示

图 10.36 安全策略查询结果

提示：也可选择方向、源地址、目的地址、服务和时间的某一条件进行模糊查询。

10.8 连接信息管理

防毒墙连接信息显示了当前系统连接的状态信息，您也可输入条件对连接信息进行查询。单击【防火墙】➔【连接信息管理】，查看已经与防毒墙建立连接客户端的详细信息，如图 10.37 所示。

图 10.37 连接信息

输入搜索条件：

1. 输入源地址和目的地址
2. 在协议处选择进行查询的协议
3. 输入端口范围
4. 输入上传包/下载包的范围
5. 输入空闲时间
6. 选择连接状态
7. 在统计条件处选择是否显示防毒墙请求的连接和合并源 IP、目的 IP、目的端口、协议相同的连接
8. 单击统计控制处的【开始统计】将开始连接信息的统计。如果想重新进行统计，请再次单击统计控制处的【开始统计】按钮
9. 选择查看详细记录结果
10. 选择查看统计结果，并使用连接数、上传字节或下载字节进行排序
11. 单击【搜索】

提示：也可输入上述条件的某一条或几条进行模糊查询。必须进行统计后才能够进行查询。

图 10.37 连接信息各字段文字说明

字段	说明
序号	按照阿拉伯数字排序连接信息
协议	采用何种协议进行通信
源地址	连接的来源IP地址
目的地址	连接的目的IP地址
端口对	源地址通过防毒墙连接目的地址所使用的端口映射，*代表任意端口
上传字节数/包	从源地址流向目的地址的字节数
下载字节数/包	从目的地址流向源地址的字节数
连接数	当前建立的连接的数量
在线时间	从建立连接后一共运行了多长时间
空闲时间	建立连接后该连接的空闲时间

表 10.7 防毒墙连接帮助信息

10.9 MAC 地址管理

单击【防火墙】➔【MAC 地址管理】，该页面显示目前系统在本地局域网内使用的 IP 地址与 MAC 物理地址的对应暂存表和绑定状态，如图 10.38 所示。

图 10.38 MAC 地址管理

MAC 绑定：分为自动绑定和手动绑定。

- 自动绑定，填写 IP 地址和子网掩码，单击【执行绑定】，防毒墙会自动将 IP 地址和使用该 IP

地址的计算机实际 MAC 地址进行绑定。

- 手动绑定，自行输入 IP 地址和 MAC 地址信息，单击【执行绑定】进行绑定。

MAC 信息列表：显示绑定的以及没有绑定的 IP 地址和 MAC 地址对应表。

字段	说明
序号	按照阿拉伯数字排序
名称	为唯一MAC地址关联到用户，可在操作下单击  图标进行设置
MAC	网卡物理地址（MAC）。
IP	IP地址
接口	该IP地址连接到的防毒墙的接口，分为：E0、E1、E2和E3
状态	显示该MAC是否与IP地址绑定，显示“yes”表示绑定，“no”为未绑定。
冲突	该IP地址是否在网络上被其他用户使用，如果冲突的话计数冲突次数，并在检测下提示
检测	分为“新增”、“修改”和“冲突”，新增为防毒墙刚刚检测到该计算机的MAC和IP地址信息；修改为拥有该MAC地址的计算机所使用IP地址被修改过；冲突为拥有该MAC地址的计算机所使用的IP地址被其他用户尝试使用过，引起冲突
相关IP	如果该MAC的IP地址被修改或在网络上有冲突，会在此处显示修改的IP地址或引起冲突的IP地址
次数	IP地址修改的次数
时间	对MAC管理进行操作的时间
操作	对于列表中没有绑定的IP地址，可以单击  图标进行绑定，绑定后该地址状态变为“yes”。如果需要撤销绑定，选择该地址记录单击  图标撤销绑定，撤销绑定后该地址状态变为“no”
撤销绑定	选择MAC地址管理列表中的记录，单击  进行批量撤销MAC地址绑定
删除	选择MAC地址管理列表中的记录，单击  进行批量删除MAC地址绑定记录
刷新	单击  刷新当前MAC地址列表
导出	单击  导出当前MAC地址列表到本地计算机
导入	单击  导入之前备份的MAC地址列表

表 10.8 MAC 管理名词解释

第十一章 地址转换

本章我们从两个方面了解防毒墙的地址转换：

- 源地址转换：将企业内部的多个地址转换成合法的公网地址
- 目的地址转换：将目标地址转换成真实的子网地址或内部服务器地址

NAT（Network Address Translation），可译为网络地址转换。随着互联网日益壮大，IP V4 所提供可用的 IP 地址数目已经不能满足众多用户接入互联网需要。使用 NAT 技术可以使一个机构内的所有用户通过少量合法 IP 地址访问 Internet，从而节省了 Internet 上的合法 IP 地址；另一方面，通过地址转换，可以隐藏内网上主机的真实 IP 地址，从而提高网络的安全性。如图 11.1 所示，防毒墙将内部私有地址转换为公网 IP 地址， 内部多个用户可通过公网 IP 地址进行访问互联网；同时，对于互联网只有公网 IP 地址是可见的，而内部 IP 地址是无法探测到的。

当局域网内的一个主机把一个数据包送到因特网（公网）之前，NAT 服务会把来源 IP 地址转换为一个公网的 IP 地址，再送出数据包。同理，当一个响应数据包从公网送进防毒墙时，NAT 服务会把目的地址由公网 IP 地址转换原先的私有 IP 地址后，再传送给局域网原主机。

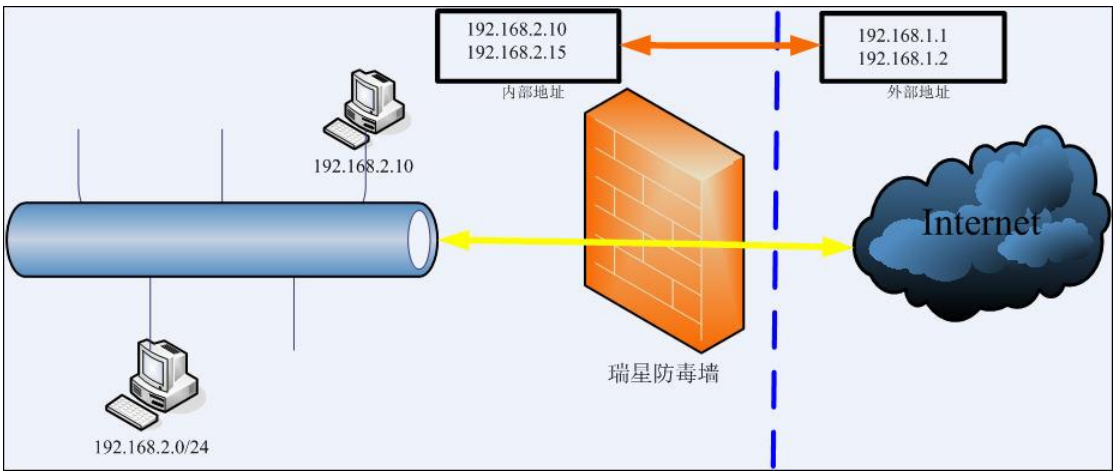


图 11.1 网络地址转换示意图

11.1 源地址转换

源地址转换通常用于公网 IP 地址紧缺，而局域网内部有大量客户端需对外部网络进行访问的情况。瑞星防毒墙对传输数据包的源地址进行转换，使局域网内的主机通过防毒墙地址转换后能够通过合法地址访问外部网络，并对内部地址伪装，从而使外部无法了解局域网的网络拓扑结构，防止一些潜在的攻击。同时，还可缓解 IP 地址短缺等问题。主要包括以下转换形式：

- 1:1 的转换：将内部一个 IP 地址与外部一个 IP 地址建立以一一对应的关系
- N:1 的转换：采用多对一的地址转换功能可以缓解企业公网 IP 地址短缺的问题。并消除企业在变换公网 IP 地址时，重新划分 IP 地址的麻烦
- N:M 的转换，可将内部一个网段转换成外部的一个地址段

11.1.1 增加源地址转换

单击【增加】，为防毒墙增加一条源地址转换记录。如图 11.2 所示。

图 11.2 增加源地址转换记录

1. 输入该策略的友好名称

2. 选择源地址类型，用户可以通过三种方式定义源地址，分别为地址、地址组和自定义。有关此部分设置请参考本文档关于源地址类型和源地址内容的描述

3. 选择目的地址类型和内容，用户可根据指定源地址相同方法设置此部分内容

4. 选择出口，如果使用该接口默认 IP 地址请勾选使用该接口默认地址；如果进行 N：1 的转换，请在转换 IP 处选择转换后的 IP 地址（接口包含多个 IP 地址时需进行选择，如果该接口地址唯一无需进行选择）；如果进行 N：M 的转换，请输入转换后的 IP 地址段范围

5. 选择【启用记录】复选框，则在防毒墙网络日志中记录相应的记录

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条源地址转换记录后，源地址转换记录会在主页面上显示出来。如图 11.3 所示。

图 11.3 源地址转换记录列表

图 11.3 上各字段的说明如下：

字段	说明
序号	按照阿拉伯数字排序。
状态	指示此规则的是否开启。绿色图标表示开启，红色图标表示停用状态。鼠标停留在图标上

	时，会自动显示状态信息
源地址	显示此记录的来源 IP 地址
目的地址	显示此记录的目标 IP 地址
出口	进行地址转换后经由哪个网络接口进行传输
转换 IP	显示转换后 IP 地址，即出口 IP 地址。Default 为该接口默认 IP 地址
设为启用	如果要开启某个被停用的记录，选中该记录，单击【设为启用】，则该记录被启用开始提供 IP 地址转换服务
设为停用	如果要停用某个被启用的记录，选中该记录，单击【设为停用】，则该记录停止服务不再进行 IP 地址的转换服务

表 11.1 地址转换名词解释

11.1.2 删除源地址转换

若要删除某个记录，先选中该记录，然后单击【删除】按钮。

11.2 目的地址转换

目的地址转换功能通常用于外部网络对内部服务器的访问。它是通过对数据包的目的地址或目标端口的重定向，实现伪装内部服务器地址的功能。该功能可保护对外提供服务的计算机安全运行。瑞星防毒墙提供自定义服务功能，使用这些预先定义好的策略阻止一些恶意的网络攻击。

11.2.1 增加目的地址转换

单击【增加】，为防毒墙增加一条目的地址转换记录。如图 11.4 所示。

图 11.4 增加目的地址转换

1. 输入该策略的友好名称

2. 选择源地址类型，用户可以通过三种方式定义源地址，分别为地址、地址组和自定义。有关此部分设置请参考本文档关于源地址类型和源地址内容的描述

3. 选择服务类型，用户可以通过三种方式定义服务，分别为服务、服务组和自定义。有关此部分设

置请参考本文档关于服务的描述

4. 选择接口，在目的地址下拉框中就会显示出可供选择的 IP 地址

5. 选择一个对外提供访问的 IP 地址

提示：如果 E3 接口模式为 PPPoE/DHCP 时，由于其 IP 地址是动态获取的，在下拉框中只显示为“E3 接口的 IP”。

6. 输入进行目的地址转换后的内部服务器 IP 地址，也可对一个 IP 地址段进行转换

7. 选择【启用记录】复选框，则在防毒墙网络日志中记录相应的记录

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条目的地址转换记录后，目的地址转换记录会在主页面上显示出来。如图 11.5 所示。

图 11.5 目的地址转换

图 11.5 各字段的说明

字段	说明
序号	按照阿拉伯数字排序
状态	指示此规则的是否开启。绿色图标表示开启，红色图标表示停用状态。鼠标停留在图标上时，会自动显示状态信息
源地址	显示此记录的来源IP地址。地址在【对象配置】➔【地址】进行设置；地址组在【对象配置】➔【地址组】进行设置
入口	接口位置（通常为连接到Internet的接口）
目的地址	入口的IP地址
服务	采用何种服务。服务在【对象配置】➔【服务】进行设置，也可选中自定义服务设置
转换IP	转换后指向内部主机的IP地址
设为启用	如果要开启某个被停用的记录，选中该记录，单击【设为启用】，则该记录被启用开始提供IP地址转换服务
设为停用	如果要停用某个被启用的记录，选中该记录，单击【设为停用】，则该记录停止服务不再进行IP地址的转换服务

表 11.2 目的地址转换名词解释

11.2.2 删除目的地址转换

若要删除某个记录，先选中该记录，然后单击【删除】按钮。

第十二章 VPN 配置

VPN（Virtual Private Network）即虚拟专用网，虚拟专用网不是真的专用网络，但却能够实现专用网络的功能。虚拟专用网指的是依靠 ISP（Internet 服务提供商）和其它 NSP（网络服务提供商），在公用网络中建立专用的数据通信网络的技术。在虚拟专用网中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公众网的资源动态组成的。

企业用户可以通过瑞星防毒墙 VPN 功能快速建立本地与分支机构和企业部门间的加密通讯，使一些重要数据通过点对点隧道加密传输，确保其他未经授权用户无法读取到传输的数据信息，大大节省了企业使用专用网络和另外购买 VPN 设备的开销。

本节从以下六个方面介绍防毒墙的 VPN 功能：

- SA 配置：密钥交换技术，是建立 IPSec VPN 方式连接的重要组成部分
- VPN 通道：通过防毒墙建立 VPN 通道
- 通道状态：查看 VPN 通道的状态
- L2TP 设置：一种支持多协议虚拟专用网络的联网技术，它允许远程用户通过 Internet 安全地访问企业网络
- PPTP 设置：远程用户能够通过 Microsoft Windows 2000 和 Microsoft Windows XP 等全系列 Windows 操作系统以及其它装有点对点协议的系统安全访问公司网络
- SSLVPN 配置：通过 SSL 建立安全访问通道的 VPN 技术
- 用户设置：设置通过 L2TP 和 PPTP 方式建立 VPN 连接时所需的认证信息

提示：启用防毒墙 VPN 功能需要在相应的接口上启用相应的服务，如何启用 VPN 服务请参阅本手册 3.1 接口配置部分内容。

12.1 SA 配置

进行 VPN 通讯，首先需要建立 SA 协商信息。通过在会话的两端设置相同密钥信息，在双方进行通讯时，使用这种方法彼此验证对方。在【VPN 配置】➔【SA 配置】，进入 SA 配置页面，如图 12.1 所示。

图 12.1 SA 设置页面

12.1.1 增加 SA

单击【增加】，为防毒墙增加一条 SA 密钥，如图 12.2 所示。

图 12.2 增加 SA

1. 输入该条 SA 的名称，不能和其他 SA 名称冲突需唯一
2. 选择 IKE 认证方式，目前支持预共享密钥验证方式
3. 输入交互时协商密钥
4. 确认认证密钥，防止误操作
5. 选择协商密钥的加密方式
6. 选择数据传输密钥的加密方式
7. 是否启用 PFS，向前保密加密传输数据，防止攻击者破解密钥
8. 输入协商超时时间
9. 输入 IPSEC 加密传输超时时间

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙添加一条 SA 协商密钥后，SA 记录会在主页面上显示出来。如图 12.3 所示。

图 12.3 SA 配置列表

12.1.2 修改 SA

单击该条 SA 记录操作下的 图标进入修改页面，如图 12.4 所示。

图 12.4 修改 SA 协商密钥

1. 选择 IKE 认证方式，目前支持预共享密钥验证方式
2. 输入交互时协商密钥
3. 确认认证密钥，防止误操作
4. 选择协商密钥的加密方式
5. 选择数据传输密钥的加密方式
6. 是否启用 PFS，向前保密加密传输数据，防止攻击者破解密钥
7. 输入协商超时时间
8. 输入 IPSEC 加密传输超时时间
9. 单击【确定】完成修改，单击 【返回】取消修改

12.1.3 删除 SA

若要删除某条 SA 记录，请选中该记录，单击【删除】按钮。

12.2 VPN 通道

建立 VPN 会话通道需要使用 SA 协商密钥，通过在需要建立 VPN 会话的两端配置相同的密钥，使用密钥去彼此验证对方，(这个过程由 SA 自动完成，无需用户参与)，通道建立后，会话双方的所有数据通讯都会通过该通道加密传输。单击【VPN 配置】➔【VPN 通道】进入添加 VPN 通道页面，如图 12.5 所示。

12.5 VPN 通道列表

12.2.1 增加 VPN 通道

在 VPN 通道配置页面单击【增加】，进入 VPN 通道增加页面，如图 12.6 所示。

图 12.6 增加 VPN 通道

图 12.6 各字段文字说明

字段	说明
通道名	为建立的通道设置名称，方便管理
本地网关	VPN端点的本地网络的网关地址
本地子网	VPN端点内部接口的本地局域网络
远程网关	VPN远端的网关地址
远程子网	VPN远程端点的子网地址
SA	自动协商密钥
DPD	监视VPN隧道两个端点间的VPN连接
DPD间隔	DPD查询间隔时间
DPD超时	DPD查询已建立隧道连接的超时时间
DPD操作	包含“hold”和“clear”,hold为不做任何操作；clear为清除VPN连接。

表 12.1 VPN 通道说明

增加步骤：

1. 在通道名处输入一个通道名称

2. 选择本地网关地址。选择 IP 为选择提供 VPN 服务接口的 IP 地址，使用设备 ID 则通过瑞星防毒墙唯一的设备 ID 号查询该接口的公网 IP 地址

3. 在本地子网处输入在该通道内进行 VPN 通讯的子网 IP 地址或网段

4. 在远程网关处填写隧道另一端网络中的网关地址。“任意”为任意 IP 地址通过协商认证均可连接到本端网络；“指定 IP”为指定远端网络的网关地址；“使用域名”为通过域名解析远端网关地址；“使用设备 ID”则通过瑞星防毒墙唯一的设备 ID 号查询远程网关的公网 IP 地址

5. 在远程子网处填写隧道另一端网络中的子网地址。“任意”为任意 IP 地址通过协商认证均可连接到本端网络；“无”为只提供本端到远端固定主机的隧道连接，不提供远端局域网主机的连接；“自定义”为设置远程子网的 IP 地址或网段

6. DPD 功能为检测隧道连接的状态，此功能为可选配置。启用该功能后，可在固定的周期内定时检测 VPN 隧道连接的状态，如果发现隧道中的两点连接在 DPD 超时时间后仍然没有连接上，可进行 hold 或 clear 操作。

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条 VPN 通道后，VPN 通道记录会在主页面上显示出来。如图 12.7 所示。

图 12.7 VPN 通道

12.2.2 修改 VPN 通道

单击该条通道记录操作下的 图标进入修改页面，如图 12.8 所示。

图 12.8 修改 VPN 通道

1. 选择本地网关地址。选择 IP 为选择提供 VPN 服务接口的 IP 地址，使用设备 ID 则通过瑞星防毒墙唯一的设备 ID 号进行查询地址该接口的公网 IP 地址

2. 在本地子网处输入在该通道内进行 VPN 通讯的子网 IP 地址或网段

3. 在远程网关处填写隧道另一端网络中的网关地址。“任意”为任意 IP 地址通过协商认证均可连接到本端网络；“指定 IP”为指定远端网络的网关地址；“使用域名”为通过域名解析远端网关地址；“使用设备 ID”则通过瑞星防毒墙唯一的设备 ID 号进行查询远程网关的公网 IP 地址

4. 在远程子网处填写隧道另一端网络中的子网地址。“任意”为任意 IP 地址通过协商认证均可连接到本端网络；“无”为只提供本端到远端固定主机的隧道连接，不提供远端局域网主机的连接；“自定义”为设置远程子网的 IP 地址或网段

5. DPD 功能为检测隧道连接的状态，此功能为可选配置。启用该功能后，可在固定的周期内定时检测 VPN 隧道连接的状态，如果发现隧道中的两点连接在 DPD 超时时间后仍然没有连接上，可进行 hold 或 clear 操作。

6. 单击【确定】完成修改，单击【返回】取消修改

12.2.3 删除 VPN 通道

若要删除某条 VPN 通道，请选中该通道记录，单击【删除】按钮。如图 12.9 所示。

图 12.9 删除 VPN 通道

12.3 通道状态

单击【VPN 配置】➔【通道状态】处查看远程网关到本端已经建立 VPN 连接通道的状态，如图 12.10 所示。

图 12.10 VPN 连接状态

图 12.10 各字段文字说明

字段	说明
序号	按阿拉伯数字排序通道序号
通道名称	为建立的通道设置名称，方便管理
本地网关	VPN端点的本地网络的网关地址
本地子网	VPN端点内部接口的本地局域网地址
远程网关	VPN远端的网关地址
远程子网	VPN远程端点的子网地址
状态	connected为连接状态， waiting为等待状态，括号内为通道连接采取的加密算法
刷新	刷新防毒墙VPN连接的状态

表 12.2 VPN 通道状态说明

12.4 L2TP 设置

第二层隧道协议（L2TP）是一种支持多协议虚拟专用网络的联网技术，它允许远程用户通过 Internet 安全地访问企业网络。单击【VPN 配置】➔【L2TP 设置】进入 L2TP 设置页面，如图 12.11 所示。

图 12.11 L2TP 设置

图 12.11 中各字段说明

字段	说明
启用服务	是否启用L2TP服务
认证方式	包含两种认证方式，PAP密码认证方式；CHAP挑战握手认证方式，BOTH为支持PAP和CHAP两种认证方式。
接口	选择提供L2TP服务的接口
接口地址	选择接口IP地址
起始地址	用于分配给L2TP客户端的IP地址段的起始IP地址
终止地址	用于分配给L2TP客户端的IP地址段的终止IP地址
配置内部DNS	分配给L2TP客户端的内部域名解析服务器地址
配置内部WINS	分配给L2TP客户端的内部网际名称服务器地址
应用	单击【应用】，保存L2TP设置

表 12.3 L2TP 设置说明

12.5 PPTP 设置

点对点隧道协议（PPTP）是一种支持多协议虚拟专用网络的网络技术。通过该协议，远程用户能够通过 Microsoft Windows 2000 和 Microsoft Windows XP 等全系列 Windows 操作系统以及其它装有点对点协议的系统安全访问公司网络。单击【VPN 配置】➔【PPTP 设置】进入 PPTP 设置页面，如图 12.12 所示。

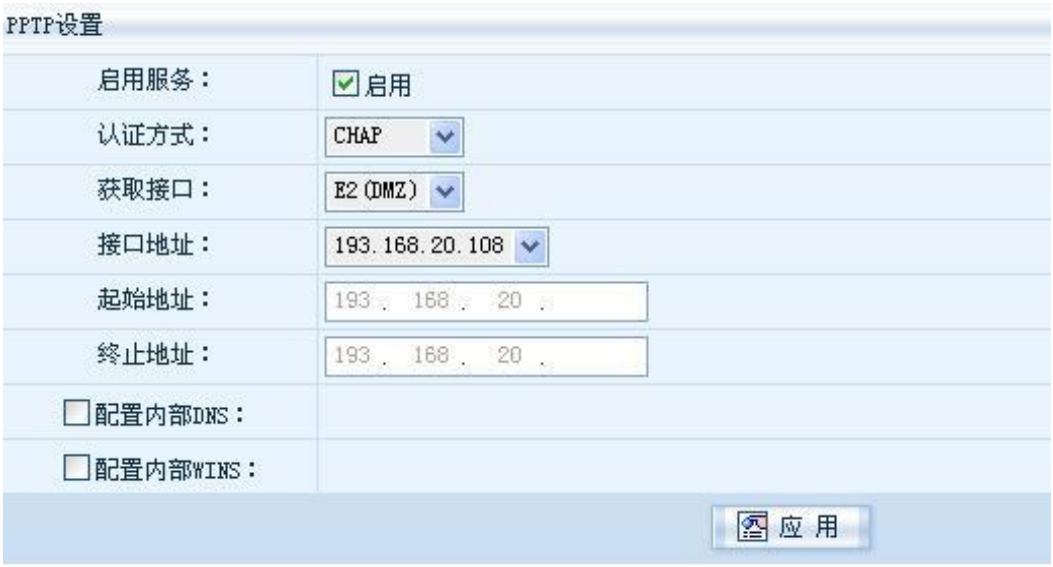


图 12.12 PPTP 设置

字段	说明
启用服务	是否启用PPTP服务
认证方式	包含三种认证方式，PAP密码认证方式；CHAP挑战握手认证方式；MS-CHAP是Microsoft Windows家族提供的唯一支持在身份验证过程中更改密码的身份验证协议
接口	选择提供PPTP服务的接口
接口地址	选择接口IP地址
起始地址	用于分配给PPTP客户端的IP地址段的起始IP地址
终止地址	用于分配给PPTP客户端的IP地址段的终止IP地址
配置内部DNS	分配给PPTP客户端的内部域名解析服务器地址
配置内部WINS	分配给PPTP客户端的内部网际名称服务器地址
应用	单击【应用】，保存PPTP设置

表 12.4 PPTP 设置说明

12.6 SSLVPN 配置

SSLVPN 是基于安全套接层协议建立的远程安全访问通道。单击【VPN 配置】➔【SSLVPN 配置】，进入 SSLVPN 配置页面，如图 12.13 所示。

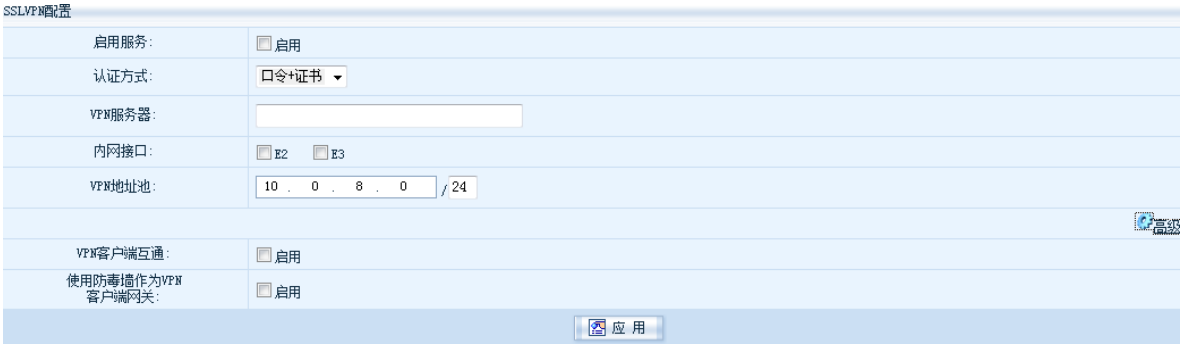


图 12.13 SSLVPN 配置页面

字段	说明
启用服务	是否启用SSLVPN服务
认证方式	包含证书和口令+证书的认证方式，请根据VPN用户设置信息选择认证方式
VPN服务器	此处填写防毒墙外网口启用SSLVPN服务的接口地址或域名
内网接口	SSLVPN拨入与内网通讯接口
VPN地址池	SSLVPN拨入客户获取IP地址范围
VPN客户端互通	单击【高级】，如图12.13所示，启用该选项则SSLVPN拨入的客户端相互之间可以进行网络通讯
使用防毒墙作为VPN客户端网关	单击【高级】，如图12.13所示，启用该选项则SSLVPN拨入客户端使用防毒墙分配的网关地址
应用	单击【应用】，保存SSLVPN设置

表 12.5 SSLVPN 配置说明

12.7 用户设置

外部通过 L2TP、PPTP 和 SSLVPN 方式连接企业内部客户端时，需要输入用户认证信息。单击【VPN 配置】➔【用户设置】，进行用户信息的设置，如图 12.14 所示。

图 12.14 VPN 用户配置列表

12.7.1 增加 VPN 用户

在 VPN 用户配置页面，单击【增加】按钮，如图 12.15 所示。

图 12.15 增加 VPN 用户

1. 在用户名处输入此用户使用的用户名
2. 在密码和重复密码处输入密码
3. 输入 IP 地址，如果不指定 IP 地址，客户端将从防毒墙上指定地址段中动态获取地址

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条 VPN 用户信息后，该记录会在主页面上显示出来。如图 12.16 所示。如需使用 SSLVPN 方式，请单击图标下载证书。

图 12.16 VPN 用户配置列表

12.7.2 修改 VPN 用户

在 VPN 用户配置页面单击图标，如图 12.17 所示。

图 12.17 修改 VPN 用户

1. 在密码和重复密码处输入需要修改的密码

2. 在 IP 地址处输入需要修改的 IP 地址，如果不指定 IP 地址，客户端将从防毒墙上指定地址段中动态获取地址

当填写好相关修改内容后，单击【确定】按钮确认修改，【返回】按钮取消修改。

12.7.3 删除 VPN 用户

选中该条记录前的复选框，单击【删除】按钮。

第十三章 流量配置

流量管理功能可对某一 IP 或网段在单位时间内的数据流量进行管理。本章将从五个方面进行介绍：

- 统计配置：对防毒墙内部的客户端的数据流量进行统计
- 控制配置：对防毒墙内部的客户端进行数据流量控制
- 流量查看：查看防毒墙内部客户端的数据流量
- 流量分析：根据流量搜索条件查看客户端的详细流量
- 带宽管理：对客户端的上传、下载带宽进行详细的控制

13.1 统计配置

流量管理功能方便管理员管理网络，进行流量管理和流量分析之前，首先要对网络中的网络设备、主机和服务器进行流量统计。

13.1.1 增加流量统计配置

要进行流量统计，首先要对统计的接口以及网段进行配置，单击【流量配置】➔【统计配置】进入统计配置页面，单击【增加】按钮如图 13.1 所示。

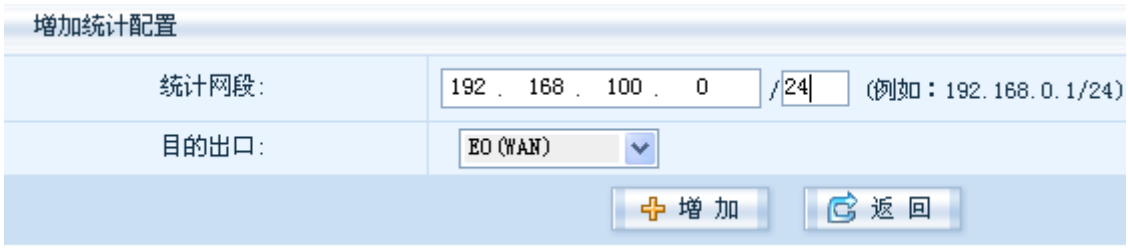


图 13.1 增加流量统计配置

增加步骤：

1. 在统计网段处填写需要进行统计的网段或主机
2. 选择该网段的出口

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条流量统计配置规则后，流量统计配置记录会在主页面上显示出来。如图 13.2 所示。

图 13.2 增加统计配置

字段	说明
序号	按照阿拉伯数字排序

状态	代表该策略是否开启。绿色图标表示开启，红色图标表示停用状态。
统计网段	统计规则所适用的网段
目的出口	所有经策略传输的接口
设为启用	如果要开启某个被停用的规则，选中该规则前的复选框单击【设为启用】，则该规则被启用并开始统计
设为停用	如果要停用某个被启用的规则，选中该规则前的复选框单击【设为停用】，则该规则停止流量统计服务

表 13.1 流量统计名词解释

13.1.2 删除流量统计配置

若要删除某条流量统计记录，选中该记录单击【删除】按钮，如图 13.3 所示。

图 13.3 删除流量统计配置

13.2 控制配置

在控制配置管理页面中可以按 IP 地址或者网段进行流量控制，并可灵活设置控制的时间周期。单击【流量配置】➔【控制配置】进入控制配置页面。如图 13.4 所示。

图 13.4 流量控制配置

13.2.1 增加流量控制配置

单击【增加】进入增加控制配置页面，如图 13.5 所示。

图 13.5 增加控制配置

其中：

字段	说明
主机/网络	填写主机IP地址或IP网段。书写格式为IP地址/掩码
流量限额	设定流量限制，单位:MB

控制周期	设定控制周期，周期分为每年、每月、每周、每天、每小时。
每年	统计周期为一整年 ,结束时间为该年的最后一秒。例如 :2005-1-1 0:00:00～2005-12-31 23:59:59。
每月	统计周期为一整月，结束时间为该月的最后一秒。例如：5月1日 0:00:00～5月31日 23:59:59。
每周	统计周期为一整周，结束时间为该周的最后一秒。例如：周一0:00:00～该周周日 23:59:59。
每天	统计周期为一整天，结束时间为该天的最后一秒。例如：0:00:00～23:59:59。
每小时	统计周期为一小时，例如：15:00:00～15:59:59。

表 13.2 流量控制名词解释

增加步骤：

1. 在主机/网络处填写需要进行控制的网段或主机
2. 在流量限额处输入该网段或主机在控制周期内允许的最大数据流量
3. 选择控制周期

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条流量控制配置规则后，流量控制配置记录会在主页面上显示出来。如图 13.6 所示。

图 13.6 防毒墙控制配置记录

在控制周期内，进行流量控制的网段或主机超过流量限额允许的范围，防毒墙将拒绝这个网段或主机的访问请求，并在下一个周期开始时进行自解锁。管理员也可解除锁定状态，关于解除锁定状态参阅本文档 13.3 流量查看部分。

13.2.2 删除流量控制配置

若要删除某条流量控制配置规则，选中该记录，单击【删除】按钮。如图 13.7 所示。

图 13.7 删除流量控制配置

13.3 流量查看

网络管理员可以实时查看当前被统计主机的网络流量，单击【流量配置】➔【流量查看】，进入流量查看页面，如图 13.8 所示。

流量查看

序号	▲地址	控制周期	▽限额(字节)	▽上传包	▽下载包	▽上传字节	▽下载字节	▽总合	状态	操作
1	193.168.20.12	无	0	77	67	10083	9330	19413	正常	-
2	193.168.20.74	无	0	393	335	55299	83516	138815	正常	-
3	193.168.20.75	无	0	231	209	29045	28628	57673	正常	-
4	193.168.20.99	无	0	108	77	7872	17428	25300	正常	-
5	193.168.20.100	无	0	77	66	9768	8877	18645	正常	-
6	193.168.20.108	无	0	1838	2123	359807	266662	626469	正常	-
7	193.168.20.110	无	0	77	66	9768	8877	18645	正常	-
8	193.168.20.112	无	0	84	75	10692	9516	20208	正常	-
9	193.168.20.131	无	0	104	92	13322	25312	38634	正常	-
10	193.168.20.215	无	0	102	91	13378	21883	35261	正常	-
11	193.168.20.242	无	0	714	619	87586	86668	174254	正常	-
12	193.168.20.243	无	0	156	141	19849	59772	79621	正常	-

图 13.8 查看流量

图 13.8 各字段文字说明

字段	说明
序号	按照阿拉伯数字排序。
地址	统计流量的IP地址
控制周期	当前IP地址的控制周期，“无”表示没有对该IP启用流量控制
限额	在控制周期内允许的数据流量范围
上传包	该IP地址在统计周期内经防毒墙上传的数据包
下载包	该IP地址在统计周期内经防毒墙下载的数据包
上传字节	该IP地址在统计周期内经防毒墙上传的字节数
下载字节	该IP地址在统计周期内经防毒墙下载的字节数
总合	该IP地址在统计周期内经防毒墙上传和下载的字节数总和
状态	分为正常和锁定状态，当该IP地址在控制周期内超出流量限额就会被防毒墙锁定
操作	正常状态下无需任何操作，当前IP地址被锁定后，管理员可以单击 图标解除当前IP地址的锁定状态

表 13.3 流量查看名词解释

查看具体 IP 地址的流量，单击需要查看的 IP 地址，弹出如图 13.9 所示页面。该页面显示了此 IP 地址近期数据流量的曲线图。

图 13.9 显示某个 IP 流量图

高级设置

单击【显示高级设置】，根据防毒墙提供的搜索条件，缩小查找范围，如图 13.10 所示。

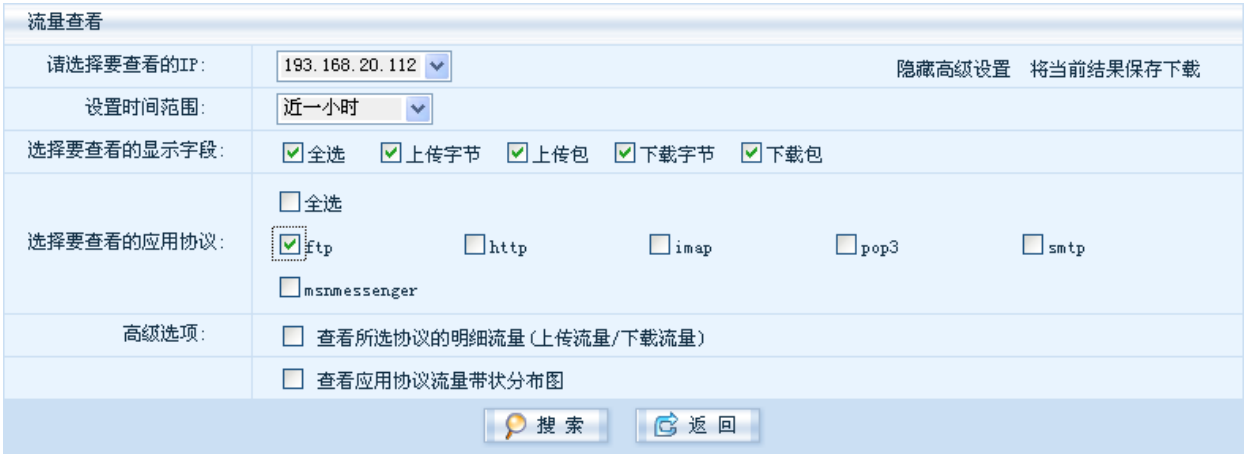


图 13.10 流量查看高级设置

图 13.10 各字段文字说明

字段	说明
请选择要查看的IP	选择进行统计流量的IP地址，可单击下拉按钮选择显示其他地址
隐藏高级设置	隐藏高级设置选项
将当前结果保存下载	将当前IP地址的数据流量统计信息通过网页下载到本地
设置时间范围	设置查询的时间范围，共有六个可选项，分别是：近一小时、近一天、近一周、指定历史周、指定历史日期和指定历史时间
选择要查看的显示字段	分为上传字节、上传包、下载字节、下载包，也可全选。对上述选项进行选择，该IP地址

	的详细流量信息会显示勾选选项的详细信息
选择要查看的应用协议	对进行协议识别的协议都可进行查看，对上述选项进行选择，该IP地址的详细流量信息会显示勾选协议的详细信息
高级选项	是否查看所选协议的详细流量，包括协议的上传流量和下载流量
	是否查看应用协议流量带状分布图

表 13.4 流量查看名词解释

当选择好相关内容后，单击【搜索】进行查询，单击【返回】按钮则取消查询。

13.4 流量分析

瑞星防毒墙提供详细的流量数据分析功能，如图 13.11 所示。可按时间条件、异常流量和带宽条件进行分类查询。

图 13.11 流量查询

进行流量分析的步骤：

1. 在时间条件处输入搜索的时间范围，可选择时间介于 99 分钟内或历史某个时段
2. 单击【只显示异常流量记录】复选框，如图 13.12 所示

图 13.12 设置防毒墙异常流量

3. 瑞星防毒墙默认将发包量大于收包量的十倍时认作是异常流量，用户可通过实际使用情况更改这个值
4. 在带宽条件处输入上传字节大于某值或下载字节大于某值
5. 如需进一步缩小搜索范围，请单击图 13.11 按条件查询右下的【显示高级设置】，如图 13.13 所示

图 13.13 流量分析高级搜索条件

字段	说明
时间条件	输入查询的时间范围
选择要查看的应用协议	选择进行协议识别的一种或多种协议进行搜索
高级选项	查看选中协议的上传/下载流量
异常流量	当发包流量和收包流量不成正比的时候，防毒墙认为是异常流量，管理员可根据实际情况设定发包和收包的比例来查看异常流量
带宽条件	对上传/下载字节大于某值的流量进行搜索

表 13.5 流量分析名词解释

6. 单击【搜索】

查询结果如图 13.13 所示

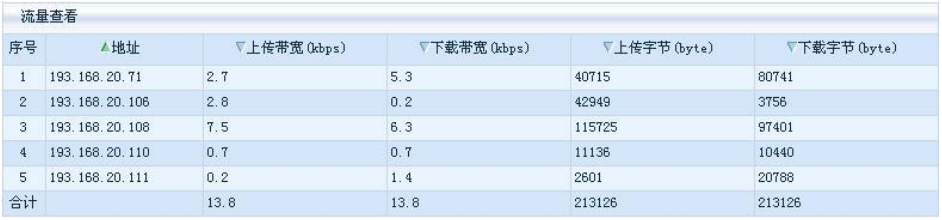


图 13.14 流量查看

13.5 带宽管理

带宽管理功能让管理员可以方便地管理通过防毒墙的数据流量。管理员可以在不同的接口上，根据不同的带宽策略和不同优先级别控制分配网络流量。防毒墙的带宽控制是基于 IP 地址进行控制，可以对一个网段或者单个 IP 地址进行带宽控制。

我们首先要对企业网络带宽管理进行详细规划。例如：一个企业包含很多部门，如：财务部、人力资源部、生产部、销售部等等，各个部门对网络带宽的需求也是不同的，根据各个部门的带宽需求进行带宽

分配，既保证一些部门的特殊需求，也保证了带宽的合理使用。

13.5.1 带宽分类

假设 E0 接口的网络区域为 LAN 区，在 E0 接口下的网络拓扑图，如图 13.15 所示。

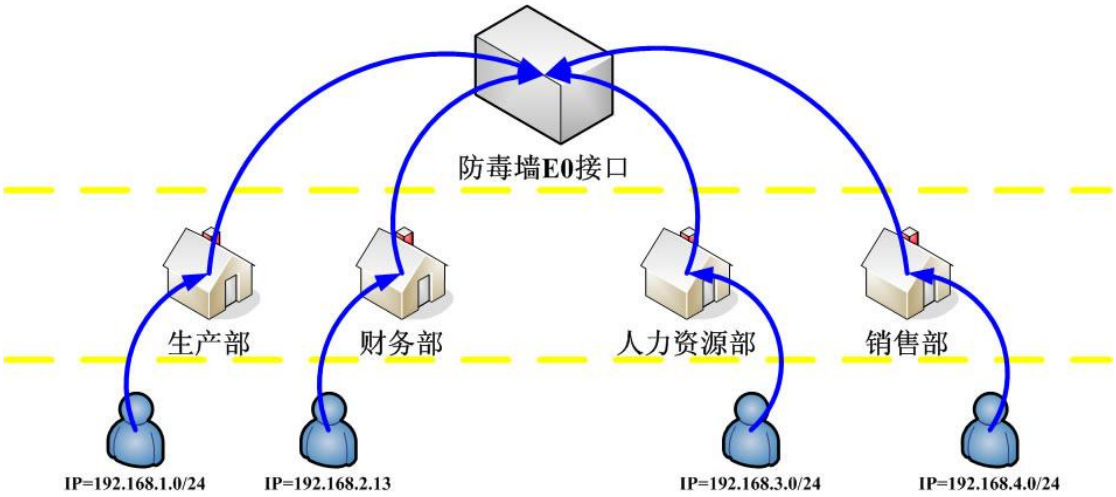


图 13.15 企业内部局域网网络拓扑图

该拓扑结构需要在 E0 接口上增加四个一级带宽分类进行带宽控制。

13.5.1.1 增加带宽分类

1. 单击【流量配置】➔【带宽管理】进入带宽配置页面，如图 13.16 所示。

图 13.16 防毒墙带宽配置

2. 单击【增加】，进入增加带宽分类页面，如图 13.17 所示

图 13.17 增加带宽分类

字段	说明
名称	输入带宽分类的名称
接口	进行带宽控制的网络接口
上级分类	瑞星防毒墙可进行两级带宽分类,上级分类显示了当前分类规则所隶属的上级分类规则名称

上传带宽	单位时间内上传数据的最大数据流量，其换算比例为 1000Kbps=1M
下载带宽	单位时间内下载数据的最大数据流量，其换算比例为 1000Kbps=1M
优先级	带宽分类的优先级别，数字越小优先级别越高

表 13.6 带宽分类名词解释

3. 在名称处输入带宽分类的名称
4. 在上传带宽处输入单位时间内的允许上传最大数据流量值
5. 在下载带宽处输入单位时间内的允许下载最大数据流量值
6. 在优先级处输入该带宽分类的优先级别

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条带宽分类规则后，带宽分类记录会在主页面上显示出来。如图 13.18 所示。

图 13.18 带宽分类规则

13.5.1.2 修改带宽分类

单击带宽分类记录的图标，进入修改带宽分类页面，如图 13.19 所示。

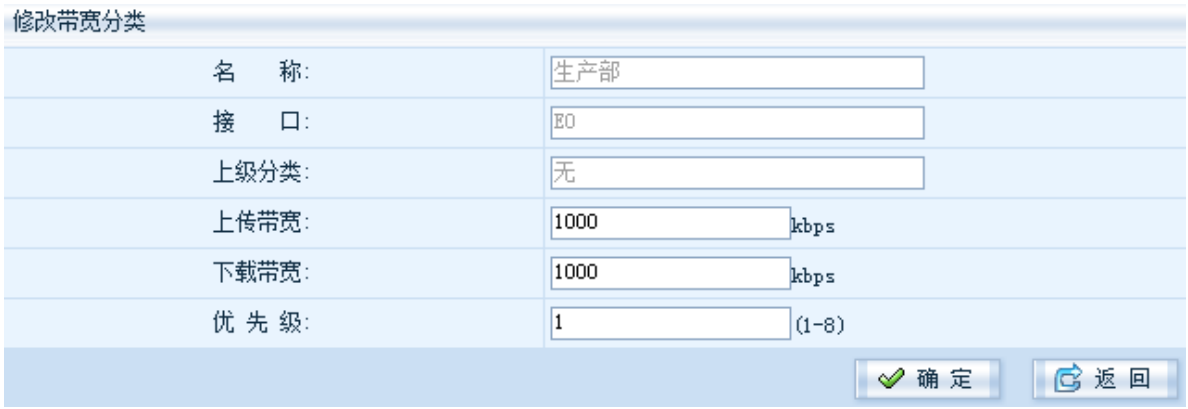


图 13.19 修改带宽分类

1. 在上传带宽处输入需要更改的上传带宽值
2. 在下载带宽处输入需要更改的下载带宽值
3. 在优先级别处输入需要修改的优先级别

当填写好相关修改内容后，单击【确定】按钮确认修改，【返回】按钮取消修改。

13.5.1.3 删除带宽分类

单击带宽分类记录的图标，删除该条带宽分类记录。

> 提示：如果删除带宽分类，则该分类下的所有规则将被全部删除。

13.5.2 二级带宽分类

单击【流量管理】➔【带宽管理】进入带宽配置页面，如图 13.20 所示。

图 13.20 带宽分类记录列表

> 提示：如果您的企业网络拓扑结构使用一级带宽分类即可完成带宽控制，可跳过此部分内容的阅读。

13.5.2.1 增加二级带宽分类

1. 选中带宽分类为生产部的带宽分类记录，单击【增加】进入增加带宽分类页面，如图 13.21 所示

图 13.21 增加带宽分类

字段	说明
类型	分为带宽分类和过滤规则，这里增加的带宽分类为二级带宽分类，可进一步将带宽策略细化，方便管理

	员进行管理。而过滤规则为增加带宽控制策略
名称	输入带宽分类的名称
接口	进行带宽控制的网络接口
上级分类	瑞星防毒墙可进行两级带宽分类,上级分类显示了当前分类规则所隶属的上级分类规则名称
上传带宽	单位时间内上传数据的最大数据流量，其换算比例为 1000Kbps=1M
下载带宽	单位时间内下载数据的最大数据流量，其换算比例为 1000Kbps=1M
优先级	带宽分类的优先级别，数字越小优先级别越高

表 13.7 二级带宽分类名词解释

2. 在类型处选择带宽分类
3. 在名称处输入二级带宽分类的名称
4. 在上传带宽处输入单位时间内的允许上传最大数据流量值
5. 在下载带宽处输入单位时间内的允许下载最大数据流量值
6. 在优先级处输入该带宽分类的优先级别

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条带宽分类规则后，带宽分类记录会在主页面上显示出来。如图 13.22 所示。

图 13.22 二级带宽分类

13.5.2.2 修改二级带宽分类

此部分设置与本文档 13.5.1.2 修改带宽分类内容相同，如需进行更改请参阅该部分内容。

13.5.2.3 删除二级带宽分类

此部分设置与本文档 13.5.1.3 删除带宽分类内容相同，如需进行更改请参阅该部分内容。

13.5.3 带宽策略

完成带宽分类设置后，就可增加带宽策略进行带宽控制，单击【流量配置】➔【带宽管理】进入带宽配置页面，如图 13.23 所示。

图 13.23 带宽分类记录列表

13.5.3.1增加带宽策略

增加带宽过滤规则分为两类：

- 从一级分类增加带宽过滤规则

1. 选中带宽分类为生产部的带宽分类记录，单击【增加】进入增加带宽分类页面，如图 13.24 所示

图 13.24 增加带宽策略

2. 在类型处选择【过滤规则】单选按钮，进入增加过滤规则页面，如图 13.25 所示

图 13.25 带宽过滤规则

- 从二级分类增加带宽过滤规则：

  选中生产部一组带宽分类单击【增加】进入增加过滤规则页面，如图 13.26 所示

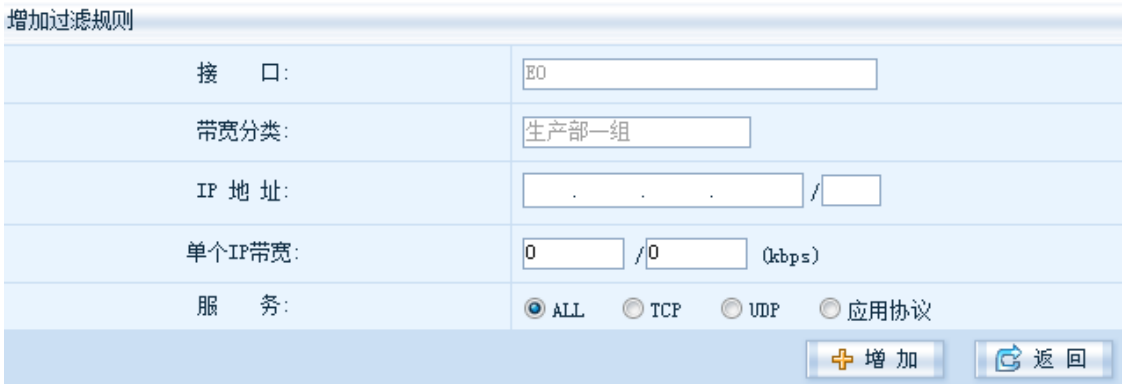


图 13.26 带宽过滤规则

字段	说明	
接口	进行带宽控制的网络接口	
带宽分类	瑞星防毒墙可进行两级带宽分类，带宽分类表示过滤规则所隶属的带宽分类规则	
IP 地址	需要进行控制的客户端地址，可以是网段或某个主机地址	
单个 IP 带宽	如果 IP 地址处输入的是一个地址段，此处可对该地址段的单个 IP 进行带宽控制。前一个输入框输入上传带宽值；后一个输入框输入下载带宽值；0 表示不进行单个 IP 的带宽控制。	
服务	ALL	分为 ALL、TCP 和 UDP。ALL 包含 TCP 和 UDP 的所有源端口和目的端口
	TCP	分为匹配所有端口、匹配源端口和匹配目的端口。匹配所有端口：对 TCP 源端口和目的端口为 1-65535 的所有端口进行匹配；匹配源端口：对 TCP 源端口为 1-65535 的所有端口进行选择性匹配；匹配目的端口：对 TCP 目的端口为 1-65535 的所有端口进行选择性匹配
	UDP	分为匹配所有端口、匹配源端口和匹配目的端口。匹配所有端口：对 UDP 源端口和目的端口为 1-65535 的所有端口进行匹配；匹配源端口：对 UDP 源端口为 1-65535 的所有端口进行选择性匹配；匹配目的端口：对 UDP 目的端口为 1-65535 的所有端口进行选择性匹配
	应用协议	根据识别出的协议进行带宽控制，有关此部分内容请参阅本手册 8.7 应用协议部分内容

表 13.8 带宽过滤规则名词解释

- **增加带宽控制**

  1. 在 IP 地址处输入客户端的 IP 地址或网段
  2. 在单个 IP 带宽输入需要控制该地址段每个 IP 地址的上传下载带宽值
  3. 在服务处选择需要进行的端口或应用协议控制规则，如图 13.27 所示

图 13.27 增加带宽过滤规则

当填写好相关内容后，单击【增加】按钮保存设置，【返回】按钮取消操作。当向防毒墙增加一条下载带宽控制规则后，带宽控制记录会在主页面上显示出来。如图 13.28 所示。

图 13.28 防毒墙带宽控制规则

13.5.3.2修改带宽策略

单击带宽策略记录的图标，进入修改过滤规则页面，如图 13.29 所示。

图 13.29 修改带宽策略

1. 在 IP 地址处输入需要修改客户端的 IP 地址或网段
2. 在单个 IP 带宽输入需要修改的上传下载带宽值
3. 在服务处输入需要修改的服务

当填写好相关修改内容后，单击【确定】按钮确认修改，【返回】按钮取消修改。

13.5.3.3删除带宽策略

单击带宽策略记录的图标，删除该条带宽分类记录。

第十四章 日志审计

本章我们从八个方面了解防毒墙日志审计的详细设置：

- 病毒日志：查看防毒墙过滤的病毒日志
- 垃圾邮件：查看防毒墙过滤的垃圾邮件日志
- 隔离文件：查看防毒墙隔离的病毒文件和垃圾邮件
- 管理日志：查看防毒墙管理员进行防毒墙管理操作日志
- 系统日志：查看防毒墙系统日志
- 网络日志：查看防毒墙网络安全日志
- URL 日志：查看内网客户端上网网址详细记录
- 可疑文件：查看防毒墙可疑文件日志
- 入侵日志：查看防毒墙入侵防御日志
- 告警配置：对防毒墙日志存储和防毒墙告警功能进行配置

14.1 病毒日志

单击【日志审计】➔【病毒日志】，进入防毒墙病毒日志查询页面，该页面显示近期防毒墙的病毒查杀日志，如图 14.1 所示。

图 14.1 防毒墙病毒日志查询

病毒日志详细信息各字段文字详细说明

字段	说明
序号	事件日志的序号
时间	事件的发生时间（以防毒墙系统时间记录）
协议	通过何种协议进行传播
源IP	数据包发送IP地址
目的IP	数据包目的IP地址
描述	病毒信息的详细描述

病毒名	病毒的名称
处理方式	显示防毒墙对当前病毒所做操作，操作分为记录、杀毒、阻断

表 14.1 病毒查杀日志名词解释

查询病毒日志：

1. 在协议处选择病毒通过哪种协议进行传播，分为：HTTP、FTP、SMTP、POP3、IMAP、MSN 和全部，全部则代表包含上述六种协议
2. 在源地址处输入进行查询的来源 IP 地址
3. 在目的地址处输入进行查询的目的 IP 地址
4. 在按时间查询处选择查询的时间范围
5. 在病毒名处输入病毒的名称信息
6. 选择查看方式，分为：查看详细记录结果或查看统计结果
7. 单击【搜索】进行查询

- 病毒查杀详细信息：可使用此功能查询防毒墙拦截病毒的详细信息，如图 14.2 所示

病毒日志详细信息(共有55条符合条件的记录)

序号	时间	协议	源IP	目的IP	描述	病毒名	处理方式
1	2007-05-29 10:43:42	HTTP	192.168.3.215	193.168.20.131	http://193.168.20.131/h.zip	1:Iceland	记录
2	2007-05-29 10:33:25	HTTP	192.168.3.215	193.168.20.131	http://193.168.20.131/h.zip	1:Iceland	记录
3	2007-05-29 09:38:18	SMTP	193.168.20.131	193.168.20.244	发件人： ryn@ryn.com 收件人： gao@gzj.com 主 题： zzzzz	1:Haddock.1355	杀毒
4	--	--	--	--	--	2:Tic-O93b	杀毒
5	--	--	--	--	--	3:Hacktic	杀毒
6	--	--	--	--	--	4:Hacktic	杀毒
7	--	--	--	--	--	5:Horse.1594	杀毒
8	--	--	--	--	--	6:Horse.1594	杀毒
9	--	--	--	--	--	7:HACKER-D	杀毒
10	--	--	--	--	--	8:Hacker-c	杀毒

首 页 上一页 下一页 末 页 到第1 页 GO [每页10条] [当前1/6页][下载日志信息]

图 14.2 病毒查杀日志的详细信息

- 病毒日志统计信息：可使用此功能查询防毒墙拦截病毒的统计信息，如图 14.3 所示

对指定时间范围内的病毒暴发百分比

排名	病毒名	数 量	百分比
1	Hacktic	8	14.55%
2	Horse.1594	8	14.55%
3	Iceland	7	12.73%
4	Tic-093b	4	7.27%
5	Hacker-c	4	7.27%
6	其 他	24	43.64%

对指定时间范围内的分协议病毒百分比

排名	协 议	数 量	百分比
1	POP3	31	56.36%
2	SMTP	20	36.36%
3	HTTP	2	3.64%
4	FTP	2	3.64%
5	IMAP	-	-
6	MSN	-	-

对指定时间范围内的源病毒事件TOP5

排名	源 IP	数 量	百分比
1	193.168.20.131	51	92.73%
2	192.168.3.215	4	7.27%
3	-	-	-
4	-	-	-
5	-	-	-

对指定时间范围内的目的病毒事件TOP5

排名	目的IP	数 量	百分比
1	193.168.20.244	51	92.73%
2	193.168.20.131	4	7.27%
3	-	-	-
4	-	-	-
5	-	-	-

图 14.3 病毒查杀日志的统计信息

14.2 垃圾邮件

单击【日志审计】➔【垃圾邮件】，进入防毒墙垃圾邮件日志页面。防毒墙的垃圾邮件日志功能可按源IP、目的 IP 和时间对检测到的垃圾邮件进行分类记录，如图 14.4 所示。

图 14.4 垃圾邮件日志详细信息

图 14.4 垃圾邮件日志详细信息各字段文字说明

字段	说明
序号	事件日志的序号
时间	事件的发生时间（以防毒墙系统时间记录）
协议	通过何种协议进行传播
源IP	发送垃圾邮件的IP地址
目的IP	垃圾邮件的接收IP地址
描述	垃圾邮件信息的详细描述
发送	将该垃圾邮件发送给邮件接收者

表 14.2 垃圾邮件日志名词解释

查询垃圾邮件日志：

1. 选择需要查询的垃圾邮件通过哪种协议传播，分为 SMTP、POP3、IMAP 和全部，全部则代表包

含上述三种协议

2. 在源地址处输入进行查询的来源 IP 地址

3. 在目的地址处输入进行查询的目的 IP 地址

4. 按发件人处输入进行查询的发件人邮件地址

5. 按收件人处输入进行查询的收件人邮件地址

6. 在按时间查询处选择查询的时间范围

7. 单击【搜索】进行查询

- 垃圾邮件日志详细信息：可使用此功能查询防毒墙拦截垃圾邮件的详细信息，如图 14.5 所示

垃圾邮件日志详细信息(共有5条符合条件的记录)

序号	时间	协议	源IP	目的IP	描述	发送
1	2007-05-29 09:38:18	SMTP	193.168.20.131	193.168.20.244	发件人： ryn@ryn.com 收件人： gao@gzj.com 主 题： zzzzz	
2	2007-05-29 09:29:38	POP3	193.168.20.131	193.168.20.244	发件人： gao@gzj.com 收件人： gao@gzj.com 主 题： aaa	-
3	2007-05-29 09:23:44	POP3	193.168.20.131	193.168.20.244	发件人： gao@gzj.com 收件人： gao@gzj.com 主 题： rwerw	-
4	2007-05-29 09:18:47	POP3	193.168.20.131	193.168.20.244	发件人： gao@gzj.com 收件人： gao@gzj.com 主 题： 23233	-
5	2007-05-29 09:14:18	POP3	193.168.20.131	193.168.20.244	发件人： gao@gzj.com 收件人： gao@gzj.com 主 题： v	-

首 页 上一页 下一页 末 页 到第1 页 GO [每页10条] [当前1/1页][下载日志信息] [发送检索到的邮件]

图 14.5 垃圾邮件日志的详细信息

- 垃圾邮件统计信息：可使用此功能查询防毒墙拦截垃圾邮件统计信息，如图 14.6 所示

对指定时间范围内的分协议垃圾邮件百分比

排名	协 议	数 量	百分比
1	POP3	4	80%
2	SMTP	1	20%
3	IMAP	-	-

对指定时间范围内的源垃圾邮件TOP5

排名	源 IP	数 量	百分比
1	193.168.20.131	5	100%
2	-	-	-
3	-	-	-
4	-	-	-
5	-	-	-

对指定时间范围内的发件人垃圾邮件TOP5

排名	发件人	数 量	百分比
1	gao@gzj.com	4	80%
2	ryn@ryn.com	1	20%
3	-	-	-
4	-	-	-
5	-	-	-

对指定时间范围内的收件人垃圾邮件TOP5

排名	收件人	数 量	百分比
1	gao@gzj.com	5	100%
2	-	-	-
3	-	-	-
4	-	-	-
5	-	-	-

图 14.6 垃圾邮件日志的统计信息

14.3 隔离文件

单击【日志审计】➔【隔离文件】，进入防毒墙隔离文件日志页面。防毒墙的隔离文件日志功能可按时间、协议、源 IP、目的 IP 和文件信息对检测到的文件进行分类记录，如图 14.7 所示。

图 14.7 隔离文件日志

图 14.7 隔离文件日志详细信息各字段文字说明

字段	说明
序号	隔离文件日志的序号
时间	隔离文件日志的发生时间（以防毒墙系统时间记录）
协议	通过何种协议进行传播
源IP	发送文件的IP地址
目的IP	接收文件的IP地址
描述	隔离文件信息的详细描述
文件	文件名称
文件大小	被隔离文件数据包的大小
隔离原因	被防毒墙隔离的原因

表 14.3 隔离文件日志名词解释

查询隔离文件日志：

1. 在协议处选择病毒通过哪种协议进行传播，分为：HTTP、FTP、SMTP、POP3、MSN、IMAP 和全部，全部则代表包含上述六种协议
2. 在源地址处输入进行查询的来源 IP 地址
3. 在目的地址处输入进行查询的目的 IP 地址
4. 按发件人处输入进行查询的发件人邮件地址
5. 按收件人处输入进行查询的收件人邮件地址
6. 在按时间查询处选择查询的时间范围
7. 单击【搜索】进行查询

14.4 管理日志

单击【日志审计】➔【管理日志】，进入防毒墙管理日志页面，管理日志包含管理员对防毒墙配置的所有修改信息，每个日志条目都带有事件描述和日期时间戳。远程及本地管理接口登录失败时将被记录在管理日志中，如图 14.8 所示。

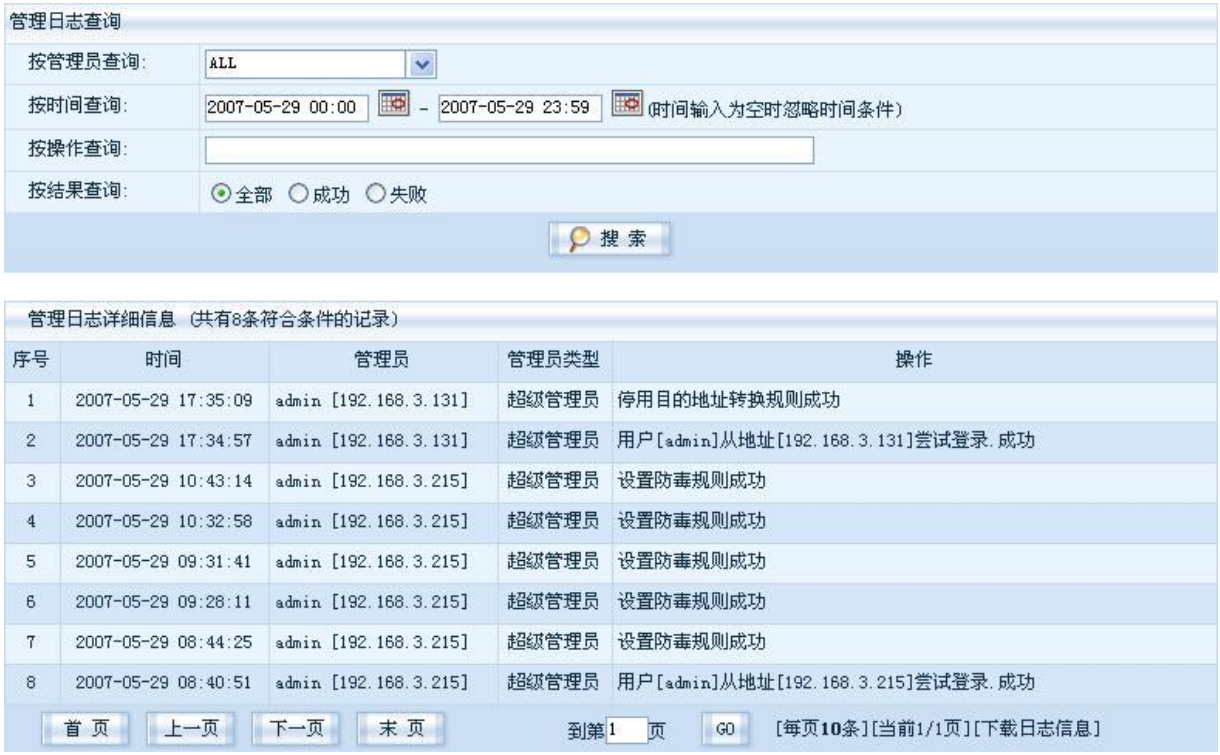


图 14.8 管理日志操作信息

字段	说明
序号	管理日志的序号
时间	管理操作的发生时间（以防毒墙系统时间记录）
管理员	管理员的名称和进行管理时使用的IP地址
管理员类型	显示当前管理员所属的管理组，不同的管理组具备不同的管理权限
操作	防毒墙管理员进行的管理操作

表 14.4 防毒墙管理日志名词解释

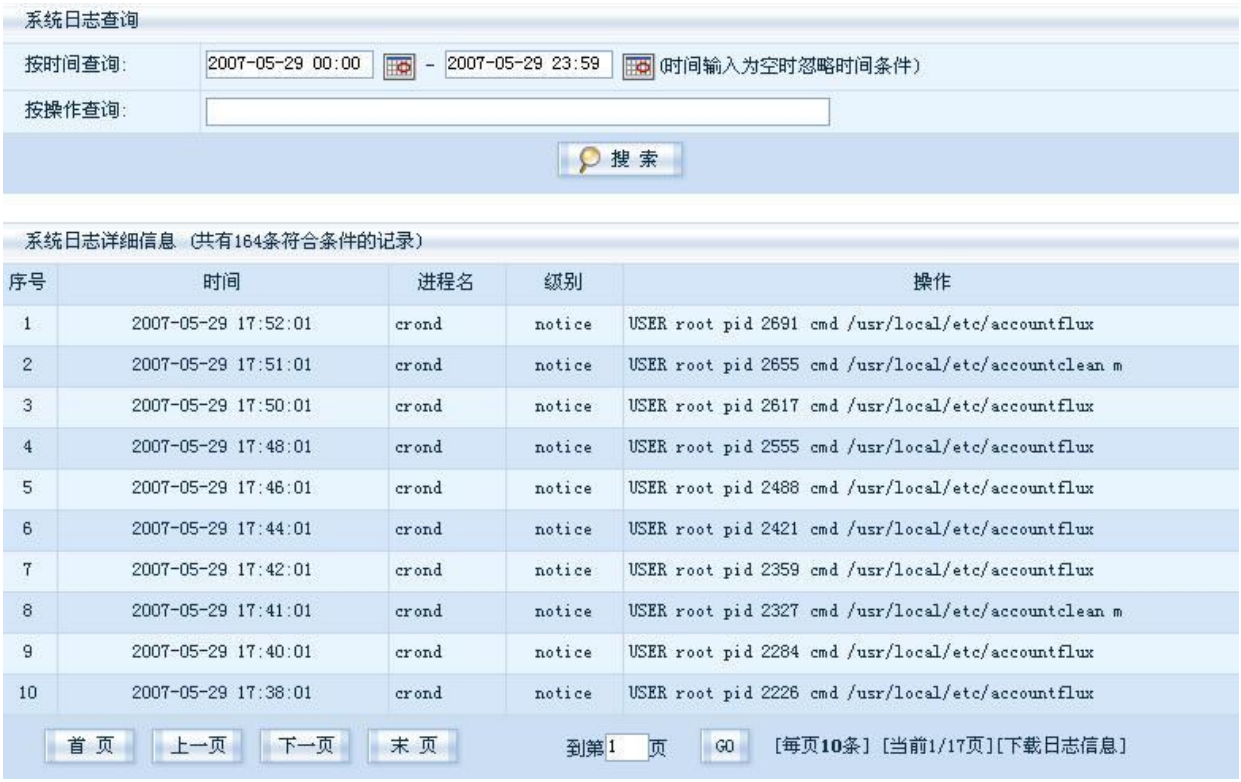
查询管理日志：

1. 在按管理员查询处选择管理员或手动输入管理员帐号，ALL 则代表选择全部的防毒墙管理员进行查询
2. 在按时间查询处选择查询的时间范围
3. 在按操作查询处输入管理员对防毒墙所进行的操作
4. 在按结果查询处选择按成功、失败或全部结果进行查询
5. 单击【搜索】进行查询

单击右下角的【下载日志信息】，系统日志将以 CSV 格式文件下载到本地计算机，供管理员日后分析。

14.5 系统日志

单击【日志审计】➔【系统日志】，进入防毒墙系统日志页面，系统日志包含任何关于瑞星防毒墙系统的操作信息。每个日志条目都带有事件描述和日期时间戳，如图 14.9 所示。



序号	时间	进程名	级别	操作
1	2007-05-29 17:52:01	crond	notice	USER root pid 2691 cmd /usr/local/etc/accountflux
2	2007-05-29 17:51:01	crond	notice	USER root pid 2655 cmd /usr/local/etc/accountclean m
3	2007-05-29 17:50:01	crond	notice	USER root pid 2617 cmd /usr/local/etc/accountflux
4	2007-05-29 17:48:01	crond	notice	USER root pid 2555 cmd /usr/local/etc/accountflux
5	2007-05-29 17:46:01	crond	notice	USER root pid 2488 cmd /usr/local/etc/accountflux
6	2007-05-29 17:44:01	crond	notice	USER root pid 2421 cmd /usr/local/etc/accountflux
7	2007-05-29 17:42:01	crond	notice	USER root pid 2359 cmd /usr/local/etc/accountflux
8	2007-05-29 17:41:01	crond	notice	USER root pid 2327 cmd /usr/local/etc/accountclean m
9	2007-05-29 17:40:01	crond	notice	USER root pid 2284 cmd /usr/local/etc/accountflux
10	2007-05-29 17:38:01	crond	notice	USER root pid 2226 cmd /usr/local/etc/accountflux

图 14.9 系统日志信息

图 14.9 系统日志各字段文字说明

字段	说明
序号	系统日志序号
时间	对防毒墙系统进行操作的发生时间（以防毒墙系统时间记录）
进程名	进行系统操作的进程名称
级别	日志的性质
操作	进行的系统操作

表 14.5 防毒墙系统日志名词解释

查询系统日志

1. 在按时间查询处选择查询的时间范围
2. 在按操作查询处输入防毒墙进行的系统操作
3. 单击【搜索】进行查询

单击右下【下载日志信息】，系统日志将以 CSV 格式文件下载到本地计算机，供管理员日后分析。

14.6 网络日志

单击【日志审计】➔【网络日志】，进入防毒墙网络日志页面。防毒墙的网络日志功能可按协议、入口、

出口、操作、规则名、源 IP、目的 IP、端口和时间进行分类查询，如图 14.10 所示。

序号	时间	协议	规则名	入口	出口	源IP	目的IP	信息
1	2007-05-29 17:53:27	TCP	a	-	E1	192.168.3.131	193.168.20.108	数据包长度:48 数据包端口:2604-443 类型：源地址转换 状态:SYN
2	2007-05-29 17:53:27	TCP	全通规则	E0	E1	192.168.3.131	193.168.20.108	数据包长度:48 数据包端口:2604-443 类型：安全策略 状态:SYN
3	2007-05-29 17:53:24	TCP	a	-	E1	192.168.3.131	193.168.20.108	数据包长度:48 数据包端口:2602-443 类型：源地址转换 状态:SYN
4	2007-05-29 17:53:24	TCP	全通规则	E0	E1	192.168.3.131	193.168.20.108	数据包长度:48 数据包端口:2602-443 类型：安全策略 状态:SYN
5	2007-05-29 17:53:18	TCP	a	-	E1	192.168.3.131	193.168.20.108	数据包长度:48 数据包端口:2601-443 类型：源地址转换 状态:SYN
6	2007-05-29 17:53:18	TCP	全通规则	E0	E1	192.168.3.131	193.168.20.108	数据包长度:48 数据包端口:2601-443 类型：安全策略 状态:SYN
7	2007-05-29 17:53:08	TCP	a	-	E1	192.168.3.131	193.168.20.108	数据包长度:48 数据包端口:2599-443 类型：源地址转换 状态:SYN
8	2007-05-29 17:53:08	TCP	全通规则	E0	E1	192.168.3.131	193.168.20.108	数据包长度:48 数据包端口:2599-443 类型：安全策略 状态:SYN

图 14.10 网络日志

图 14.10 网络日志详细信息各字段文字说明

字段	说明
序号	网络日志的序号
时间	网络日志的发生时间（以防毒墙系统时间记录）
协议	通过何种协议进行传输
规则名	该网络连接进行连接时所采用的规则
入口	该网络连接的入口
出口	该网络连接的出口
源IP	发起网络连接的IP地址
目的IP	网络连接的目的IP地址
信息	显示当前网络连接的详细信息

表 14.6 网络日志名词解释

查询网络日志：

1. 在协议处选择网络连接时采用何种协议进行连接，分为：TCP、UDP、ICMP 和全部，全部则代表包含上述三种协议

2. 在入口处选择需要查询的连接的防毒墙入口

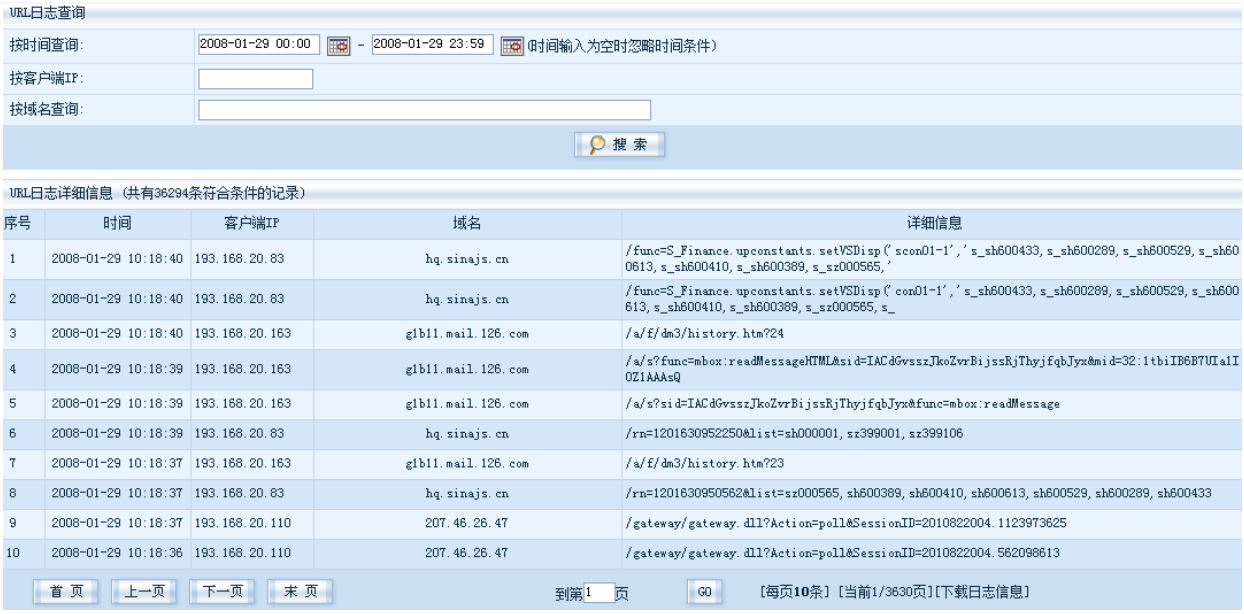
3. 在出口处选择需要查询的连接的防毒墙出口

4. 在类型处选择根据何种操作进行查询，分为安全策略、接口防御、入侵检测、源地址转换、目的地址转换和全部，全部则代表查询全部网络连接

5. 在规则名处输入进行查询自定义策略的规则名称
6. 在源地址处输入进行查询的来源 IP 地址
7. 在目的地址处输入进行查询的目的 IP 地址
8. 在端口处输入需要查询的端口范围
9. 在按时间查询处选择查询的时间范围
10. 单击【搜索】进行查询

14.7 URL 日志

单击【日志审计】➔【URL 日志】，进入防毒墙 URL 日志页面。防毒墙的 URL 日志功能可按时间、客户端 IP 和域名进行分类记录，如图 14.11 所示。


URL日志查询

按时间查询: 2008-01-29 00:00 - 2008-01-29 23:59 (时间输入为空时忽略时间条件)

按客户端IP:

按域名查询:

搜 索

URL日志详细信息 (共有36294条符合条件的记录)

序号	时间	客户端IP	域名	详细信息
1	2008-01-29 10:18:40	193.168.20.83	hq.sinajs.cn	/func=S_Finance.upconstants.setVSDisp('sconO1-1','s_sh600433,s_sh600289,s_sh600529,s_sh600613,s_sh600410,s_sh600389,s_sz000565,'
2	2008-01-29 10:18:40	193.168.20.83	hq.sinajs.cn	/func=S_Finance.upconstants.setVSDisp('conO1-1','s_sh600433,s_sh600289,s_sh600529,s_sh600613,s_sh600410,s_sh600389,s_sz000565,s_
3	2008-01-29 10:18:40	193.168.20.163	glb11.mail.126.com	/a/f/dm3/history.htm?24
4	2008-01-29 10:18:39	193.168.20.163	glb11.mail.126.com	/a/s?func=mbox:readMessageHTML&sid=IACdGvssxJkoZvrBijssRjThyjfqbJyx&mid=32:1tbiIB6B7UIalIOZ1AAAsQ
5	2008-01-29 10:18:39	193.168.20.163	glb11.mail.126.com	/a/s?sid=IACdGvssxJkoZvrBijssRjThyjfqbJyx&func=mbox:readMessage
6	2008-01-29 10:18:39	193.168.20.83	hq.sinajs.cn	/rn=1201630952250&list=sh000001,sz399001,sz399106
7	2008-01-29 10:18:37	193.168.20.163	glb11.mail.126.com	/a/f/dm3/history.htm?23
8	2008-01-29 10:18:37	193.168.20.83	hq.sinajs.cn	/rn=1201630950562&list=sz000565,sh600389,sh600410,sh600613,sh600529,sh600289,sh600433
9	2008-01-29 10:18:37	193.168.20.110	207.46.26.47	/gateway/gateway.dll?Action=poll&SessionID=2010822004.1123973625
10	2008-01-29 10:18:36	193.168.20.110	207.46.26.47	/gateway/gateway.dll?Action=poll&SessionID=2010822004.562098613

首 页 上一页 下一页 末 页 到第1页 GO [每页10条] [当前1/3630页][下载日志信息]

图 14.11 URL 日志详细信息

图 14.11 URL 日志详细信息各字段文字说明

字段	说明
序号	URL日志的序号
时间	URL日志的发生时间（以防毒墙系统时间记录）
客户端IP	发起访问请求的客户端IP
域名	客户端IP所访问的域名地址
详细信息	客户端访问该域名的详细信息

表 14.7 URL 日志名词解释

查询 URL 日志：

1. 在按时间查询处输入查询时间范围
2. 在按客户端 IP 处输入查询 IP 地址

3. 在按域名查询处输入客户端访问域名地址

4. 单击【搜索】进行查询

14.8 可疑文件

单击【日志审计】➔【可疑文件】，进入防毒墙可疑文件页面，如图 14.12 所示，当有可疑文件经过防毒墙进行传输时，防毒墙记录这些文件传输的详细信息，管理员可通过查询可疑文件日志确定网络中存在的问题。

序号	时间	客户端IP	域名	详细信息	统计次数	操作
1	2008-05-12 10:46:27	193.168.20.111	dl_dir.qq.com	/qqfile/ims/qqdoctor/tsepb.dat	86	过滤
2	2008-05-12 10:46:26	193.168.20.51	dl_dir.qq.com	/qqfile/ims/qqdoctor/tsvulchk.dat	47	过滤
3	2008-05-12 08:59:04	193.168.20.111	dl_dir.qq.com	/qqfile/ims/qqdoctor/tsengine.dat	37	过滤
4	2008-05-12 10:17:24	193.168.20.51	scdown.qq.com	/download/AddrSearch.dll	34	过滤
5	2008-05-12 11:01:44	193.168.20.27	dl.sanhaostreet.com	/Soft/multimedia/REC/dcsetup512.exe	31	过滤
6	2008-05-12 08:45:55	193.168.20.115	dl_dir.qq.com	/qqfile/ims/qqdoctor/selfupdate.exe	16	过滤
7	2008-05-12 09:12:23	193.168.20.213	www.sosodui.cn	/adshell.exe	12	过滤
8	2008-05-12 09:12:32	193.168.20.213	219.148.34.10	/dmupdate/sss.exe	6	过滤
9	2008-05-12 11:01:08	193.168.20.27	download2.5jsoft.com	/c2hznl9kfoj5jto8ug6n7yccekyzkrln/4/6/dcsetup.exe?gfgrgghrght4/6/dcsetup.exe	3	过滤
10	2008-05-12 09:08:35	193.168.20.74	1.ad8da.com.cn	/jk.exe	2	过滤

图 14.12 防毒墙可疑文件日志

图 14.12 各字段文字说明

字段	说明
序号	可疑文件日志的序号
时间	可疑文件日志的发生时间（以防毒墙系统时间记录）
客户端IP	发起访问请求的客户端IP
域名	客户端访问的详细URL地址
详细信息	客户端访问文件的详细信息
统计次数	显示客户端访问该文件的次数总和
操作	防毒墙对此次请求所进行的操作

表 14.8 可疑文件日志名词解释

查询可疑文件日志：

1. 在【活跃时间】处输入需要进行查询的时间范围，活跃时间是指可疑文件日志记录发生时间距当前查询时间的时间范围

2. 单击【搜索】进行查询，可疑文件日志会显示活跃时间范围内的日志记录

14.9 入侵日志

单击【日志审计】➔【入侵日志】，进入防毒墙入侵日志页面，如图 14.13 所示，该页面显示当前防毒

墙已经阻断的来自外部网络的攻击行为。

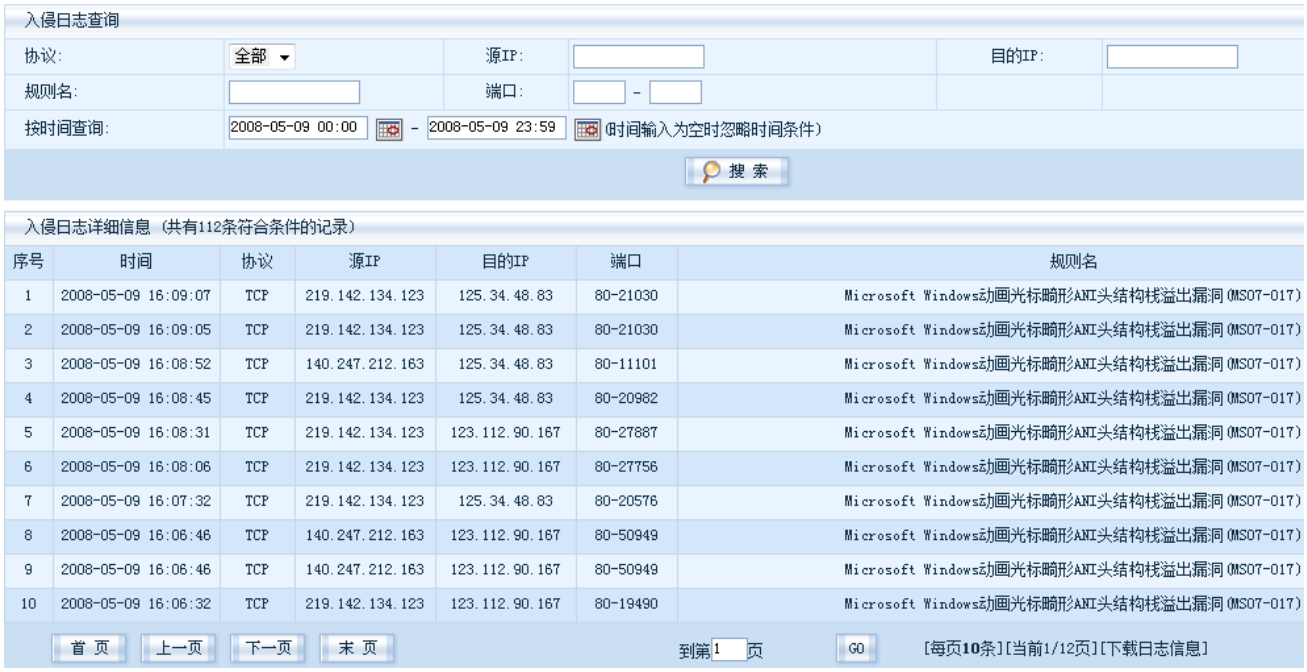


图 14.13 防毒墙入侵日志

图 14.13 各字段文字说明

字段	说明
序号	入侵日志的序号
时间	入侵日志的发生时间（以防毒墙系统时间记录）
协议	通过何种协议进行传输
源IP	发起网络连接的IP地址
目的IP	网络连接的目的IP地址
端口	源IP和目的IP所使用的端口对应情况
规则名	该攻击行为所匹配到防毒墙的入侵防御规则

表 14.9 入侵日志名词解释

查询入侵日志：

1. 在协议处选择网络连接时采用何种协议进行连接，分为：TCP、UDP、ICMP 和全部，全部则代表包含上述三种协议
2. 在源地址处输入进行查询的来源 IP 地址
3. 在目的地址处输入进行查询的目的 IP 地址
4. 在规则名处输入进行查询入侵防御的规则名称
5. 在端口处输入需要查询的端口范围
6. 在按时间查询处选择查询的时间范围
7. 单击【搜索】进行查询

14.10 告警配置

14.10.1 邮件告警

瑞星防毒墙邮件告警功能使用指定的邮件服务器发送告警邮件，定时为防毒墙管理员发送防毒墙预定义统计信息，方便管理员及时在防毒墙出现问题或即将出现问题时做出处理，保证防毒墙的正常运转。单击【日志审计】➔【告警设置】进入防毒墙邮件告警设置页面，如图 14.14 所示。

图 14.14 设置防毒墙邮件告警

1. 单击【启用】使用远程 SMTP 服务器，如图 14.15 所示

图 14.15 SMTP 服务器设置

2. 输入邮件服务器的 IP 地址或域名以及 SMTP 端口号
3. 输入发件人 Email 地址
4. 如果发送 Email 的邮件服务器需要验证，请单击【启用】用户名密码验证，如图 14.16 所示

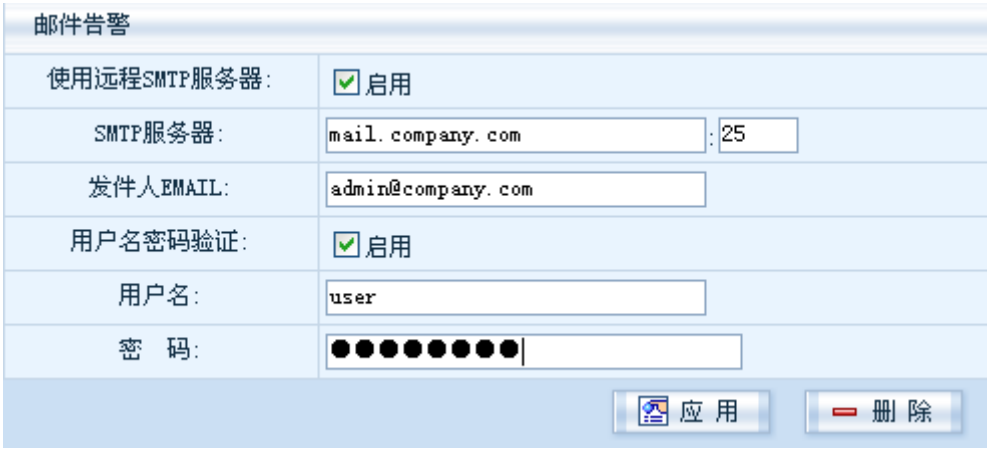


图 14.16 SMTP 用户名验证

5. 输入该邮件地址的用户名和密码供邮件服务器认证

6. 单击【应用】保存邮件告警设置

7. 如果邮件服务器不可达或用户验证失败，则弹出错误的提示，如图 14.17 所示

图 14.17 邮件告警配置失败信息

8. 如果设置成功，则弹出以下信息，如图 14.18 所示

图 14.18 邮件告警设置成功提示

14.10.2 日志配置

由于一般企业的网络流量很大，系统日志增长较快。为防止日志超出防毒墙设备容量，瑞星防毒墙允许以本地、远程 syslog 及 mysql 三种方式记录日志。防毒墙采用滚动日志机制，同时可设置日志的磁盘占用百分比，超过磁盘占用限额的日志文件将被自动删除。该功能确保防毒墙不会因磁盘空间被日志占满而导致系统崩溃。

单击【日志审计】➔【告警设置】，进入防毒墙远程日志设置页面，如图 14.19 所示。

图 14.19 远程日志

- **设置 Syslog 远程日志存储**

1. 在远程日志下启用 Syslog 日志

2. 输入远程 Syslog 日志服务器的 IP 地址和端口

3. 单击【应用】完成远程 Syslog 日志存储设置

- **设置 Mysql 远程日志存储**

1. 在远程日志下启用 Mysql 日志

2. 输入远程 Mysql 数据库服务器的 IP 地址和端口

3. 输入 Mysql 数据库服务器的用户名和密码

4. 输入 Mysql 为防毒墙建立的数据库名称

5. 单击【应用】完成远程 Mysql 日志存储设置

14.10.3 本地存储告警

用户可以选择日志在防毒墙上最多占用磁盘空间的百分比。单击【日志审计】➔【告警设置】，进入防毒墙本地日志存储设置页面，如图 14.18 所示。

图 14.20 日志保存设置

设置本地存储控制：

1. 在日志占磁盘限额处输入日志存储最多占用磁盘容量的百分比

2. 单击【应用】完成本地日志设置

APPENDIX 1 防毒墙串口管理

串口管理程序是用于防毒墙配置出现错误使系统无法正常工作时的补充手段，接通串口后将进入一个定制的 shell 环境，下面将要介绍有关的操作细节。

A1.1 登录串口

下面的步骤将指导如何将防毒墙设备与控制台进行连接。用串口线（RS-232 线）将控制台串口与防毒墙串口连接好，然后在控制台上执行终端程序。以 Windows XP 系统下的超级终端程序为例：

1. 通过以下路径打开程序：【开始】➔【所有程序】➔【附件】➔【通讯】➔【超级终端】
2. 创建一个新的连接，输入连接名称并为连接选择一个图标，单击【确定】按钮
3. 选择连接所用的接口，默认为 COM1
4. 在端口设置中选择如下属性：
   - 速率： 9600
   - 数据位： 8
   - 奇偶校验： 无
   - 停止位： 1
   - 数据流控制： 无
5. 单击【确定】按钮创建连接。此时连接已建立，单击回车键显示登录信息，如下所示：

```
Antivirus_Gateway login: _
```

6. 输入登录用户名及密码，此用户名及密码与 Web 管理界面的相同。
7. 如果用户名及密码输入无误，将显示如下信息，表示已经登录成功，可以开始进一步管理操作。

```
Antivirus_Gateway login: admin
Password:
[RsShell]$
```

A1.2 查看帮助信息

a) 查看基本系统命令

```
命令格式：?|help
```

示例：

```
[RsShell]$ ?
?           show command list
help        show command list
exit        exit shell
reset       reset to default setting.
shutdown    shutdown machine
```

```
reboot      reboot machine
time        display of set system time
showsn      show device ID and serial No.
ping        Send ICMP ECHO_REQUEST packets to network hosts
user        user administration
padmin      configure hosts who can administrate the gateway
zone        show or configure interface zone
topo        show or configue system topology
service     interface service management
vlan        VLAN interface management
ipaddr      interface IP address management
hwaddr      display hardware address of the gateway
route       static route configure
dns         configure DNS
version     display version
```

b) **查看系统命令的帮助信息**

用户可以根据相关信息进行设置操作

```
命令格式：〈基本命令〉？或 help〈基本命令〉
```

示例：

```
[RsShell]$ topo ?
topo
topo iface {BR0|BR1|DHCP|PPPOE|STATIC|DISABLE}
```

A1.3 退出串口管理

```
命令格式： exit
```

A1.4 恢复出厂默认设置

将系统恢复出厂状态

```
命令格式：reset system
```

示例：

```
[RsShell]$ reset system
Reset will lose all current setting, do you want to reset to default setting?
(y or n)
```

将系统配置恢复出厂状态

```
命令格式：reset config
```

示例：

```
[RsShell]$ reset config
Reset will lose all current setting, do you want to reset to default setting?
```

```
(y or n)
```

提示：关于恢复出厂设置

reset system 此操作将防毒墙恢复至出厂状态

reset config 此操作将防毒墙配置恢复至出厂状态，系统和病毒库版本将不会变化

A1.5 关闭防毒墙

利用串口命令关闭防毒墙系统。

```
命令格式：shutdown
```

示例：

```
[RsShell]$ shutdown
Confirm to shutdown the machine? (y or n)
```

A1.6 重启系统

利用串口命令重新启动防毒墙系统。

```
命令格式： reboot
```

示例：

```
[RsShell]$ reboot
Confirm to reboot the machine? (y or n)
```

A1.7 时间设置

a) 查看当前防毒墙系统时间设置

```
命令格式：time
```

示例：

```
[RsShell]$ time
Thu Mar 22 10:22:55 CST 2007
```

b) 系统时间设置

```
命令格式：time set <YYYY-MM-DD[_hh:mm:ss]>        (year between 1970 and 2037)
```

注意：时间年份修改只能介于 1970 年和 2037 年之间。

示例：将防毒墙系统时间设置为 2007 年 3 月 22 日 10 点 22 分 0 秒

```
[RsShell]$ time set 2007-03-22_10:22:00
```

c) 系统时间与时间服务器同步

```
命令格式：time sync <ntpserver>
```

示例：设置防毒墙系统时间与网络时间服务器 cn.pool.ntp.org 同步

```
[RsShell]$ time sync cn.pool.ntp.org
```

d) 系统时间时区设置

```
命令格式： time zone {CST|UTC}
```

示例：设置系统时间时区为 UTC

```
[RsShell]$ time zone UTC
```

A1.8 查看设备信息

```
命令格式：showsn
```

示例：

```
[RsShell]$ showsn
Device ID: V527XXXXXXXX
Serial No:XXXXXX-XXXXXX-XXXXXX-XXXXXX
Spam SN: XXXXXX-XXXXXX-XXXXXX-XXXXXX
Hardware SN: XXXXXX-XXXXXX-XXXXXX-XXXXXX
```

A1.9 Ping 命令

```
命令格式： ping <host>
```

示例：

```
[RsShell]$ ping 193.168.20.108
PING 193.168.20.108 (193.168.20.108): 56 data bytes
84 bytes from 193.168.20.108: icmp_seq=0 ttl=64 time=0.0 ms
84 bytes from 193.168.20.108: icmp_seq=1 ttl=64 time=0.0 ms
--- 193.168.20.108 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

提示：按 Ctrl+C 停止 Ping 测试。

A1.10 管理员帐号

a) 查看当前系统管理员信息

```
命令格式：user
```

示例：

```
[RsShell]$ user
admin:SUPER:0.0.0.0/0:2147483647::unlock
ccttmgmt:SUPER:127.0.0.1:2147483647::unlock
bobtian:SUPER:0.0.0.0/0:2147483647::unlock
```

b) 添加和删除管理员

```
命令格式：user {add|del} <username>
```

示例：添加用户名为 rising 的管理员

提示：串口命令下添加的管理员默认权限为超级管理员，没有登录密码和帐号的有效期限。

```
[RsShell]$ user add rising
```

示例：删除用户名为 rising 的管理员

```
[RsShell]$ user del rising
```

c) 设置管理员密码

```
命令格式：user edit <用户名> passwd <密码>
```

示例：设置用户名为 rising 的管理员密码为 123456

```
[RsShell]$ user edit rising passwd 123456
```

d) 设置管理员权限

```
命令格式：user edit <username> purview {AUDIT|SYSTEM|SUPER}
```

示例：修改用户名为 rising 的管理员权限为审计管理员

```
[RsShell]$ user edit rising purview AUDIT
```

e) 管理员锁定或解除锁定

```
命令格式：user edit <username> {lock|unlock}
```

示例：锁定用户名为 rising 的管理员

```
[RsShell]$ user edit rising lock
```

示例：解除用户名为 rising 的管理员锁定状态

```
[RsShell]$ user edit rising unlock
```

A1.11 远程管理设置

a) 查看当前允许管理访问的 IP 地址规则列表，当列表为空时表示允许任何 IP 地址访问

```
命令格式： padmin host
```

示例：

```
[RsShell]$ padmin host
  ID     Enable        Allow         Host Addr
  101    true          true          192.168.50.1
  102    true          true          192.168.50.5
```

b) 添加 IP 地址管理访问规则

命令格式： padmin host add <host-addr>

示例：添加 193.68.60.0/24 网段到管理访问规则列表。

```
[RsShell]$ padmin host add 193.168.60.0/24
```

c) 从 IP 地址管理访问规则中删除，此操作只能通过规则 ID 进行，规则 ID 可以通过上边的查看列表命令查看。

命令格式： padmin host del <规则 ID>

示例：删除 ID 为 102 的访问规则。

```
[RsShell]$ padmin host del 102
```

A1.12 接口安全区域设置

a) 查看所有接口区域类型

命令格式：zone

示例：

```
[RsShell]$ zone
E0 WAN
E1 WAN
E2 LAN
E3 LAN
```

b) 设置接口区域类型

命令格式：zone iface {WAN|LAN|DMZ}

示例：

```
[RsShell]$ zone E3 WAN
```

A1.13 查看系统拓扑和设置拓扑

a) 查看系统当前各接口工作模式

命令格式： topo

示例：

```
[RsShell]$ topo
E0 BR0
E1 BR0
```

```
E2 STATIC
E3 PPPOE
```

b) 对系统拓扑进行配置

```
命令格式： topo <接口> <工作模式>
```

示例：将 E0 设置为 PPPoE 拨号上网模式。

```
[RsShell]$ topo E0 PPPOE
```

示例：删除 E2 工作模式

```
[RsShell]$ topo E2 DISABLE
```

A1.14 服务管理

a) 查看端口服务

```
命令格式：service <iface>
```

示例：

```
[RsShell]$ service E0
ssh=false
web=false
snmp=false
ping=false
vpn=false
l2tp=false
pptp=false
```

b) 设置端口服务

```
命令格式：service <iface> {enable|disable} <service>
```

示例：设置 E3 接口提供 Web 服务

```
[RsShell]$ service E3 enable web
```

A1.15 VLAN 管理

a) 查看 vlan 信息

```
命令格式：vlan
```

示例：

```
[RsShell]$ vlan
1001 E3.2 STATIC
```

b) 增加或删除 VLAN

```
命令格式：vlan {add|del} <iface> <vlanid>
```

示例：为防毒墙 E3 接口添加 ID 为 2 的 Vlan

```
[RsShell]$ vlan add E3 2
```

c) 更改 VLAN 工作模式

```
命令格式：vlan mode <iface> <vlanid> {BR0|BR1|STATIC}
```

示例：设置 E3 接口 ID 号为 2 的 VLan 接口工作模式为网桥二

```
[RsShell]$ vlan mode E3 2 BR1
```

A1.16 接口 IP 地址

a) 查看系统当前所有接口或指定接口的 IP 地址

```
命令格式： ipaddr
```

示例：

```
[RsShell]$ ipaddr
1001 B0 1.1.1.1 255.255.255.255
1002 B1 1.1.2.1 255.255.255.255
1003 E2 193.168.20.108 255.255.255.0
```

b) 添加指定接口的 IP 地址

```
命令格式： ipaddr add <接口><IP 地址><掩码>
```

示例：将 E0 接口的 IP 地址改为 192.168.50.50，掩码为 255.255.255.0。

```
[RsShell]$ ipaddr add E0 192.168.50.50 255.255.255.0
```

c) 修改指定接口的 IP 地址

```
命令格式： ipaddr edit <接口><IP 地址><掩码>
```

示例：修改 E0 接口的 IP 地址改为 193.168.20.108，掩码为 255.255.255.0。

```
[RsShell]$ ipaddr edit E2 193.168.20.108 255.255.255.0
```

d) 删除指定接口的 IP 地址

```
命令格式： ipaddr del <接口>
```

示例：删除 E2 接口的 IP 地址。

```
[RsShell]$ ipaddr del E2
```

A1.17 查看接口硬件地址

```
命令格式：hwaddr
```

示例：

```
[RsShell]$ hwaddr
E0 00:90:fb:03:83:16
E1 00:90:fb:03:83:17
E2 00:90:fb:03:83:18
E3 00:90:fb:03:83:19
```

A1.18 静态路由设置

a) 显示当前系统静态路由表

```
命令格式： route
```

示例：

```
[RsShell]$ route
O 193.168.20.0 255.255.255.0 0.0.0.0 E2
```

b) 为指定接口添加静态路由

```
命令格式： route add <nets> <netmask> dev-out <iface>
```

示例：

```
[RsShell]$ route add 192.168.15.0 255.255.255.0 dev-out E3
```

c) 为指定网关添加静态路由

```
命令格式： route add <nets> <netmask> gateway <gateway>
```

示例：

```
[RsShell]$ route add 192.168.15.0 255.255.255.0 gateway 193.168.15.1
```

d) 删除指定接口静态路由

```
命令格式： route del <id>
```

示例：删除 ID 号为 1001 的静态路由

```
[RsShell]$ route del 1001
```

A1.19 DNS 服务器设置

a) 查看当前系统 DNS 设置

```
命令格式： dns
```

示例：

```
[RsShell]$ dns
1st DNS: 193.168.10.9
2nd DNS: 193.168.50.1
```

b) 为系统设置 DNS 服务器

```
命令格式： dns <首选 DNS 服务器> [<备用 DNS 服务器>]
```

示例：设置首选 DNS 服务器地址为 202.106.0.20，备用 DNS 服务器为 202.106.3.45。

注意：当命令中没有备用 DNS 服务器内容时，现有的备用 DNS 服务器将被删除

A1.20 查看系统版本

查看当前系统版本

```
命令格式： version
```

示例：

```
[RsShell]$ version
system_ver 2.16063
```

APPENDIX 2 专业术语表

A

安全套接层（SSL）

SSL 为 Security Sockets Layer 的缩写，是一种基于允许加密和授权的互联网通讯协议。SSL 运行于 TCP/IP 之上。

D

DoS 攻击

DoS 为 Denial of Service 的缩写。DoS 攻击是指发送大量服务请求耗尽服务器资源，使其无法响应合法用户请求的一种攻击方式。

DDoS 攻击

分布式的拒绝服务攻击手段（DDoS），是指在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般采用一对一方式的，而 DDoS 采用多对一的方式进行攻击。

DNS 查询

DNS 为 Domain Name Server 的缩写。在互联网上域名和 IP 地址是一一对应的，为了方便大家的记忆，大型的 ISP 服务器商提供专门的域名解析服务器提供相关的服务。输入一个 IP 地址将输出相应的域名，输入域名则输出相应的 IP 地址。

DDNS

Dynamic Domain Name Server 是动态域名服务的缩写，DDNS 是将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务项目器程序负责提供 DNS 服务并实现动态域名解析。

动态主机配置协议(DHCP)

DHCP 为 Dynamic Host Configuration Protocol 的缩写，是局域网内为客户端自动分配临时网络地址的配置信息协议。

F

防毒墙

防毒墙是计算机网络之间的一个屏障。所有从一个网络传输到另一个网络的数据必须通过防毒墙，在防毒墙的策略和规则允许下才可完成数据的交换。

G

跟踪路由

跟踪数据包到达目的地的路径的程序。跟踪路由发送一系列具有低存活时间的数据报，利用返回的 ICMP 超时信息判断一条路径上的路由器。

管理防毒墙

管理防毒墙是管理员用于访问瑞星防毒墙设备，进行防毒墙的系统管理。

管理信息库（MIB）

MIB 是 Management Information Base 的缩写。一个 MIB 就是一个分布式数据库，用于提供关于一台设备的信息。MIB 被用在 SNMP 接收和设置命令中。设置命令用于初始化设备上的一些操作，而接收命令用于恢复信息。

管理帐号

管理帐号提供对瑞星防毒墙管理界面不同级别的读-写访问。

J

简单网络管理协议（SNMP）

SNMP 为 Simple Network Management Protocol 的缩写，是一种通过网络监测和管理远程设备的协议。SNMP 是专门设计用于在 IP 网络管理网络节点（服务器、工作站、路由器、交换机及 HUBS 等）的一种标准协议，它是一种应用层协议。 SNMP 使网络管理员能够管理网络效能，发现并解决网络问题以及规划网络增长。通过 SNMP 接收随机消息（及事件报告）网络管理系统获知网络出现问题。

L

路由表

路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表（Routing Table），供路由选择时使用。

M

MAC-IP 绑定

MAC-IP 绑定定义了一个独一无二的网络接口卡（NIC）和一个特定的 IP 地址之间的关联。当一个 MAC-IP 绑定以后，只有通过被绑定的 MAC 地址应用相对应的 IP 才会生效。

N

NAT 模式

在 NAT 模式中，内部 IP 地址对外界是隐藏的。

内网 IP

在 NAT 模式中，分配给内网接口的 IP 地址。所有的内部主机都通过这个端口与设备连接。

P

Ping

一种用在 TCP/IP 网络中的程序，通过发出 ICMP 回复请求和等待应答，测试目标的主机是否可到达。

Q

千比特每秒（Kbps）

1Kbps 表示每秒钟 1000 比特。

缺省网关

局域网（LAN）上的一种单一 IP 地址，通过它，所有没有明确地址的信息都会进行路由。

T

Telnet 远程登录

远程终端设备的标准。Telnet 允许一个远程站点上的用户与另一个站点上的系统建立连接，用户可以像进行本地计算机操作一样控制连接上的远程计算机。

统一资源定位（URL）

一种提供信息的位置的字符串。一个 URL 以一种协议类型开始，随后是特定信息的标识符，包括到该特定目标的路径名称。例如：http://www.rising.com.cn。

透明模式

透明模式使用现存的网络设施允许瑞星防毒墙的“即插即用”功能。在透明模式中，现存的 IP 地址可以用于瑞星防毒墙设备。

W

外网 IP

在 NAT 模式中，分配给外网接口的 IP 地址。所有的外部主机都通过这个端口与设备进行连接。

网络掩码

网络掩码是一种 32 比特以小数点标记的符号，它允许路由设备区分一个 IP 地址的网络部分和主机部分。例如：255.255.255.0 代表网络掩码 11111111.11111111.11111111.00000000，这表示地址的前 24 比特为网络地址，后 8 比特为主机地址。

文件传输协议（FTP）

FTP 为 File Transfer Protocol 的缩写，即远程文件传输协议，是一个用于简化 IP 网络上系统之间文件传送的协议， 采用 FTP 协议可使 INTERNET 用户高效地从网上的 FTP 服务器下载大信息量的数据文件， 将远程主机上的文件拷贝到自己的计算机上。以达到资源共享和传递信息的目的。FTP 使用客户方的某个随机接口的 TCP，与服务方的端口 21 相连接。

Windows-Internet 名称服务器（WINS）

WINS（微软开发的域名服务系统），是 Windows Internet Name Server 的缩写，一个配置为 WINS 的服务器，可以为 Windows NetBIOS 名称提供名称注册、更新、释放和转换服务。

X

信报控制协议（ICMP）

ICMP 为 Internet Control Message Protocol（Internet 控制消息协议）的缩写。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

ping 就是 ICMP 的一个实施例。

虚拟专用网络（VPN）

VPN 为 Virtual Private Network 的缩写，是一种将专用网络的内部数据包通过公用网络传输到另一个站点的网络。由于数据包通过公共网络传输，所以使用了加密保护。为了保证接收者能够接收到数据包，对连接的两端都提供了授权。

虚拟局域网（VLAN）

VLAN（Virtual Local Area Network）又称虚拟局域网，是指在交换局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。一个 VLAN 组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。

组建 VLAN 的条件

VLAN 是建立在物理网络基础上的一种逻辑子网，因此建立 VLAN 需要相应的支持 VLAN 技术的网络设备。当网络中的不同 VLAN 间进行相互通信时，需要路由的支持，这时就需要增加路由设备。要实现路由功能，既可采用路由器，也可采用三层交换机来完成。

划分 VLAN 的基本策略，从技术角度讲，VLAN 的划分可依据不同原则，一般有以下三种划分方法：

- 基于端口的 VLAN 划分

这种划分是把一个或多个交换机上的几个端口划分一个逻辑组，这是最简单、最有效的划分方法。该方法只需网络管理员对网络设备的交换端口进行重新分配即可，不用考虑该端口所连接的设备。

- 基于 MAC 地址的 VLAN 划分

MAC 地址其实就是指网卡的标识符，每一块网卡的 MAC 地址都是唯一且固化在网卡上的。MAC 地址由 12 位 16 进制数表示，前 8 位为厂商标识，后 4 位为网卡标识。网络管理员可按 MAC 地址把一些站点划分为一个逻辑子网。

- 基于路由的 VLAN 划分

路由协议工作在网络层，相应的工作设备有路由器和路由交换机（即三层交换机）。该方式允许一个 VLAN 跨越多个交换机，或一个端口位于多个 VLAN 中。

就目前来说，对于 VLAN 的划分主要采取上述第一种和第三种方式，第二种方式为辅助性的方案。

使用 VLAN 具有以下优点：

- 控制广播风暴：一个 VLAN 就是一个逻辑广播域，通过对 VLAN 的创建，隔离了广播，缩小了广播范围，可以控制广播风暴的产生。
- 提高网络整体安全性：通过路由访问列表和 MAC 地址分配等 VLAN 划分原则，可以控制用户访问权限和逻辑网段大小，将不同用户群划分在不同 VLAN，从而提高交换式网络的整体性能和安全性。
- 网络管理简单、直观：对于交换式以太网，如果对某些用户重新进行网段分配，需要网络管理员对网络系统的物理结构重新进行调整，甚至需要追加网络设备，增大网络管理的工作量。而对于采用 VLAN 技术的网络来说，一个 VLAN 可以根据部门职能、对象组或者应用将不同地理位置的网络用户划分为一个逻辑网段。在不改动网络物理连接的情况下可以任意地将工作

站在工作组或子网之间移动。利用虚拟网络技术，大大减轻了网络管理和维护工作的负担，降低了网络维护费用。在一个交换网络中，VLAN 提供了网段和机构的弹性组合机制。

三层交换技术

传统的路由器在网络中有路由转发、防火墙、隔离广播等作用，而在一个划分了 VLAN 以后的网络中，逻辑上划分的不同网段之间通信仍然要通过路由器转发。由于在局域网上，不同 VLAN 之间的通信数据量是很大的，这样，如果路由器要对每一个数据包都路由一次，随着网络上数据量的不断增大，路由器将不堪重负，路由器将成为整个网络运行的瓶颈。

在这种情况下，出现了第三层交换技术，它是将路由技术与交换技术合二为一的技术。三层交换机在对第一个数据流进行路由后，会产生一个 MAC 地址与 IP 地址的映射表，当同样的数据流再次通过时，将根据此表直接从二层通过而不是再次路由，从而消除了路由器进行路由选择而造成网络的延迟，提高了数据包转发的效率，消除了路由器可能产生的网络瓶颈问题。可见，三层交换机集路由与交换于一身，在交换机内部实现了路由，提高了网络的整体性能。

在以三层交换机为核心的千兆网络中，为保证不同职能部门管理的方便性和安全性以及整个网络运行的稳定性，可采用 VLAN 技术进行虚拟网络划分。VLAN 子网隔离了广播风暴，对一些重要部门实施了安全保护；且当某一部门物理位置发生变化时，只需对交换机进行设置，就可以实现网络的重组，非常方便、快捷，同时节约了成本。

Y

以太网

以太网是当今现有局域网采用的最通用的通信协议标准，在以太网中，所有计算机被连接在一条同轴光缆上，采用具有冲突检测的载波感应多处访问（CSMA/CD）方法，采用竞争机制和总线拓扑结构。基本上，以太网由共享传输媒体，如双绞线电缆或同轴电缆和多端口集线器、网桥或交换机构成。

以太网上点对点协议（PPPoE），PPPoE 将以太网和点对点协议（PPP）标准结合起来，专门用于宽带调制解调器。

域名系统（DNS）

DNS 是 Domain Name System（域名系统） 的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。DNS 命名用于 Internet 等 TCP/IP 网络中，建立域名与 IP 地址一一映射的关系。

Z

兆比特每秒（Mbps）

1Mbps 表示每秒 1,000,000 字节。

中立区（DMZ）

DMZ 是 “demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”。它在内部网络和外部网络之间建立一个安全系统和非安全系统之间的缓冲区，这个网络位于企业内部和外部之间的区域内，可以有效的保护内部服务器的安全。

子网

一个单独 IP 地址的再分。子网是通过屏蔽地址中最重要的字节，只保留其中独一无二的部分完成的。

最大传输单元（MTU）

MTU 是 Maximum Transmission Unit 的缩写。意思是网络上传送的最大数据包，MTU 的单位是字节。

APPENDIX 3 攻击介绍

- SYN Flood 攻击

它利用 TCP 三次握手协议的缺陷，向目标主机发送大量的伪造源地址的 SYN 连接请求，消耗目标主机的资源，从而不能够为正常用户提供服务。

攻击原理

在 SYN Flood 攻击中，黑客机器向被攻击主机发送大量伪造源地址的 TCP SYN 报文，被攻击主机分配必要的资源，然后向源地址返回 SYN＋ACK 包，并等待源地址返回 ACK 包。由于源地址是伪造的，所以源地址永远都不会返回 ACK 报文，被攻击主机继续发送 SYN＋ACK 包，并将半连接放入端口的积压队列中，虽然一般的主机都有超时机制和默认的重传次数，但是由于端口的半连接队列的长度是有限的，如果不断的向受害主机发送大量的 TCP SYN 报文，半连接队列就会很快填满，服务器拒绝新的连接，将导致该端口无法响应其他机器进行的正常连接请求，最终使被攻击主机的资源耗尽。

解决方法

地址状态监控的解决方法是利用监控工具对网络中的有关 TCP 连接的数据包进行监控，并对监听到的数据包进行处理。处理的主要依据是连接请求的源地址。

每个源地址都有一个状态与之对应，总共有四种状态：

1) 初态：任何源地址刚开始的状态；

2) NEW 状态：第一次出现或出现多次也不能断定存在的源地址的状态；

3) GOOD 状态：断定存在的源地址所处的状态；

4) BAD 状态：源地址不存在或不可达时所处的状态。

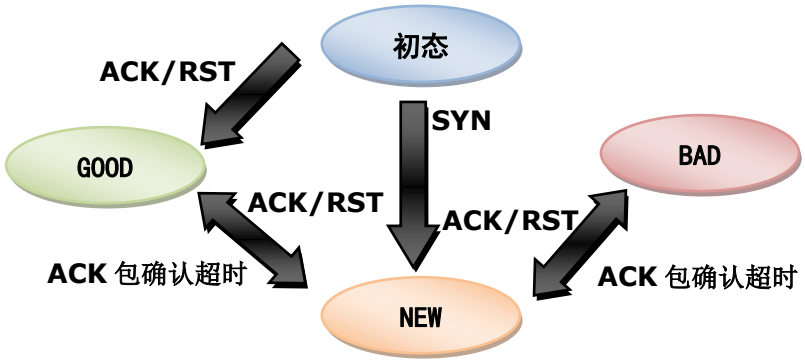
具体的动作和状态转换根据 TCP 头中的位码值决定：

1) 监听到 SYN 包，如果源地址是第一次出现，则置该源地址的状态为 NEW 状态；如果是 NEW 状态或 BAD 状态；则将该包的 RST 位置 1 然后重新发出去，如果是 GOOD 状态不作任何处理。

2) 监听到 ACK 或 RST 包，如果源地址的状态为 NEW 状态，则转为 GOOD 状态；如果是 GOOD 状态则不变；如果是 BAD 状态则转为 NEW 状态。

3) 监听到从服务器来的 SYN ACK 报文（目的地址为 addr），表明服务器已经为从 addr 发来的连接请求建立了一个半连接，为防止建立的半连接过多，向服务器发送一个 ACK 包，建立连接，同时，开始计时，如果超时，还未收到 ACK 报文，证明 addr 不可达，如果此时 addr 的状态为 GOOD 则转为 NEW 状态；如果 addr 的状态为 NEW 状态则转为 BAD 状态；如果为 addr 的状态为 BAD 状态则不变。

状态的转换图如下图所示：



附 3　Flood 攻击状态转换图

下面分析一下基于地址状态监控的方法如何能够防御 SYN Flood 攻击。

1) 对于一个伪造源地址的 SYN 报文，若源地址第一次出现，则源地址的状态为 NEW 状态，当监听到服务器的 SYN+ACK 报文，表明服务器已经为该源地址的连接请求建立了半连接。此时，监控程序代源地址发送一个 ACK 报文完成连接。这样，半连接队列中的半连接数不是很多。计时器开始计时，由于源地址是伪造的，所以不会收到 ACK 报文，超时后，监控程序发送 RST 数据包，服务器释放该连接，该源地址的状态转为 BAD 状态。之后，对于每一个来自该源地址的 SYN 报文，监控程序都会主动发送一个 RST 报文。

2) 对于一个合法的 SYN 报文，若源地址第一次出现，则源地址的状态为 NEW 状态，服务器响应请求，发送 SYN＋ACK 报文，监控程序发送 ACK 报文，连接建立完毕。之后，来自客户端的 ACK 很快会到达，该源地址的状态转为 GOOD 状态。服务器可以很好的处理重复到达的 ACK 包。

- **碎片攻击**

IP 首部有两个字节表示整个 IP 数据包的长度，所以 IP 数据包最长只能为 0xFFFF，就是 65535 字节。如果有意发送总长度超过 65535 的 IP 碎片，一些老的系统内核在处理的时候就会出现问题，导致崩溃或者拒绝服务。

APPENDIX 4 DDoS 攻击介绍

DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用更多的服务资源，从而使合法用户无法得到服务的响应。

DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的，当攻击目标 CPU 速度低、内存小或者网络带宽小等等各项性能指标不高的时候，它的效果十分明显。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了，目标对恶意攻击包的“消化能力”加强了不少，例如您的攻击软件每秒钟可以发送 3,000 个攻击包，但我的主机与网络带宽每秒钟可以处理 10,000 个攻击包，这样一来攻击就不会产生什么效果。

这时候分布式的拒绝服务攻击手段（DDoS）就应运而生了，它的攻击原理和 DoS 类似。如果说计算机与网络的处理能力加大了 10 倍，用一台攻击机来攻击不再能起作用的话，攻击者使用 10 台攻击机同时攻击呢？用 100 台呢？DDoS 就是利用更多的傀儡机来发起进攻，用多对一的攻击方式达到进攻目的。

高速广泛的 Internet 网络给大家带来了方便，也为 DDoS 攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干节点之间的连接都是以 G 为级别的，大城市之间更可以达到 2.5G 的连接速度，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以在分布在更大的范围，选择起来更灵活了。

APPENDIX 5 防毒墙产品质保服务说明

A5.1 重要提示

- 请在首次使用产品时立即进行服务激活操作。为保障正版用户的权益，服务激活前包括产品升级在内的部分产品功能将处于禁用状态；
- 服务激活之日起，产品可获得一年的保修服务。用户可通过登录瑞星网站查询产品的“超保日期”。

  “超保日期”是指产品超过保修期的时间；

  查询网址：http://reg.rising.com.cn/enterprise/hardware/index.aspx
- 请勿自行拆卸或维修产品。如产品封条破裂，保修无效，用户需自费维修；
- 无论从任何销售渠道购买产品，售后服务及相关服务业务由瑞星公司负责。

本产品质保服务说明仅适用于瑞星公司出品的网络安全硬件产品。瑞星公司对已经购买瑞星产品的最终用户提供如下产品服务。

A5.2 免费服务

A5.2.1 保修服务

服务范围：产品在保修期内发生系统故障时，为用户提供保修服务。

1. 用户需要向瑞星公司索取《产品报修单》，并详细填写其中各项内容，传真或邮件发至瑞星公司，以保证得到最及时准确的服务。
2. 用户负责将故障产品用安全方式邮寄到瑞星公司。维修完毕后，瑞星公司将产品邮寄给用户。双方各自承担邮寄所需要的费用。

3. 在产品发生故障，不能及时修复的情况下，为了尽量缩短产品中断使用的时间，用户可以向瑞星公司申请备机响应服务，具体申请事宜请联系瑞星公司。
4. 如需瑞星公司现场安装调试产品，可向瑞星公司申请现场服务，收费标准请参见“现场服务”的规定。

A5.2.2 技术咨询服务

瑞星公司为客户提供电话咨询、邮件咨询、远程调试和网站支持等服务，解决与产品相关的技术问题。如需瑞星公司现场为用户实施技术服务，请参见 A5.3.2 现场服务部分。

服务名称	服务说明
电话咨询服务	服务时间：法定工作日 9:00 – 17:30 服务电话：010-82678866-586

邮件咨询服务	瑞星公司为用户提供（7x24）小时的邮件支持，除了解答用户有关产品使用问题及技术咨询外，还会将最新的公司动态、网络安全技术、产品信息等发送给客户，使客户能够掌握最新的网络安全信息和产品的相关情况。 电子邮件：safety@rising.com.cn
远程调试服务	通过远程调试的方式解决用户产品问题，协助用户进行产品部署和调试，保证用户产品正常使用。 **注意：用户网络需要具备远程调试所需条件。**
网站服务	用户可以登录瑞星网站 http://www.rising.com.cn ，获得同版本软件的升级程序以及与产品相关的各项信息。

表 A5.1 瑞星提供的免费技术咨询服务

A5.2.3 病毒代码升级服务

服务范围：本服务仅适用于瑞星防毒墙和瑞星网络安全预警系统系列产品。如无特殊说明和协议约定，瑞星公司对以上产品均提供一年免费病毒代码升级服务。

瑞星公司为用户提供每周至少一次的病毒代码升级。用户可以采用智能或者手动的升级方式更新病毒代码。

病毒代码升级服务不包括产品功能模块升级、扩展和硬件平台的升级。有关产品功能模块升级、扩展和硬件平台升级请参见“A5.3.4 产品升级服务”部分。

A5.2.4 服务激活

请在首次使用产品时立即进行服务激活操作。为保障正版用户的权益，服务激活前包括产品升级在内的部分产品功能将处于禁用状态。完成服务激活的用户将会取得登录瑞星网站下载升级文件所必需的用户ID，同时还可以登录瑞星网站查询和修改相关的用户信息。

项目	地址
服务激活	http://reg.rising.com.cn/enterprise/hardware/hdregindex.aspx
用户产品信息查询	http://reg.rising.com.cn/enterprise/hardware/index.aspx

表 A5.2 产品激活以及用户信息查询地址

提示：服务激活过程请准确填写用户信息。

A5.3 有偿服务

A5.3.1 维修服务

服务范围：保修期内产品发生的非系统故障或超出保修期的产品故障，瑞星公司为用户提供有偿维修服务。

- 用户需要向瑞星公司索取《产品报修单》，并详细填写其中各项内容，传真或邮件发至瑞星公司，以保证得到最及时准确的服务；
- 用户负责将故障产品以安全方式邮寄到瑞星公司。维修完毕后，瑞星公司将产品邮寄给用户。双

方各自承担邮寄所需要的费用；

- 为了尽量缩短产品中断使用的时间，用户可以向瑞星公司申请备机响应服务，具体申请事宜请联系瑞星公司；
- 维修完毕如需瑞星公司现场安装调试产品，可向瑞星公司申请现场服务，收费标准请参见“现场服务”的规定：
  - 维修服务费标准：1000 元/台·次；
  - 更换硬件收费标准：瑞星收取硬件成本费用；

A5.3.2 现场服务

用户购买瑞星产品后，如需提供现场安装、调试及培训服务，可联系瑞星公司进行申请。现场服务收费标准：（瑞星产品市场价格*5%）/次。瑞星公司可向用户提供的现场服务包括：

- 将瑞星产品部署在用户指定的网络位置；
- 依据用户提供的安全策略，为用户配置瑞星产品；
- 现场调试解决产品问题，将瑞星产品恢复到正常使用状态；
- 现场对用户进行培训，内容由用户与瑞星公司协商决定；

A5.3.3 备机响应服务

用户购买瑞星产品时，可同时选择购买瑞星公司提供的备机响应服务。也可以在产品报修过程中向瑞星公司申请备机响应服务。

- 在保修期内的用户，每次备机服务的费用为产品实际购买价格的 5%，如不能提供购机发票，则以产品报价为计算依据即（市场报价*5%）；
- 超过保修期的用户，每次备机服务的费用为产品实际购买价格的 10%，如不能提供购机发票，则以产品报价为计算依据即（市场报价*10%）；

A5.3.4 产品升级服务

产品升级服务是指软件功能模块的升级、扩展和硬件平台升级，不包括病毒代码升级。

1. 如果用户需要瑞星公司提供产品升级服务，需向瑞星公司支付相应的软件升级费用或硬件升级费用。
   - 软件模块升级、扩展收费标准：按瑞星公司提供的价格为准。
   - 硬件升级收费标准：按更换时瑞星公司提供的价格为准。
2. 为保证升级的稳定和完整，用户需要将产品以安全方式邮寄到瑞星公司。升级完毕后，瑞星公司将产品邮寄给用户。双方各自承担邮寄所需要的费用。

注意：建议用产品原包装进行产品运输，瑞星不承担运输过程造成的产品

A5.4 服务标准

A5.4.1 产品服务期约定

- 产品服务期是指瑞星对产品提供无偿或有偿技术支持、产品升级、产品维修、硬件更新等相关服务的时间周期；
- 瑞星为新购产品提供的可服务期不少于一年。无法维修的产品，瑞星将为用户提供产品更换方案；

A5.4.2 保修日期

- 申请产品维修之日未超过“超保日期”为保修日期范围内。对于无法确定“超保日期”的产品瑞星公司将从出厂日期开始计算保修期，保修期为 1 年；
- 因产品标识不清而无法确定产品型号、保修属性等信息的产品均按照超出保修期处理，用户需要自费进行维修；

提示：“超保日期”见瑞星网络安全硬件产品信息卡。

A5.4.3 产品故障界定

瑞星产品故障包括系统故障和非系统故障，分别定义如下：

故障类型	说明
系统故障	即瑞星产品主机（包括硬件、软件，不包括附件如串口线、网线等产品）发生的故障。
非系统故障	由以下原因造成的瑞星产品故障属于非系统故障： ● 使用不当：指用户误操作或违反产品使用手册说明进行安装、使用等操作时造成的故障； ● 保管不当：指用户在日常使用中保管、维护不当造成的产品故障，如因电压不稳、受潮或遭受碰撞等原因造成的故障； ● 自行维修：指用户未经瑞星公司许可，自行拆卸、修理产品所造成的故障； ● 不可抗力：指由用户不能预见，对其发生和后果不能避免并且不能克服的事件造成的故障，如：雷击、地震、火灾等； ● 过度使用：指用户超过产品性能参数进行超负荷使用而造成的故障。

表 A5.3 瑞星产品故障界定

A5.4.4 维修更换部件质保约定

- 瑞星公司对保修范围外的收费维修零部件提供三个月的质量保证；
- 被更换零部件所有权属于瑞星公司；

A5.5 产品返厂维修注意事项

- 用户需要自行邮寄产品，切勿委托他人或其他公司进行邮寄；

- 产品维修返厂邮寄需使用发货方付款方式邮寄，用户与瑞星公司分别支付单程邮寄费用；
- 强烈建议使用原厂包装箱对返厂维修产品进行包装和邮寄，以免运输途中出现损坏；
- 产品维修完成后，瑞星公司将使用用户邮寄时所使用的包装箱进行回寄；
- 瑞星公司不承担运输途中导致的硬件丢失、损坏等相关责任。

APPENDIX6 常见问题解答

A6.1 Web 管理

Q：瑞星防毒墙 Web 管理对浏览器的要求？

A：瑞星建议用户使用 Internet Explorer 6.0 / Netscape 7.1 / Firefox 1.0 或相应更高版本的浏览器，且显示器分辨率大于等于 800*600。

Q：瑞星防毒墙默认的管理员用户名和密码是什么？

A：瑞星防毒墙提供了一个默认的超级管理员帐号，其默认的用户名和密码都是：admin。

Q：为什么我不能登录 Web 管理界面？

A：请确认是否存在以下几个问题：

- 确认网络通讯正常；
- 确认浏览器为 Internet Explorer 6.0 / Netscape 7.1 / Firefox 1.0 或相应更高的版本；
- 接受 Cookie；
- 采用 https://[管理接口 IP 地址]进行访问；

Q：可以限制用来管理防毒墙的 IP 地址吗？

A：可以。单击【管理配置】➔【帐号配置】，您可以通过修改一个已经存在帐号可使用的管理地址段或添加一个新帐号时限制其可以使用的地址段，有效的控制管理防毒墙系统的用户使用的 IP 地址。

A6.2 网络设置

Q：瑞星防毒墙默认的接口配置是什么？

A：瑞星根据不同的防毒墙型号对防毒墙的接口作了默认配置，如表 A6.1、表 A6.2 所示：

接口	所属区域	接口模式	IP 地址
E0	WAN	网桥 1（br0）	1.1.1.1 / 32
E1	LAN	网桥 1（br0）	
E2	DMZ	静态 IP（Static）	192.168.100.244 / 24
E3	LAN	静态 IP（Static）	192.168.2.1 / 24
默认 DNS	202.106.0.20		

表 A6.1 RSW-1200/3200 的默认接口配置

接口	所属区域	接口模式	IP 地址
E0	WAN	网桥 1（br0）	1.1.1.1 / 32
E1	LAN	网桥 1（br0）	
E2	WAN	网桥 2（br1）	1.1.2.1 / 32
E3	DMZ	网桥 2（br1）	
E4		禁用（Disable）	
E5		禁用（Disable）	

E6	DMZ	静态 IP（Static）	192.168.100.244 / 24
E7	LAN	静态 IP（Static）	192.168.2.1 / 24
默认 DNS	202.106.0.20		

表 A6.2 RSW-9200 的默认接口配置

接口	所属区域	接口模式	IP 地址
E0	WAN	网桥 1（br0）	1.1.1.1 / 32
E1	LAN	网桥 1（br0）	
E2	WAN	网桥 2（br1）	1.1.2.1 / 32
E3	DMZ	网桥 2（br1）	
E4	LAN	禁用（Disable）	
E5	LAN	禁用（Disable）	
E6	LAN	禁用（Disable）	
E7	LAN	禁用（Disable）	
E8	LAN	静态 IP（Static）	192.168.100.244 / 24
E9	LAN	静态 IP（Static）	192.168.2.1 / 24
默认 DNS	202.106.0.20		

表 A6.3 RSW-9300 的默认接口配置

Q：瑞星防毒墙的网络接口可提供什么功能？

A：通过长时间的积累，瑞星把企业的网络按照功能和属性划分为不同的区域，分别是：WAN 区、DMZ 区和 LAN 区；提供四种接口工作模式：网桥、静态 IP、DHCP 和 PPPoE；防毒墙各个网口都可通过设置网络接口的工作区域和工作模式满足企业的各种需求。

如果您使用 RSW-1200/3200 的默认配置。则您可以把 E0 连接到 Internet，E1 连接到您的网络，E2 连接到您的 DMZ 区域，而 E3 是您的防毒墙的管理口。

Q：在连接防毒墙时应该用什么样的网线？

A：当您使用 PC 直接连接防毒墙时，请使用交叉线；如果把防毒墙连接到集线器、交换机、路由器时，请使用直连线。

Q：应该怎样设置防毒墙的物理接口？

A：瑞星防毒墙提供了两种设置防毒墙 IP 地址的方法：

- 通过超级终端，使用 ipaddr 命令设置网络参数，具体参见《瑞星防毒墙使用手册》中附录部分关于串口命令行的描述。当您无法登录 Web 管理界面的时候，可以使用该方法修改防毒墙的接口地址；
- 可以通过防毒墙的 Web 界面来修改，单击【网络配置】➔【接口配置】，在“接口模式及区域配置”页面，修改防毒墙的网口配置；

Q：用户应该把防毒墙部署在网络中的什么位置呢？

A：如果您的局域网在安装瑞星防毒墙前部署过防火墙，您可以将瑞星防毒墙部署在您的防火墙后面；如果您的网络中没有防火墙，您可以把瑞星防毒墙安装在二层和三层设备之间，这样防毒墙可以检测进出网络的所有数据流。如图 A6.1 所示：

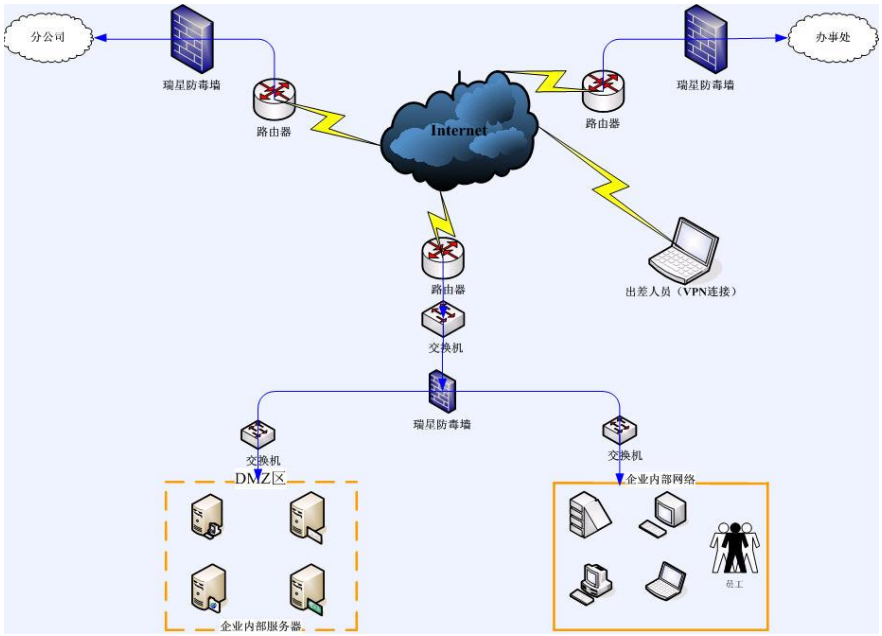


图 A6.1 瑞星防毒墙网络部署图

Q：目前我们的网络中存在其他网络安全设备，部署防毒墙时需要更改设置吗？

A：不需要。瑞星防毒墙支持透明模式，可在不更改任何网络设置的情况下正常工作。

Q：可以把瑞星防毒墙放置在通过交换机互相通讯的两个 VLAN 之间吗？

A：可以。瑞星防毒墙可以通过交换机的 Trunk 口进行 VLAN 之间的路由。

Q：我什么时候需要使用瑞星防毒墙的串口命令功能？

A：当您因为一些误操作导致无法登录防毒墙的 Web 管理页面时，您可以通过登录串口控制台来修改防毒墙的配置。另外，当防毒墙发生一些故障的时候，串口命令可以帮助您排除故障。

Q：可以在防毒墙上设定各个网络接口的工作模式或工作区域吗？

A：可以。在瑞星防毒墙中，用户可以从两方面来设定一个网口，一个是网口的工作模式；另一个是网口的工作区域。目前，瑞星防毒墙的网口支持透明、PPPoE、静态 IP、DHCP 以及禁用等工作模式。而网口的工作区则可分为：WAN（外网）、DMZ（中立区）以及 LAN（局域网）。

Q：防毒墙的网口工作模式是如何定义的？

网口的工作模式	说明
网桥 1	用户可以选定一对防毒墙接口作为一个网桥，不需要任何其他配置就可以让防毒墙工作。当用户在不想改变现有网络拓扑结构的前提下使用防毒墙的各种功能时，可以选择该模式。防毒墙的这种工作模式也被称为“透明模式”。
网桥 2	防毒墙内置了两个独立的网桥。功能同“网桥 1”。
PPPoE	当用户通过 ADSL 连接到 Internet 时，可以把防毒墙的一个接口设置成 PPPoE 模式并将该接口与 ADSL modem 连接，这样防毒墙的其他网口可以通过防毒墙的地址转换服务与 Internet 进行连接。
静态 IP	为防毒墙的网口配置一个静态的 IP。当用户需要： ● 通过该网口管理防毒墙；

	● 通过该网口提供网络服务（DHCP / NAT 等）时，需要把网口的工作模式设定成静态 IP 模式。这种工作模式也被称为“路由模式”；
DHCP	如果防毒墙的接口位于一个通过 DHCP 自动分配地址的网络中，可以把该接口配置成 DHCP 模式，让防毒墙自动获得 IP 地址，避免 IP 地址冲突（注：不要和防毒墙提供的 DHCP 服务混淆）。
禁用	如果不想使用防毒墙的某个接口，可以选择最后一项，禁用该接口

表 A6.4 防毒墙工作模式说明

Q：防毒墙的接口工作区域的含义是什么？这些区域的差别是什么？

A：处在不同区域的接口可以提供的服务是不一样的。

网口的工作区域	说明
WAN	直接和 Internet 连接的网口，也被称为“外网口”。
LAN	和企业内部局域网相连的网口，也被称为“内网口”。
DMZ	如果企业有对外提供公开服务的服务器主机（如企业的 web 服务器、ftp 服务器、邮件服务器等），为了安全考虑，应该把他们与其它不提供对外服务的主机分开。连接这些对外提供服务的主机构成的网络的网口，称为 DMZ。

表 A6.5 防毒墙工作区域说明

Q：我已经购买了瑞星网络版杀毒软件，为什么还需要防毒墙？

A：根据目前瑞星对病毒发展的统计和研究，目前几乎所有有破坏性的病毒是通过互联网进行传播的。基于这个现状，瑞星推出了网关型防病毒产品，其目的是在网络边缘将病毒拦截在企业内部网络之外。与网络版防病毒软件相比，瑞星安全网关类产品具有以下优点：

- 将病毒拦截在企业网路之外，不会让病毒进入内部网络后再处理；
- 采用专用的硬件设备，不会占用服务器或桌面 PC 机的资源；
- 管理简便，只需要对网关设备进行管理即可；
- 升级方便，能够及时地、自动地更新最新的病毒特征库，保证对最新病毒的防范。而不象网络版防病毒软件需要很复杂地通过管理软件对桌面 PC 和服务器进行更新；
- 特征库升级不会对企业网络带宽造成影响，特别是在用户数多的网络。

Q：什么样的产品适合我？

A：请参考表 A6.5

防毒墙	适用的规模
RSW-1200	200 用户以下
RSW-3200	500 用户以下
RSW-9200	1500 用户以下
RSW-9300	3000 用户以下

表 A6.6 防毒墙适用规模说明

Q：我的网络中部署有 Cisco 的 PIX 防火墙，部署上防毒墙后，防毒墙工作不正常，如何解决。

A：防毒墙和 PIX 系列防火墙有可能存在兼容性问题，为了解决该问题，请单击【系统管理】➔【TCP/IP 选项】，在“TCP/IP 选项”页面选择“高级设置”，选中“关闭 TCP window scaling”和“关闭 TCP SACK 校验”前面的复选框，单击【应用】按钮。

A6.3 病毒扫描

Q：我在防毒配置中进行了相关的杀毒设置，为什么防毒墙不杀毒呢？

A：请在【防火墙】➔【内容过滤规则】中添加相应的内容过滤规则，防毒配置中定义的只是引擎的行为。

Q：瑞星防毒墙支持哪几种协议的病毒查杀？

A：瑞星防毒墙支持 HTTP、SMTP、POP3、FTP、IMAP 以及 MSN 协议的病毒查杀。用户可以根据需要定制查杀数据的大小、文件类型、查杀方式等内容。

Q：瑞星防毒墙可以查杀多少种病毒？

A：瑞星防毒墙使用了最新的杀毒引擎，截止到 2008 年 4 月，可以查杀 70 万种以上的病毒。

Q：由于所有的数据都会经过防毒墙，那么瑞星防毒墙会影响我的上网体验吗？

A：一般情况下不会。为了让用户获得良好的用户体验，瑞星防毒墙对 HTTP 协议进行了特殊的优化处理。在用户通过 HTTP 协议获取数据时，防毒墙会边向用户发送数据边对数据进行缓存，直到在用户完整接收到最后一个数据包的时候，防毒墙会暂时不向用户转发数据而对数据进行还原检查，当防毒墙发现病毒时，就不会将最后一个数据包转发给用户，因此避免了用户收到病毒的威胁。只有当防毒墙检查确认无毒后，才将最后一个数据包发送给用户。这一般不会影响您的上网体验，您在下载文件的时候会偶尔出现在 99% 的时候停顿一下，这属于正常现象。

Q：瑞星防毒墙发现病毒后，会采取哪些处理方式？

A：目前瑞星防毒墙支持两种方式的病毒处理：

- 查毒：只在防毒墙病毒日志中记录，而不进行任何操作，无法消除病毒给您的网络带来的潜在威胁；
- 杀毒或阻断：防毒墙对所有支持的协议传输的文件进行病毒查杀，如果检测到文件中包含病毒，如果防病毒引擎能够查杀的，则进行杀毒操作；如果不能进行查杀，则阻断文件进入网络；

Q：防毒墙默认的杀毒文件的大小是多少，对于超过这个大小的文件如何处理？

A：考虑到用户实际使用的体验，瑞星防毒墙查杀文件的大小默认设定成 2 MB，用户可以对默认的杀毒文件大小进行修改。对于超过这个大小的文件，防毒墙不会阻断文件的传输，而是让它正常通过防毒墙。

Q：防毒墙是否可以正常处理被压缩的文件？

A：可以，防毒墙对于被压缩的文件，只要它的层数不超过 100 层，就可以正常的处理；如果层数超过 100 层，则无法处理。防毒墙默认可以处理 5 层压缩。

Q：防毒墙可以识别被加壳的病毒吗？

A：可以，最新的瑞星杀毒引擎集成了虚拟脱壳技术，可以有效的识别加壳的病毒。

Q:防毒墙是如何判断文件类型的？

A：防毒墙首先会依据文件内容进行文件格式识别，对于无法进行文件格式识别的文件，则按照扩展名进行

识别。

Q：防毒墙是否扫描加密文件？

A：防毒墙无法对加密的文件进行查杀。

Q：如何处理加密邮件？

A：防毒墙不会扫描加密的邮件。

A6.4 关于日志

Q：防毒墙支持远程日志吗？

A：支持。防毒墙支持 syslog 和 mysql 远程日志，瑞星建议您备份日志到远程服务器上。

Q：我们需要做什么设定，系统才会自动发送 Log 文件？

A：用户无须做任何设定，系统就会将日志记录在硬盘的相应 Log 文件中，并在管理界面上显示实时的 log 信息。但用户可以设定其占用硬盘限额的百分比，日志共有如下几种：病毒日志、垃圾邮件日志、隔离文件日志、管理日志、系统日志及网络日志。

Q：系统如何处理超过设定空间的日志文件？

A:对于超过设定空间的日志，防毒墙采用日志回滚机制，即以最新的日志来替换最旧的日志。

A6.5 关于升级

Q：防毒墙的升级服务都有哪些？

A：防毒墙的升级服务由系统升级和病毒库升级两部分组成。

Q：为什么要进行系统升级和病毒库更新？

A：防毒墙系统自身 bug 的修复以及新功能的添加都是通过系统升级完成的。而为了保证您的防毒墙能够查杀当前最流行的病毒，您需要定期的对防毒墙的病毒库进行更新。

Q：我可以通过哪些方式对防毒墙进行升级？

A：对于系统升级，您只能通过您的用户 ID 到瑞星网站上下载手动升级包，在防毒墙的本地进行升级，而且为了使您的系统升级生效，您需要重新启动防毒墙，这可能会给您的网络带来 1 分钟左右的中断。对于病毒库升级，防毒墙支持以下几种升级方式：

- 网站升级：防毒墙会自动连接到瑞星网站下载病毒库，这是最简单的升级方式；
- 局域网升级：如果您的防毒墙无法连接互联网，您可以把病毒库下载到本地的 HTTP 服务器，通过本地 HTTP 服务器进行升级；
- 本地升级：直接把病毒库升级包下载到管理 PC 上进行升级；

无论您采用上述哪种升级方式，病毒库升级都不需要您重新启动防毒墙。

Q：如何知道系统已经升级成功？

A：系统升级或病毒库升级成功后，会在 Web 管理页面上显示当前的防毒墙系统和病毒库软件版本。

Q：为什么我的防毒墙不能升级？

A：如果您购买的防毒墙不能正常升级，请检查以下设置：

- 检查防毒墙网络设置是否正确，包括：IP 地址、子网掩码、网关等信息；
- 确认您已经成功在瑞星网站上注册您的产品；
- 确认您的产品在瑞星产品服务期内；
- 确认升级服务器上有最新的升级程序；

Q：瑞星公司一般多长时间升级一次病毒库？

A：防毒墙的病毒库每天都会进行更新。如果网上爆发了某种恶意病毒，公司的病毒紧急处理小组会在最短的时间内发布病毒特征码。

A6.6 关于协议

Q：瑞星防毒墙支持那些协议的病毒查杀？

A：瑞星防毒墙支持以下协议的病毒查杀

瑞星防毒墙进行病毒查杀的各种协议默认值	
SMTP	SMTP 协议的预设扫描端口是 25
POP3	POP3 协议的预设扫描端口是 110
HTTP	HTTP 协议的预设扫描端口是 80
FTP	FTP 协议的预设扫描端口是 21
IMAP	IMAP 协议的预设扫描端口是 143
MSN	MSN 协议的预设扫描端口是 1863

表 A6.7 防毒墙支持病毒查杀的协议

Q：如果我通过 Web 来接收邮件，防毒墙能否检查出病毒？

A：可以。

Q：通过断点续传的方式下载带毒文件，防毒墙是否会对其进行病毒扫描？

A：只要下载文件的大小在防毒墙杀毒文件大小的范围以内，防毒墙就会进行病毒查杀，而与下载方式无关。

A6.7 垃圾邮件

Q：如何使用防毒墙黑白名单功能？

A：防毒墙支持对垃圾邮件的过滤，用户可以进入防毒墙垃圾邮件判定功能菜单中，选择是否启用发件人白名单、发件人黑名单、标题中的关键字等方式来过滤垃圾邮件，用户只需在相应的区域内填写过滤信息，防毒墙即可按照您所设定的过滤策略对垃圾邮件进行过滤。

Q：瑞星防毒墙的反垃圾邮件功能支持过滤图片垃圾邮件吗？

A：支持。

Q：瑞星防毒墙的反垃圾邮件误报率和准确率有多少？

A：瑞星防毒墙垃圾邮件的误报率低于 0.1%；准确率高于 90%。

APPENDIX7 服务联系方式

公司名称：北京瑞星信息技术有限公司

通讯地址：北京市中关村大街 22 号 • 中科大厦 1305 室

邮政编码：100190

服务电话：+86-10-82678866-586

电子邮件：safety@rising.com.cn

公司网址：http://www.rising.com.cn