瑞星 RSW-320 防毒墙用户手册

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

2009 年 4 月

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 2.21698 编写，适用于瑞星 RSW-320 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

2009 年 4 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 8000 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

第一章 前言

产品简介

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、防火和 VPN 等功能的综合安全网关产品。瑞星防毒墙 RSW-320 根据小型企业的实际需求量身定做，其功能强大部署简单并且易用性更强。关于本产品的更多信息，请访问：http://hardware.rising.com.cn。

目标读者

企业网络管理员和企业网络规划的决策人员。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。

本文约定

单击	本手册中“单击”指单击鼠标左键
病毒	本手册中“计算机病毒”简称为“病毒”
注意	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	“提示”则为一些帮助用户管理和使用防毒墙的经验
系统提示	为了帮助用户使用防毒墙，系统将对容易出现错误的功能点增加提示，用户可通过将鼠标悬停在对话框或功能点上进行查看
【】	带“【】”表示防毒墙按钮名称，如“单击【确定】按钮”
➔	简单的操作步骤用➔连接，如“请单击【上网控制】➔【连接管理】按钮”
	显示当前配置的详细信息，文档中简称扩展图标
	隐藏当前配置的详细信息，文档中简称隐藏图标
	修改相应配置或策略的设置，文档中简称设置图标
	删除防毒墙某功能的一条或多条策略，文档中简称删除图标
	修改或是设置防毒墙的某条规则，文档中简称修改图标
	展开该配置的详细信息，文档中简称展开图标
	最小化该配置的详细信息，文档中简称收缩图标
	执行 MAC 绑定，文档中简称绑定图标
	解除 MAC 绑定，文档中简称解除绑定图标

第二章 准备工作

安装瑞星防毒墙之前应做好以下两项准备工作：

- 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

2.1 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。如图 2.1 所示，这是目前大多数企业采取的网络拓扑结构。

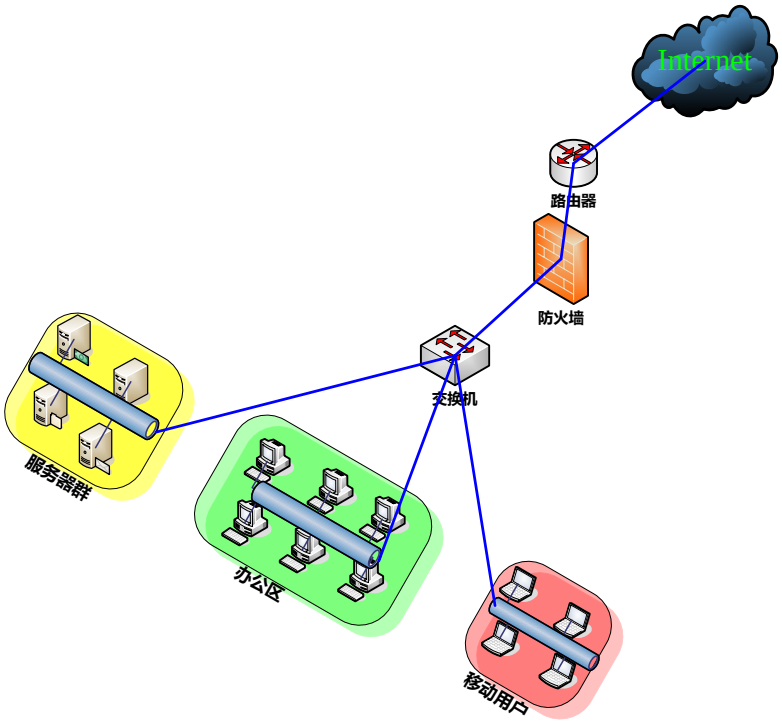


图 2.1 中小企业网络拓扑图

在未部署防毒墙前，各个网络相互之间可以无限制的访问，病毒、攻击和恶意网络资源的使用充斥着企业内部网络，给正常业务的开展带来很大的阻碍。瑞星 RSW-320 防毒墙是针对中小企业网络安全需求而开发的一款网关防毒设备。它可以根据企业实际需要以不同的方式接入企业网络，保障企业网络安全。

瑞星防毒墙有两种工作模式：宽带模式和透明模式。当企业购买瑞星 RSW-320 防毒墙后，根据使用网络设备和外部接入方式的不同，采用防毒墙部署的方式略有差异。

防毒墙默认工作模式为宽带模式，又称“路由模式”，这种方式可扩展性强，并且可以随着企业网络需求的放大而进行适当的网路扩充。例如：某个企业在购买防毒墙后，因企业业务量的迅猛增长需要对网络进行适当的扩充，当企业需要其它 ISP 运营商的接入服务或无法增大当前接入带宽时，可以在防毒墙的其他外网口增加新的链路满足企业的需要。宽带模式下的网络拓扑如图 2.2 所示。

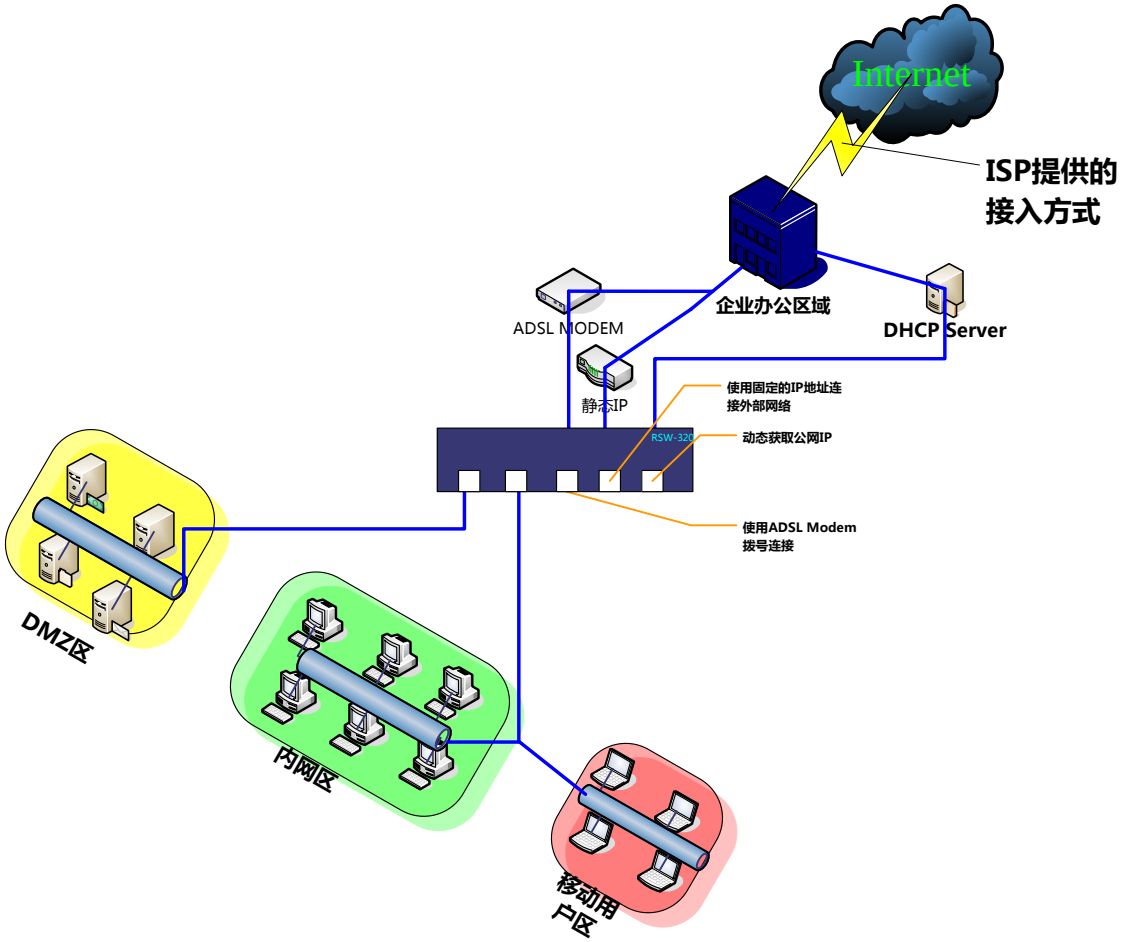


图 2.2 防毒墙宽带模式部署

在透明模式下，用户可以选定一对防毒墙接口作为一个网桥，根据企业的需求和实际情况制定防毒墙的杀毒和安全策略规则后，防毒墙就可以正常工作。防毒墙的透明模式适用于企业在网络设备比较充足的情况下进行快速部署。透明模式又称“网桥模式”，这种模式下防毒墙对数据包不进行任何更改而直接转发，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。此时防毒墙除了查杀病毒的功能外，在物理连接上就相当于一根网线。透明模式下的网络拓扑如图 2.3 所示。

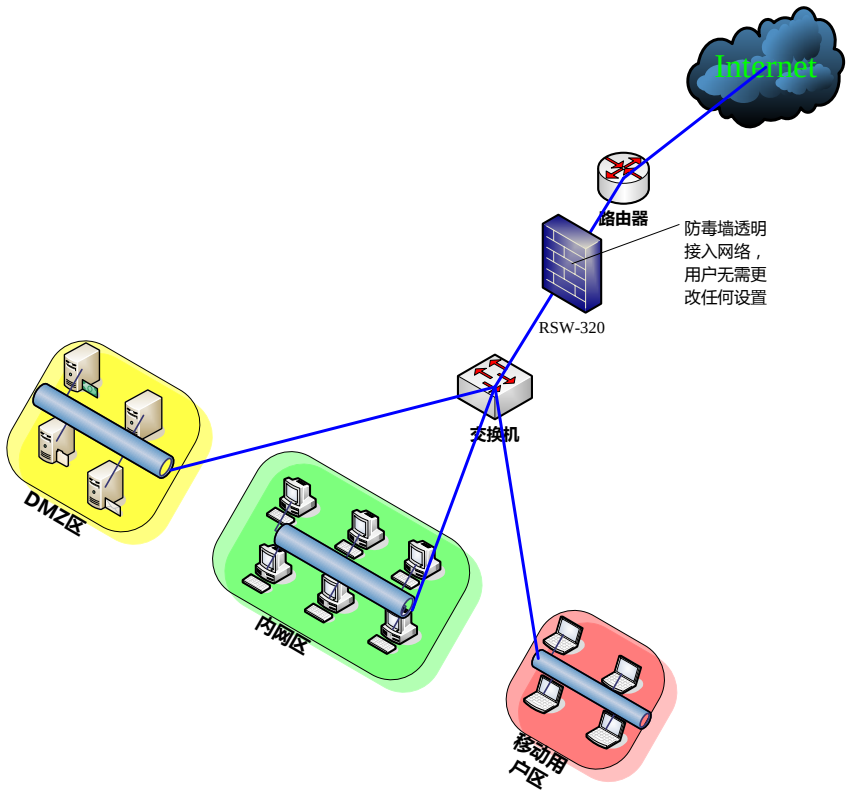


图 2.3 防毒墙透明模式部署

2.2 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，需要为防毒墙分配一个用于管理的 IP 地址并设置网桥接口的内网范围。如果选择宽带模式，需要选择进行外部连接时接口的工作模式（此部分配置请参阅本手册 4.1 接口配置）。

- 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
- 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
- 企业邮件系统的地址及所处区域
- 企业安全策略是如何制定的

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。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。

第三章 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

3.1 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-320 默认接口配置如下：

接口	所属区域	接口模式	IP 地址/子网掩码
E0	外网	未启用	无
E1	外网	未启用	无
E2	外网	未启用	无
E3	内网	静态 IP	192.168.100.244 /24
E4	内网	静态 IP	192.168.2.1/24

表 3.1 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 E4 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 3.1 所示。

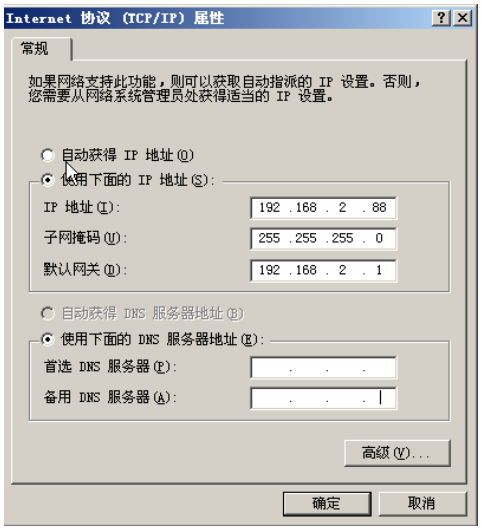


图 3.1 设置主机 IP 地址

3.2 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 5.2 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 3.2 所示

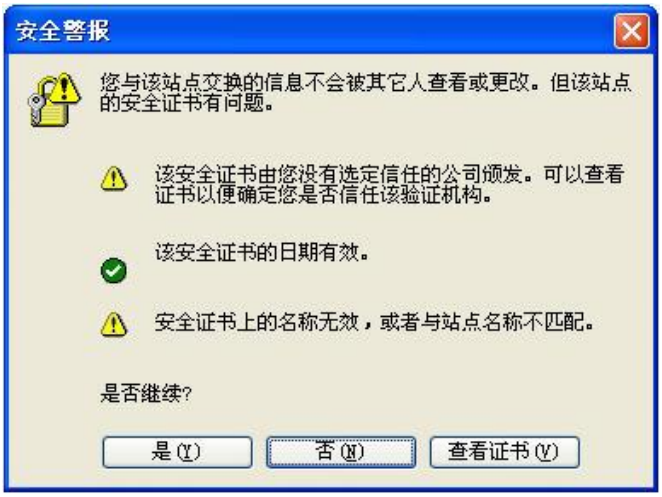


图 3.2 防毒墙证书

提示：当用户使用 IE7.0 或更高版本的浏览器时，会弹出以下警告，如图 3.3 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 3.3 使用 IE7.0 时遇到的安全提示

2. 请单击【是】，进入防毒墙登录界面。如图 3.4 所示

图 3.4 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 3.5 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 5.2 帐号管理。

图 3.5 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	设备号	显示当前防毒墙硬件设备序列号
	设备名称	显示当前防毒墙设备名称，单击当前的设备名称进行修改
	联系 Email	显示当前防毒墙设备联系人 Email 地址 ,单击当前联系人 Email 地址进行修改
	系统时间	显示当前防毒墙系统时间
	运行时间	显示当前防毒墙系统无故障运行时间，鼠标停留在该处显示系统启动时间。
	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 5.1.2 软件升级
	反病毒引擎	请在第一次登录防毒墙时输入购买的反病毒引擎序列号 ,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，您必须注册您的防毒墙，单击【授权】输入反病毒引擎注册码
	病毒库版本	当您购买瑞星防毒墙产品后，请在首次升级之后的 30 日内到指定网址完成产品服务的激活，30 日后仍未进行服务激活的用户将无法进行产品更新。有关产品激活内容请参见《快速使用指南》；该处显示当前防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 5.1.2 软件升级
	连接数	显示当前防毒墙与客户端建立的连接数和与防毒墙连接的客户端的数目
	在线管理员	显示当前防毒墙在线管理员的数目 ,单击【查看】进入帐号管理页面，如何进行在线用户管理请参见本手册 5.2.2 查看在线用户管理
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 [近一天]	显示防毒墙内主机一天中上传前五名客户端信息	
内网主机下载 TOP5 [近一天]	显示防毒墙内主机一天中下载前五名客户端信息	
【历史统计报告列表】	防毒墙自动将日志生成日报、周报和月报，管理员可以在历史统计报告列表下拉框选择所要查看的统计报告，即可进入报告查看界面	
关闭系统	关闭防毒墙系统	
重启系统	重新启动防毒墙系统	
定时刷新	选择系统首页定时刷新时间，分为 1 分钟、2 分钟、5 分钟、10 分钟、30 分钟和 1 小时。	

表 3.2 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，单击防毒墙管理页面右上角的  图标或者按 F5 刷新键能够快速返回到防毒墙基本信息页面。

3.3 防毒墙管理菜单

防毒墙管理分为九项功能区域，每一项功能都由相应的主页面构成，如图 3.6 所示。

图 3.6 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、路由配置和 DDNS 配置（网桥模式下无此功能）
- **系统维护**：系统维护、帐号管理和网络诊断
- **内网管理**：主机信息、主机历史和端口映射（网桥模式下无此功能）
- **上网控制**：安全策略、连接管理、URL 过滤和 IP 黑名单
- **虚拟专网（网桥模式下无此功能）**： PPTP VPN 配置和 IPSEC VPN 配置
- **防病毒**：防毒配置和瑞星网络版联动配置
- **入侵防御**：启用防毒墙入侵防御规则
- **日志审计**：日志审计和日志统计
- **退出**：退出防毒墙的管理

第四章 网络配置

防毒墙有宽带模式和透明模式两种工作模式，本章主要介绍在这两种工作模式下如何进行防毒墙的网络配置，分为以下三点：

- 接口配置：定义接口工作模式、接口配置信息和防毒墙 DNS 设置
- 路由配置：定义防毒墙路由表
- DDNS 配置：配置防毒墙某一接口获取固定的免费二级域名

4.1 接口配置

RSW-320 瑞星防毒墙支持透明模式和宽带模式两种工作模式，用户可以通过本手册 2.1 节的防毒墙网络部署图了解防毒墙在网络中工作的位置，从而快速完成防毒墙的部署工作。

- 宽带模式：在宽带模式下，防毒墙支持多种 ISP 接入方式，网络具有良好的可扩展性，管理员可以根据企业接入 Internet 的方式选择防毒墙的接口工作方式。
- 透明模式：在透明模式下，防毒墙自动将四个网口设置成两路网桥，在不改变用户原有网络拓扑的情况下对数据包进行透明转发，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。

4.1.1 宽带模式

在宽带模式下，防毒墙为用户提供三种 ISP 接入方式，分别为：静态 IP、动态 IP 和 PPPoE，管理员可以根据企业接入 Internet 的方式选择防毒墙的接口工作方式。宽带模式是防毒墙的默认工作模式。 在防毒墙功能菜单中单击【网络配置】，即可进入接口配置主页面，如图 4.1 所示。

图 4.1 宽带模式下接口配置界面

对宽带模式下接口配置界面中的各字段做如下说明：

字段	说明
当前工作模式	显示当前防毒墙的工作模式：宽带模式或透明模式。
切换为透明模式	此按钮可以完成防毒墙的工作模式切换，在宽带模式下单击此按钮即可使防毒墙切换到透明模式
外网	“外网”下的三个接口 E0、E1、E2 （以下简称为外网口），是防毒墙与外部网络连接的接口
未启用	表明接口为停用状态，若选择了接口的接入方式则接口变为启用状态
DNS 服务器	配置防毒墙 DNS 解析服务器地址
内网	“内网”下的两个接口 E3、E4 （以下简称为内网口），是防毒墙与企业内部网络连接的接口
	黄色图标表示该接口已经连接网线并且为启用状态
	表示该接口未连接网线
	蓝色图标表示该接口连接网线但是为未启用状态
	单击可以进行接口信息的设置，以下简称为设置图标

表 4.1 宽带模式下接口配置界面字段说明

在宽带模式下，E0、E1、E2 为防毒墙与外部网络的连接接口，管理员可以根据企业接入 Internet 的方式选择接口的 ISP 接入方式。接口 E3、E4 为防毒墙与企业内部网络的连接接口，防毒墙在两种工作模式切换过程中仅 E4 接口的设置不变，出于防毒墙易用性方面的考虑，建议用户使用 E4 接口作为管理口。外网口和内网口所提供的服务不同，下面分别介绍外网口和内网口的接口配置。

- **外网口的接口配置**

外网口是防毒墙与 Internet 连接的网络接口，防毒墙对进入内部网络的数据进行杀毒处理从而加强企业内部网络的安全。以下先对不同的 ISP 接入方式向用户说明。

ISP 即 Internet 服务提供商(Internet Service Provider)。它提供互联网的拨入帐号，是网络最终用户进入 Internet 的入口和桥梁。以下对三种 ISP 接入方式进行说明：

接口的工作模式	说明
静态 IP	ISP 提供固定的 IP 地址和网关地址供用户进行 Internet 接入 ,除非用户自己主动的去申请更换，否则 IP 地址不会改变
动态 IP	ISP 服务商通过 DHCP 服务为用户分配一个临时 IP 地址使用户可以连接到 Internet 上，这些用户通常会在每次连通 ISP 的主机后，自动获得一个动态的 IP 地址，该地址当然不是任意的，而是该 ISP 申请的网络 ID 和主机 ID 的合法区间中的某个地址。用户任意两次连接时的 IP 地址很可能不同，但是在每次连接时间内 IP 地址不变
PPPoE	ISP 为用户提供拨号上网帐号和密码，当用户进行拨号连接时，ISP 为用户分配一个 IP 地址供用户连接到 Internet 上

表 4.2 ISP 三种接入方式

在外网口未进行接口配置以前，接口默认为停用状态，用户可以根据企业的 Internet 接入方式对防毒墙各接口进行配置。下面分三部分介绍静态 IP、动态 IP 和 PPPoE 三种 ISP 接入方式下接口的配置。(以 E0 接口为例进行说明，其他外网口的配置与 E0 相同)

✓ **静态 IP 方式**

1. 在宽带模式下接口配置主界面，单击 E0 接口右侧的设置图标，进入接口配置界面，如图 4.2 所示

图 4.2 接口配置界面

2. 单击【静态 IP】，选中静态 IP 如图 4.3 所示

图 4.3 静态 IP 配置界面

对静态 IP 模式配置界面各字段做如下说明：

字段	说明
ISP 接入方式	根据企业的连网方式选择接口的 ISP 接入方式，单击 表示选中，此处选择静态 IP 模式
选择当前带宽	单击【选择当前带宽】后面的下拉框选择接口当前带宽，有 1M、2M、5M、10M、50M 五种选择 ,用户可以根据 ISP 供应商提供的带宽选择合适带宽 ,应保证选择的带宽大于等于 ISP 供应商提供的带宽，用户也可以手动输入带宽值，最小为 512K
接口	显示用户当前正在配置的接口
IP 地址	设置接口的 IP 地址
掩码	设置接口的子网掩码，默认为 255.255.255.0
网关	设置接口网关地址
设置为默认网关	将当前输入的网关 IP 作为防毒墙的默认网关
当前默认路由	显示接口当前默认路由信息

表 4.3 静态 IP 模式配置界面各字段说明

提示：关于防毒墙唯一的二级域名

防毒墙拥有一个唯一的设备 ID 号，使用这个唯一的设备 ID 号在互联网上将一个外网接口注册一个二级域名地址，通过这个二级域名可以迅速解析到该接口的 IP 地址。当防毒墙使用多条链路进行互联网接入时，该二级域名只在设置为默认网关的接口上进行注册，也可通过更改默认网关地址对其进行切换。

3. 单击【选择当前带宽】后面的下拉框，选择合适的带宽，也可以手动输入带宽值
4. 填写 IP 地址：由 ISP 服务商提供
5. 填写掩码：由 ISP 服务商提供
6. 填写网关：由 ISP 服务商提供。如需将该接口网关地址设置为防毒墙默认网关地址，可选中【设置为默认网关】的单选框
7. 单击【确定】保存设置，系统弹出如图 4.4 所示成功提示对话框；单击【关闭】取消操作。

图 4.4 接口配置成功提示界面

8. 单击【确定】按钮，完成接口信息的配置操作。

提示：关于设置 IP 别名

当接口接入方式设置为静态 IP 模式时，重新单击设置图标进入接口界面如图 4.5 所示。

图 4.5 接口设置为静态 IP 模式后的设置界面

防毒墙为静态 IP 模式下的接口设置提供增加多个别名 IP 的功能，具体设置可以参看本节设置别名 IP 部分。

在接口的一般配置完成以后，如果需要对接口进行高级设置，可再次通过单击接口右侧的设置图标，进行接口的高级设置，主要是接口提供服务类型的设置。

提示：关于高级设置的说明

停用模式下高级设置不可用。接口的一般设置没有完成前高级设置也不可用。

1. 单击接口 E0 右侧的设置图标，进入接口配置界面，如图 4.6 所示。

图 4.6 E0 接口配置服务初始界面

2. 单击【高级设置】，进入接口服务配置界面如图 4.7 所示。

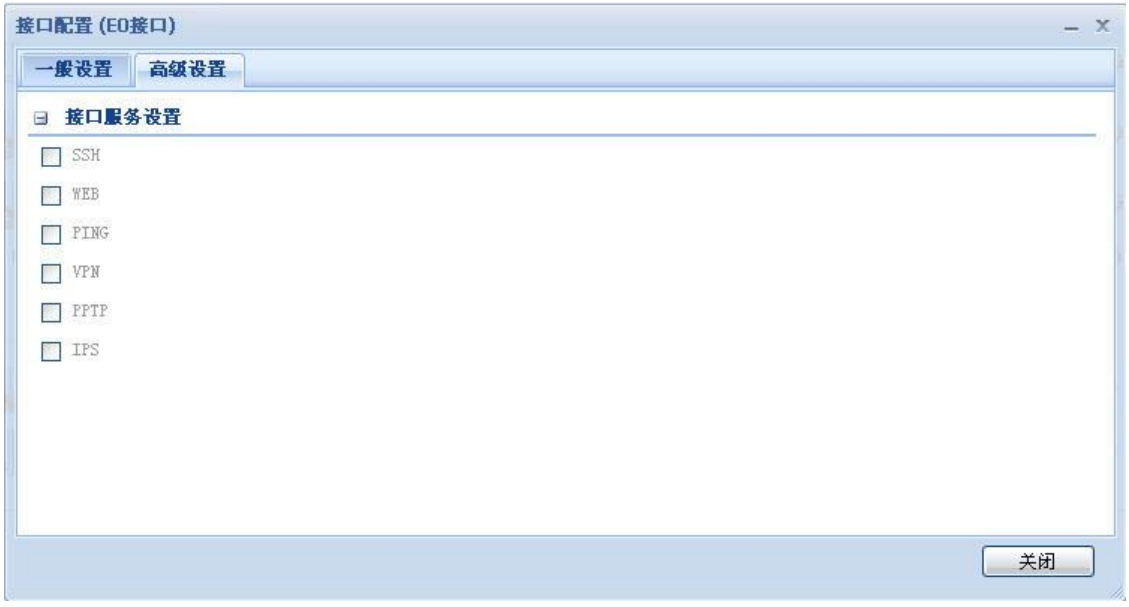


图 4.7 接口服务设置界面

对于接口服务设置界面中的各种服务我们做以下说明：

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
PING	响应 ping 命令
VPN	开启 VPN 服务，防毒墙可以建立 VPN 通道
PPTP	使用点对点隧道协议在运行 Windows 操作系统的远程客户计算机通过防毒墙和您的内部网络之间建立一个虚拟专用网络
IPS	接口启用该服务后，过滤经过该接口的数据包，如果防毒墙发现潜在的危险信息，阻断该数

	据包并记入网络日志
	复选框，表示此时所需服务未开启，单击复选框后服务开启，图标变为 ，可以同时选中多个复选框。

表 4.4 接口服务说明

提示：关于服务的开启

Web、SSH 和 Ping 是为方便防毒墙管理所开启的服务，在外网口开启这三种服务，使防毒墙在互联网中暴露，导致企业网络存在一定的安全隐患。

3. 单击要设置的接口服务左侧的复选框，启用服务，在界面左下角会出现系统处理中的提示信息如图 4.8。若是要取消启用的服务，只需再次单击服务左侧复选框便可取消服务。

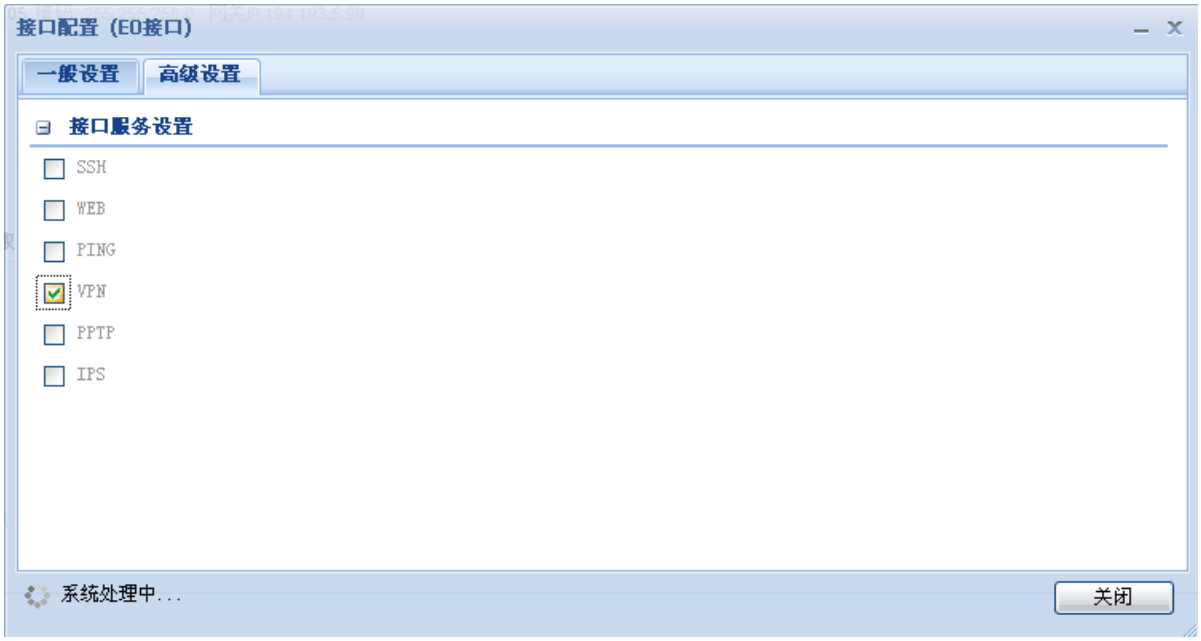


图 4.8 系统处理提示信息

4. 单击【关闭】按钮，完成接口的高级设置。

✓ **动态 IP 方式**

1. 在宽带模式下接口配置界面，单击 E0 接口右侧的设置图标，进入接口配置界面，如图 4.9 所示。

图 4.9 接口配置界面

2. 单击【动态 IP】，选中动态 IP，如图 4.10 所示。

图 4.10 动态 IP 方式的配置界面

3. 单击【选择当前接口带宽】后面的下拉框，选择合适的带宽，也可手动输入带宽值

4. 单击【确定】保存设置，系统弹出如图 4.11 所示成功提示对话框；单击【关闭】取消操作。

图 4.11 成功提示框

5. 单击【确定】按钮，完成接口信息的配置操作。

动态 IP 方式下接口的一般设置完成后，用户如果需要进行接口的高级设置，可参看静态 IP 方式下的高级设置。

✓ PPPoE 方式

1. 在宽带模式下接口配置界面，单击 E0 接口右侧的设置图标，进入接口配置界面，如图 4.12 所示。

图 4.12 接口配置界面

2. 单击【PPPoE】，选中 PPPoE 如图 4.13 所示。

图 4.13 PPPoE 方式下配置界面

关于输入信息的几点说明如下：

字段	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
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进行拨号操作，适用于上网时间不固定的用户。自动拨号就是防毒墙在启动时自动进行 PPPoE 拨号，若是不启用定时拨号，防毒墙将在每次掉线后自动重连；若是启用定时拨号，防毒墙在设置的开始时间进行拨号，一直保持连接，直到结束时间才断开连接

表 4.5 PPPoE 方式下用户输入信息说明

3. 单击【选择当前带宽】后面的下拉框，选择合适的带宽，也可手动输入带宽值

4. 输入进行拨号的 ADSL 用户名

5. 输入进行拨号的密码（6 位-30 位）

6. 重复输入密码，防止误操作

7. 选择拨号模式，有手动拨号和自动拨号两种方式，默认为手动拨号

手动拨号

1) 单击手动拨号前的单选框选中手动拨号

2) 单击【确定】保存设置，系统弹出成功提示对话框如图 4.14 所示；单击【关闭】取消操作。

图 4.14 接口信息设置成功提示界面

3) 单击【确定】按钮，返回接口配置主界面，如图 4.15 所示

图 4.15 手动拨号界面

4) 单击【连接】，显示如图 4.16 所示界面，防毒墙进行 ADSL 拨号连接，若是连接时间过长，用户可以单击【刷新】按钮刷新连接状态。

图 4.16 手动拨号刷新界面

5) 连接成功后显示如图 4.17 所示界面。

图 4.17 ADSL 连接成功界面

自动拨号

1) 单击自动拨号前的单选框选中自动拨号如图 4.18 所示

图 4.18 选择自动拨号时的界面

2) 若是用户不需要启用定时拨号的功能，则单击【确定并立即连接】保存设置，单击【关闭】取消操作。若是用户需要启用定时拨号，则需单击启用定时拨号前的单选框，如图 4.19 所示

图 4.19 启用定时拨号

3) 选择定时拨号的时间对象

单击启用定时拨号后面的下拉框可以选择拨号的时间对象，也可以选择最后一项的增加新时间对象，若是用户需要设置新的时间对象，可以参见时间对象的设置部分。这里先对已有时间对象做如下说明：

时间对象	说明
上班前	默认时间为 00：00-08：59，周一至周五
上午上班时间	默认时间为 09：00-11：59，周一至周五
下班后	默认时间为 17：30-23：59，周一至周五
下午上班时间	默认时间为 13：00-17：29，周一至周五
中午休息时间	默认时间为 12：00-12：59，周一至周五
周末	默认时间为 00：00-23：59，周六，周日
非工作时间	默认时间为 00：00-8：59，周一至周五；12：00-12：59，周一至周五；17：30-23：59，周一至周五；00：00-23：59，周六，周日
工作时间	默认时间为 09：00-11：59 和 13：00-17：29，周一至周五

表 4.6 已有时间对象说明

4) 单击【确定】保存设置，单击【关闭】取消操作。

设置完 PPPoE 方式的一般设置后，如果需要进行接口的高级设置，可参看静态 IP 方式下高级设置

✓ **时间对象的设置**

为了便于管理员对防毒墙的管理，瑞星防毒墙引用了时间对象的概念，把系统需要用到的时间以时间对象的形式定义，便于管理员统一管理。

➢ **增加时间对象**

1. 在配置 PPPoE 接口配置界面启用定时拨号，在后面的下拉框中选择【增加新时间对象】，进入增加新时间对象界面，如图 4.20 所示。（本手册其他章节涉及到时间对象的部分一般是在时间一栏的下拉框选择时间对象）

图 4.20 增加时间对象

1） 时间对象名称：填写时间对象的名称

2） 时间段：填写一个时间段，例如工作时间早上的 9 点到 12 点

3） 星期：选择该时间对象在一周内生效的时间

填写完成后，单击【增加】按钮完成时间对象的添加，如图 4.21 所示。

图 4.21 添加一个时间

2. 单击【完成】完成时间的添加。如果用户还想在一个时间对象里添加时间，重新选择时

间范围再单击【继续增加】为该时间对象继续添加时间，如图 4.22 所示。

图 4.22 继续添加时间

添加完成后，单击【完成】完成时间对象的添加。

- **修改时间对象**

防毒墙系统预先定义的时间对象可能与企业实际的工作时间存在差异，管理员可以通过对存在的时间对象的修改来满足企业的实际需求。

1. 在时间下拉框选择要修改的时间对象，例如上班前，如图 4.23 所示

图 4.23 选择要修改的时间对象

2. 单击时间对象右侧的修改图标，进入时间对象修改界面，如图 4.24 所示。时间对象修改界面各字段说明参见表 4.7。

字段	说明
序号	对一个时间对象下的多个时间段进行排序
开始时间	该时间对象的起始时间
结束时间	该时间对象的结束时间
星期	该时间对象每周的生效时间
操作	对时间设置执行的操作，单击 可以删除设置的时间对象

表 4.7 时间对象修改界面字段说明

图 4.24 时间对象修改界面

3. 管理员可以单击已存在的时间一行的删除图标删除已存在的时间，然后按照增加时间对象的操作重新添加新的时间对象或时间组，具体步骤参看增加时间对象。

➢ **删除时间对象**

如果用户设置的某个时间对象已经失效，可以将该时间对象删除。在选择时间的下拉框选择要删除的时间对象，例如上班前，如图 4.25 所示

图 4.25 选择要修改的时间对象

单击时间对象右侧的删除图标，完成时间对象的删除操作

✓ **停用**

如果不想使用防毒墙某个接口，可以选择最后一项停用，停用该接口。停用选项在【接口配置】➔【一般配置】中，用户可以通过单击【停用】选项前的单选按钮来停用接口。如图 4.26 所示

图 4.26 停用界面

单击【确定】保存设置，单击【关闭】取消操作。

● DNS 服务器

防毒墙的 DNS 功能是设置需要进行域名解析时所要访问的上层 DNS 服务器的地址。防毒墙使用首选、

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。

在宽带模式下的接口配置界面，可以进行防毒墙的 DNS 配置，如图 4.27 所示。

图 4.27 接口设置界面 DNS 设置区界面

防毒墙 DNS 设置有两种方式。一种是手动输入 DNS 服务器地址；另一种是防毒墙自动获取 DNS。宽带模式下防毒墙支持的的三种 ISP 接入方式都可以使用手动获取的 DNS 服务器地址。当接口工作在 PPPoE 或是动态 IP 模式下时，用户也可以选择自动获取 DNS 的 IP 地址。

✓ **手动输入 DNS 服务器地址**

1. 单击 DNS 设置一行右侧的设置图标，进入 DNS 设置界面，如图 4.28 所示

图 4.28 DNS 设置界面

2. 输入首选 DNS 服务器地址，一般由 ISP 提供
3. 输入备用 DNS 服务器地址，一般由 ISP 提供

提示：首选 DNS 和备用 DNS 的区别

在进行域名解析时首先选择该地址，若是连接失败，则选择备用 DNS 服务器地址进行解析。

4. 单击【确定】，系统弹出成功提示框，如图 4.29 所示。

图 4.29 设置 DNS 服务器成功系统提示界面

5. 单击【确定】按钮，完成防毒墙的 DNS 设置。

✓ **自动获取 DNS**

单击 DNS 设置界面自动获取 DNS 前的单选框，进入自动获取 DNS 界面，如图 4.30 所示。单击【确定】按钮保存设置，单击【关闭】取消操作。

图 4.30 自动获取 DNS 界面

提示：关于 DNS 设置的修改

如果用户要对设置的 DNS 服务器地址进行修改，只需按照以上步骤重新设置 DNS 服务器地址即可。

- **内网口的接口配置**

内网口是防毒墙与企业内部网络相连接的接口。这里我们仍然分为接口的一般设置和高级设置两部分来指导用户如何配置内网口（在此以接口 E3 为例进行配置，接口 E4 的配置与 E3 相同）

✓ **一般设置**

1. 单击接口 E3 右侧的设置图标，进入接口配置界面，如图 4.31 所示界面

图 4.31 内网口接口默认配置界面

2. 填入 IP 地址
3. 填入掩码
4. 单击【确定】，系统弹出成功提示对话框，如图 4.32 所示；单击【关闭】取消操作。

图 4.32 内网口接口设置成功提示界面

5. 单击【确定】按钮，完成内网口接口配置。

提示：关于设置别名 IP

内网口默认设置为静态 IP 模式，使用过程中 E3、E4 的模式不能更改，单击内网口接口设置界面【增加别名 IP】按钮可以设置别名 IP，具体设置可以参看本节设置 IP 别名部分

✓ **高级设置**

内网口的高级设置与外网口类似，但内网口与外网口提供的服务有所差异。单击 E3 接口右侧的设置图标进入【高级设置】选项界面如图 4.33 所示。

图 4.33 内网口接口服务设置

对于接口服务我们做以下说明

服务	说明
SSH	通过 SSH 配置管理防毒墙
WEB	通过 Web 配置管理防毒墙
PING	响应 ping 命令
DHCP	为连接到该接口下的计算机提供自动分配 IP 地址的服务
IPS	接口启用该服务后，过滤经过该接口的数据包，如果防毒墙发现潜在的危险信息，在网络日志中进行记录并阻断该数据包
☐	复选框，表示此时所需服务未开启，单击复选框后服务开启，图标变为 ☑，可以同时选中多个复选框。

表 4.8 内网口接口服务说明

单击各服务左侧的复选框，可以同时选择多种服务。 接口服务设置完成以后，单击【关闭】退出配置界面。

请按照以下步骤进行 DHCP 地址范围的设置：

1. 单击 E3 接口右侧的设置图标进入【高级设置】选项，选中 DHCP 服务，界面如图 4.34 所示

图 4.34 DHCP 服务界面

2. 单击【设置 DHCP 范围】，进入 DHCP 范围设置界面如图 4.35 所示。

图 4.35 接口 DHCP 范围设置界面

3. 填写要设置的 DHCP 范围，单击【增加】按钮，在 DHCP 地址分配列表中出现该条记录，如图 4.36 所示。

图 4.36 DHCP 配置查看和删除界面

用户可以继续输入不同的网段，单击【增加】可以在一个启用 DHCP 服务的接口设置多个 DHCP 地址范围，应用于多个需要防毒墙 DHCP 服务的子网。单击【关闭】结束操作。

DHCP 范围的删除只需进入 DHCP 范围设置界面，单击所要删除 DHCP 范围条目一行的删除图标即可。

- **设置别名 IP**

当接口设置为静态 IP 模式时，防毒墙提供了一个为接口设置多个别名 IP 的功能，即一个接口拥有多个 IP 地址，可以实现不同网段间的通信。以接口 E1 为例，接口 E1 的当前接入方式为静态 IP，单击 E1 右侧的设置图标，进入接口配置界面如图 4.37 所示

图 4.37 静态 IP 模式下接口配置界面

提示：关于设置 IP 别名

只有当接口设置为静态 IP 模式时才可以进行别名 IP 的设置，其他模式下，没有该项功能。

✓ **增加别名 IP**

1. 在静态 IP 模式下的接口配置界面单击【增加别名 IP】，进入增加别名 IP 界面如图 4.38 所示。

图 4.38 增加别名 IP 配置界面

2. 填写 IP 地址

3. 填写掩码

4. 单击【增加】，成功添加别名 IP 并返回到接口配置界面，并在界面右侧显示当前别名 IP 列表，如图 4.39 所示。单击【关闭】取消操作。可以重复以上步骤为接口设置多个 IP 别名。

图 4.39 增加别名 IP 成功后显示别名 IP 列表

✓ **删除别名 IP**

如果用户要删除已经存在的别名 IP 地址，可以在该接口别名 IP 列表中进行删除操作。

单击 E1 右侧的设置图标，进入接口配置界面如图 4.40 所示，显示当前接口别名 IP 列表。

图 4.40 接口配置界面

单击要删除的别名 IP 记录一行的删除图标直接删除该别名 IP 地址。

- **查看接口详细信息**

> **提示：关于接口信息的查看**
>
> 在接口未配置的时候没有信息可以查看。

接口配置成功以后，可以通过单击查看图标查看接口网络特性，如物理地址、带宽等。单击【网络配置】➔【接口配置】进入接口配置界面如图 4.41 所示（以查看接口 E0 为例）。

图 4.41 接口配置界面

单击 E0 右侧扩展图标，展开接口 E0 详细信息如图 4.42 所示，单击隐藏图标，可以隐藏接口信息。

图 4.42 查看接口状态信息

对于接口状态信息查看界面的各字段说明：

字段	说明
	隐藏图标，通过单击该图标可以将扩展图标扩展出的接口信息隐藏
接口	显示当前用户查看的网络接口
自适应	自动检测当前网络的连接速率的大小
物理地址	防毒墙接口的 MAC 地址
链路	显示接口当前带宽和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，unknown 表示未能检测出状态，请检查网线的连通性）
连接状态	当前接口的连接状态
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

表 4.9 接口信息字段说明

- **接口配置的修改**

当用户网络环境发生改变时，可以修改接口配置以适应新的网络环境。对于内网口接口配置的修改用户只需单击接口右侧的设置图标进入接口配置界面，接口的修改与配置步骤相同，具体操作步骤请参看内网口接口配置。外网口的接口配置修改如下：（以修改接口 E1 为例，其它外网口接口配置的修改

与 E1 相同，E1 当前配置如图 4.43 所示）

图 4.43 接口配置界面（E1）

1. 在接口配置界面，单击 E1 接口右侧的设置图标，进入接口配置修改界面，如图 4.44 所示。

图 4.44 修改 E1 接口

2. 单击【修改】，重新选择 ISP 的接入方式，按外网口接口配置中的操作步骤重新配置。

4.1.2 透明模式

瑞星防毒墙的透明模式，也叫“网桥模式”，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架设在网络中，此时防毒墙有查杀病毒的功能，并且用户可以忽略它的存在。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。

接口工作模式的切换可以通过单击网络配置主界面上的【切换为透明模式】按钮来实现，如图 4.45 所示。

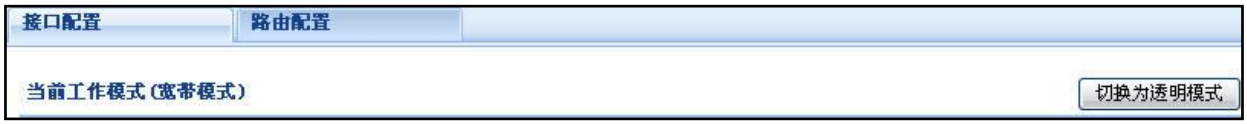


图 4.45 切换接口工作模式

切换模式时会弹出系统提示对话框，如图 4.46 所示。

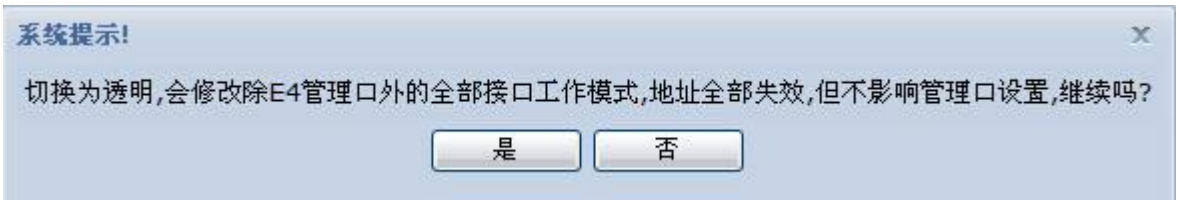


图 4.46 切换为透明模式的系统提示

提示：关于模式转换

为了便于防毒墙的管理，将接口 E4 设置为管理口，当从宽带模式转换到透明模式或是从透明模式转换到宽带模式时，除 E4 接口的设置不变以外，其他接口的设置均被清除，需要用户在模式转换后重新配置。

单击【是】按钮完成模式切换操作，进入透明模式的主界面，如图 4.47 所示；单击【否】按钮取消操作。

图 4.47 透明模式的主界面

提示：关于管理界面

接口配置切换到透明模式后，系统主界面左侧菜单缺少了【虚拟专网】，因为这项服务和路由功能有关系，而在网桥模式下无法实现这项服务，所以防毒墙隐藏了这项。

透明模式下接口配置界面中的各字段说明如下：

字段	说明
当前的工作模式	说明当前防毒墙的工作模式，有宽带模式和透明模式两种，当前为透明模式
切换为宽带模式	此按钮改变防毒墙的工作模式，在透明模式下单击此按钮即可使防毒墙切换到宽带模式
网桥	防毒墙内部提供两路网桥供用户使用。默认 E0 和 E1、E2 和 E3 组成两路网桥。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
管理接口	透明模式下可以通过 E4 口管理防毒墙
	蓝色图标表示防毒墙接口未连通
	黄色图标表示防毒墙接口为连通状态

	单击可以进行相应接口的设置

表 4.10 透明模式的界面说明

网桥模式下，防毒墙自动将接口 E0、E1、E2 和 E3 组成两路网桥，接口 E4 作为管理口，以下从网桥和管理接口两方面进行透明模式下的接口配置。

提示：关于防毒墙的 Bypass 接口

瑞星 RSW-320 防毒墙 E2 和 E3 接口支持 Bypass 功能，当工作模式切换到网桥模式时，在网桥二上自动激活 Bypass 功能，用户可以在串口模式下利用 Bypass 命令关闭或启用这个功能。关于 Bypass 功能请参见本手册专业术语表中的 Bypass。

注：在防毒墙硬件工作不正常时，支持 Bypass 功能的两个接口可以在设定时间内，自动接管防毒墙的工作，保证网络的连通性。

- **网桥**

透明模式下有两路网桥，接口 E0 和 E1 在网桥一下工作，接口 E2 和 E3 在网桥二下工作，如图 4.48 所示。

图 4.48 网桥界面

网桥界面的各个字段说明如下：

字段	说明
网桥一	接口 E0 和 E1 组成网桥一，其中 E0 设置为外网接口，E1 设置为内网接口
网桥二	接口 E2 和 E3 组成网桥二，其中 E2 设置为外网接口，E3 设置为内网接口
【未设置内网范围】	防毒墙默认配置未进行内网范围的设定，单击此处进行添加。
停用	单击停用可以将网桥二的由启用状态转换为停用状态
	以下称为扩展图标，单击扩展图标可以查看网桥的详细配置信息，图标变为（以下简称隐藏图标），单击隐藏图标可隐藏扩展的信息

表 4.11 网桥界面说明

✓ **查看网桥详细配置**

用户可以单击网桥一行的扩展图标将网桥的详细信息展开，如图 4.49 所示。

图 4.49 网桥一的详细信息

网桥一的详细信息各个字段说明如下：

字段	说明
接口	显示接口的名称和区域，E0 为外网接口，E1 为内网接口
物理地址	网卡的 MAC 地址
连接状态	当前接口的连接状态
自适应	自动检测当前网络的连接带宽的大小
链路	显示当前接口的带宽值和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

表 4.12 网桥的详细信息界面说明

✓ **设置内网范围**

在宽带模式下，在防毒墙内网接口处已经明确的设置了内网范围；而在网桥模式下，防毒墙默认提供一个管理接口供管理员管理防毒墙，只有通过在网桥接口下设置防毒墙内网范围，防毒墙才能区分内网和外网，并有效的获取内网主机信息。

➢ **增加内网范围**

单击网桥一接口右侧的【未设置内网范围】进行设置内网范围，设置如图 4.50 所示。

图 4.50 设置内网范围

设置内网范围界面各个字段说明如下：

字段	说明
IP 地址/掩码	填写内网范围，掩码可以选择 20、24、28 和 32，管理员也可以手动输入 20-32 某个数值。内网范围是防毒墙用来区分内网主机和外网主机，请管理员慎重填写
【增加】	用户输入符合规则的内网范围后，单击【增加】可执行增加内网范围的操作
序号	内网范围列表按阿拉伯数字排序
IP/掩码	设置的内网范围
操作	对网桥接口添加的内网范围可以进行删除操作

表 4.13 设置内网范围界面说明

输入符合规则的内网范围，单击【增加】按钮保存结果。当添加一条内网范围后，会在设置内网范围界上显示出来，如图 4.51 所示。

图 4.51 成功设置内网范围

同时该条记录也会在透明模式主界面上显示出来，如图 4.52 所示。

图 4.52 透明模式主界面上显示的网桥内网范围

➢ **删除内网范围**

若是内网主机的地址有变化，管理员需要删除网桥已经设置的内网范围，可以单击该网桥接口右侧的【内网范围】进入设置内网范围界面，然后单击内网条目后面的删除图标进行删除。

✓ **停用网桥二**

网桥模式下自动将接口 E0 和 E1 组成网桥一，将接口 E2 和 E3 组成网桥二，网桥一始终开启，网桥二可以根据需要开启或者关闭，单击网桥二后面的【停用】或者【启用】按钮即可实现，当网桥二启用状态时，如图 4.53 所示。

图 4.53 网桥二为启用状态

单击【停用】，系统弹出提示框如图 4.54 所示。

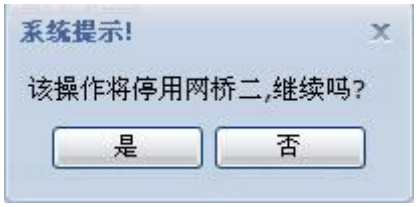


图 4.54 停用网桥二的系统提示

单击【是】按钮停用网桥二，单击【否】按钮取消操作。

- **管理接口**

网桥模式下接口 E4 为管理接口，可以通过此接口连接到防毒墙上对防毒墙进行操作。管理接口界面如图 4.55 所示。

图 4.55 管理接口

可以单击接口 E4 后面的设置图标进入接口配置界面，如图 4.56 所示。

图 4.56 管理接口配置界面

管理接口配置界面各个字段说明如下：

字段	说明
IP 地址	管理接口的内部 IP 地址，通过此 IP 可以登录防毒墙对内网进行管理
掩码	设置该 IP 地址的子网掩码
网关	填写接口的网关地址

首选DNS服务器	输入首选 DNS 服务器的 IP 地址
备用DNS服务器	如果有备用 DNS 服务器的 IP 地址，填写备用 DNS 服务器的 IP 地址

表 4.14 管理接口配置界面说明

填写完相关信息后，单击【设置】按钮保存结果，单击【关闭】取消操作。

4.2 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。

单击【网络配置】➔【路由配置】，进入路由配置界面，如图 4.57 所示，对于配置过的接口，会自动将其路由信息添加到路由配置中。

图 4.57 路由配置主页面

对于路由配置界面中的各字段，我们做如下说明：

字段	说明
【增加静态路由】	单击可以进入增加静态路由界面
序号	将路由条目按阿拉伯数字排序
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 IP 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网络设备上找到，则设置该网络设备的 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
操作	用户可以对路由条目执行的操作。对于本地路由条目，即在防毒墙接口配置过程中自动生成的路由条目，不允许执行任何操作。对于用户自定义的路由条目，用户可对其执行修改和删除操作。
	删除图标，单击删除路由记录
	修改图标，单击进入修改路由记录界面

表 4.15 路由配置界面字段说明

4.2.1 增加静态路由

1. 在路由配置主页面，单击【增加静态路由】，进入路由条目配置界面，如图 4.58 所示。

图 4.58 增加静态路由界面

2. 填写网络地址

3. 填写网络掩码

4. 填写指定网关后单击【确定】保存设置。或是选择网络接口指定前的单选框指定网络接口，如图 4.59 所示。

图 4.59 选择网络接口界面

5. 选择网络接口，单击【确定】按钮保存设置，单击【关闭】取消操作。

4.2.2 修改静态路由

瑞星 RSW-320 防毒墙的路由信息由两部分组成。一部分是用户在对防毒墙进行配置时自动生成的路由条目，我们称之为本地路由条目，这些路由条目是防毒墙正常工作的前提，所以不允许用户对其进行修改和删除操作。另一部分路由信息是用户在防毒墙工作过程中根据需要手动添加的，用户可以根据需要对其进行修改和删除操作。路由信息的修改操作如下：

1. 单击【网络配置】➔【路由配置】，进入路由配置界面，如图 4.60 所示。

图 4.60 路由配置界面

2. 单击要修改的路由条目右侧的修改按钮，进入路由信息修改界面，如图 4.61 所示。

图 4.61 路由信息修改界面

3. 填写需要修改的路由信息，具体步骤请用户参看增加静态路由部分。

4. 单击【修改】保存设置，单击【关闭】取消操作。

4.2.3 删除静态路由

1. 单击【网络配置】➔【路由配置】进入路由配置界面，如图 4.62 所示。

图 4.62 路由配置界面

2. 单击要删除的路由条目一行的删除图标，系统提示如图 4.63 所示的确认界面。

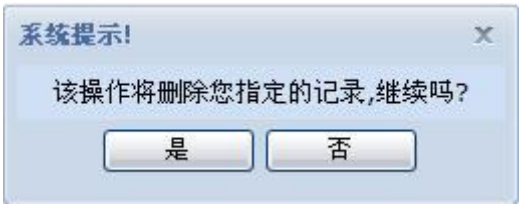


图 4.63 单击删除图标系统提示界面

3. 单击【是】执行删除操作，系统弹出如图 4.64 所示界面；单击【否】取消操作。

图 4.64 删除路由条目的提示界面

4. 单击【确定】按钮，完成静态路由的删除操作。

提示：关于路由条目的删除

在防毒墙配置过程中自动生成的路由条目是防毒墙正常工作的保障，所以不允许删除。用户可以删除自定义的路由条目，即通过【增加静态路由】操作生成的路由条目。

4.3 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 4.65 所示。

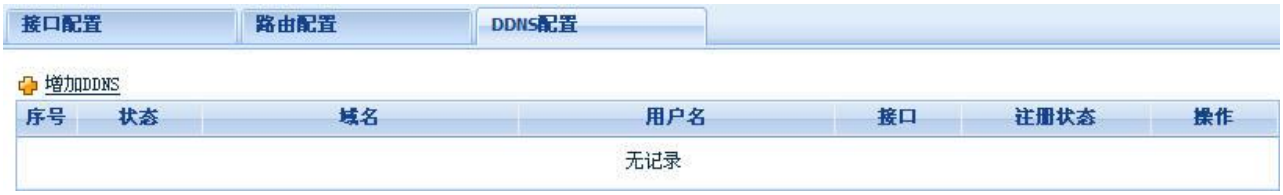


图 4.65 防毒墙 DDNS 配置界面

提示：网桥模式下不具备该功能，并且使用防毒墙 DDNS 功能前需要用户从免费域名网站注册域名。

4.3.1 增加 DDNS

在 DDNS 配置页面单击【增加 DDNS】按钮，进入增加 DDNS 页面，如图 4.66 所示

图 4.66 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

提示：进行域名注册的接口必须能够访问 Internet。

当填写好相关内容后，单击【确定】按钮保存设置，【关闭】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 4.67 所示。

图 4.67 DDNS 配置列表

图 4.67 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 PROCESS_RUNNING 和 DISABLED 两种状态，如果在域名服务器上注册成功则显示 PROCESS_RUNNING 状态，如果在域名服务器上注册失败则显示 DISABLED 状态
操作	单击 进入修改设置页面
启用 DDNS	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【启用 DDNS】，则该规则被启用
停用 DDNS	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【停用 DDNS】，则该规则被停用

表 4.16 防毒墙 DDNS 列表名词解释

4.3.2 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 4.68 所示。

图 4.68 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【修改】按钮确认修改，【关闭】按钮取消修改。

4.3.3 删除 DDNS

在 DDNS 配置页面选中某条 DDNS 记录，单击该记录的 按钮，则删除该条 DDNS 规则

第五章 系统维护

本章主要介绍以下三个模块的功能及使用方法：

- 系统维护：系统时间管理、软件升级、备份和恢复防毒墙系统配置
- 帐号管理：管理防毒墙的管理员帐号
- 网络诊断：进行防毒墙设备网络诊断

5.1 系统维护

系统维护包含系统时间、软件升级和备份管理三个部分的配置。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【系统维护】进入系统维护页面如图 5.1。

图 5.1 系统维护页面

系统维护分为以下四个模块：

- 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
- 备份管理：备份当前系统配置信息，以便在以后恢复时使用
- SSL 证书管理：安装防毒墙证书

5.1.1 系统时间

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。系统时间设置界面如图 5.2 所示。界面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，可进行防毒墙系统时间与管理主机时间或网络时间服务器的同步操作。

图 5.2 系统时间设置界面

对系统时间设置界面相关字段我们做以下说明

字段	说明
防毒墙时间	显示当前防毒墙设置的时间
本地时间	防毒墙管理主机显示的时间
时间服务器	显示当前选择的时间服务器

表 5.1 系统时间设置界面各字段说明

- **防毒墙时间设置**

图 5.3 系统时间设置界面

✓ **设置系统时间的时区**

1. 在系统时间设置界面，单击防毒墙时间右侧的设置图标，进入防毒墙时间设置界面，如图 5.4 所示。

图 5.4 选择系统时区

2. 单击【系统时区】后的下拉框选择系统时区

3. 单击【时间服务器】后的下拉框选择时间服务器地址

4. 选择是否启用定时同步。关于定时同步请参看系统时间定时同步设置

5. 单击【确定】按钮保存防毒墙时间设置，单击【关闭】按钮取消操作。

✓ **系统时间定时同步设置**

➢ **启用定时同步**

1. 在时间服务器处选择需要进行同步的时间服务器

2. 单击定时同步一行【启用】前的单选框启用定时同步

3. 在定时同步处输入何时进行同步，如图 5.5 所示

图 5.5 设置系统时间定时同步

4. 单击【确定】按钮保存定时同步设置，单击【关闭】按钮取消操作。

启用定时同步以后，定时同步设置的详细信息将在系统时间界面显示出来，如图 5.6 所示

图 5.6 启用定时同步后系统时间界面界面

➢ **修改定时同步**

启用定时同步以后，用户如果想要修改定时同步设置，可以执行如下操作：

单击定时同步右侧的设置图标，进入定时同步修改界面。后续操作请用户参看启用定时同步。

注意：防毒墙的时间影响到系统日志和升级功能的准确性，请务必保证时间的同步和正确。

- **与本地时间同步**

1. 在系统时间设置界面，单击本地时间一行的设置图标，设置防毒墙时间与本地时间同步，如图 5.7 所示。

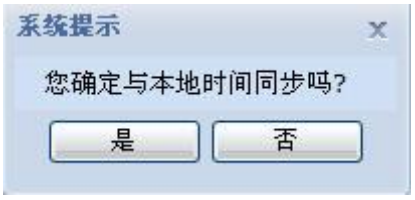


图 5.7 是否与本地时间进行同步

2. 单击【是】按钮进行防毒墙系统与管理主机本地时间进行同步；单击【否】取消操作。单击【是】按钮后系统弹出正在同步的提示框，如图 5.8 所示。

图 5.8 防毒墙时间同步进度

- **与时间服务器同步**

提示：界面说明

如果在【防毒墙时间】设置里启用了定时同步功能，这里不是【时间服务器】而是【定时同步】，所以先介绍与时间服务器同步再介绍定时同步

1. 在系统时间设置界面，单击时间服务器一行的下拉框选择同步时间的时间服务器，如图 5.9 所示

图 5.9 选择同步的网络时间服务器

2. 选定时间服务器后，单击右侧的设置图标，系统弹出提示对话框如图 5.10 所示。

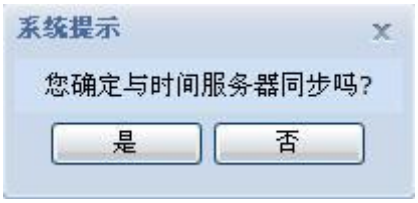


图 5.10 是否与网络时间进行同步

3. 单击【是】防毒墙系统时间与网络时间服务器进行同步，如图 5.11 所示；单击【否】取消操作。

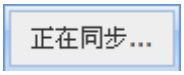


图 5.11 防毒墙时间同步进度

提示：关于同步失败提提示

如果网络时间服务器不可访问，则返回同步失败的提示框，如图 5.12 所示

图 5.12 同步时间失败

5.1.2 软件升级

软件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【系统维护】进入软件升级页面，如图 5.13 所示。

图 5.13 软件升级设置界面

对软件升级界面各字段我们做如下说明：

字段	说明
当前病毒库	显示当前正在使用的病毒库版本信息
引擎信息	显示当前使用反病毒引擎版本信息及有效期
定时升级	显示当前是否启用定时升级
系统版本	显示当前系统版本相关信息

【代理设置】	通过代理方式进行病毒库升级
【智能升级】	单击防毒墙下载升级包自动升级
【本地升级】	单击选择用户下载到本地的升级包对病毒库进行升级
	设置图标，单击此图标可以进行病毒库和引擎定时升级的设置
【系统升级】	单击进行系统升级

表 5.2 软件升级界面各字段说明

- **病毒库升级**

病毒库升级关系到防毒墙的实际使用效果，为了更好的进行病毒过滤，请及时升级防毒墙病毒库。防毒墙病毒库升级有两种方式，分别为智能升级和手动升级。

✓ **代理设置**

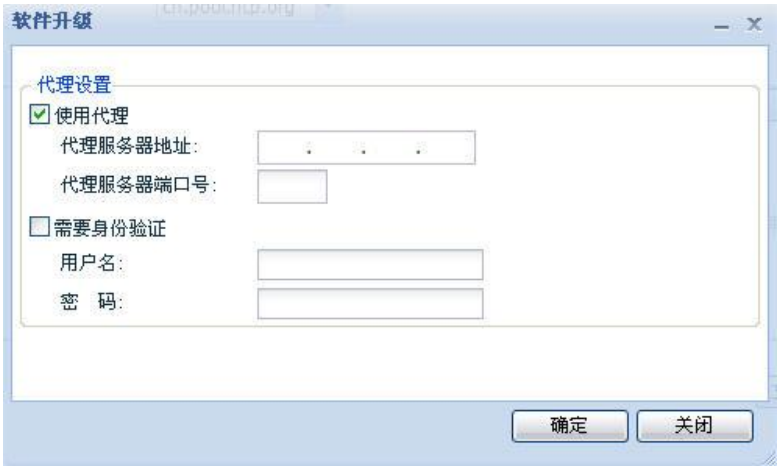


图 5.14 代理服务器详细设置

1. 在代理服务器地址和代理服务器端口处输入代理服务器的地址和端口，单击【确定】完成代理服务器设置
2. 如需验证，单击【需要身份验证】前的单选框，输入验证信息后，单击【确定】完成代理服务器设置

✓ **智能升级**

在系统维护界面当前病毒库一行单击【智能升级】按钮，进入智能升级界面如图 5.15 所示。图中进度条显示升级进度。

图 5.15 病毒库智能升级提示界面

单击【停止】会强行中止升级操作。

✓ **本地升级**

对于军队、公安等保密性较强的专用网络，或者是网络状况不稳定的网络，在使用防毒墙自动升级访问瑞星升级网站有障碍的情况下，可以通过登录瑞星主页下载病毒库升级包到本地主机，然后通过上传本地升级包到防毒墙对防毒墙进行升级。关于病毒库升级包的下载，请参见《快速使用指南》。

1. 登录瑞星主页下载病毒库升级包到本地主机。
2. 单击系统维护软件升级界面【本地升级】按钮，进入本地升级界面，如图 5.16 所示。

图 5.16 本地升级时选择病毒库升级包界面

3. 单击【浏览】进入病毒库升级包选择界面，如图 5.17 所示

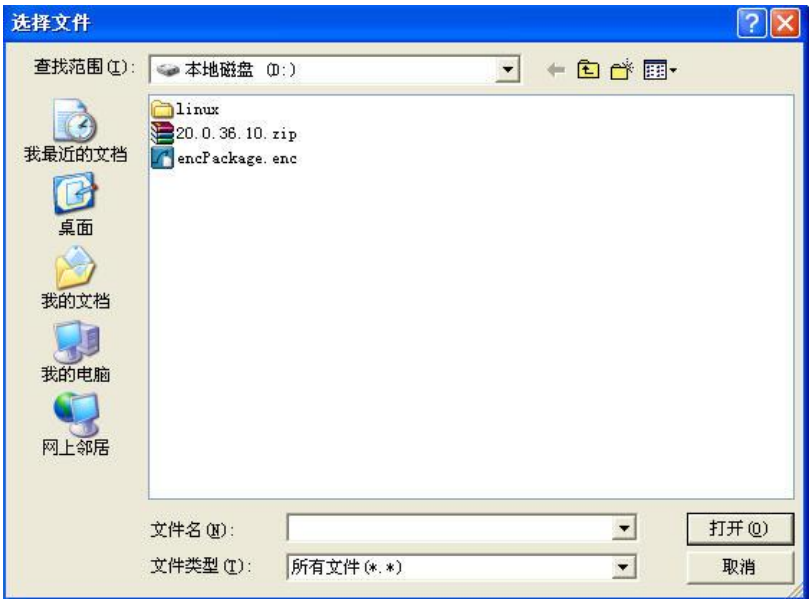


图 5.17 病毒库升级包选择界面

4. 选择病毒库升级包，单击【打开】选中升级包
5. 在选择文件处显示被选取文件的详细路径，如图 5.18 所示

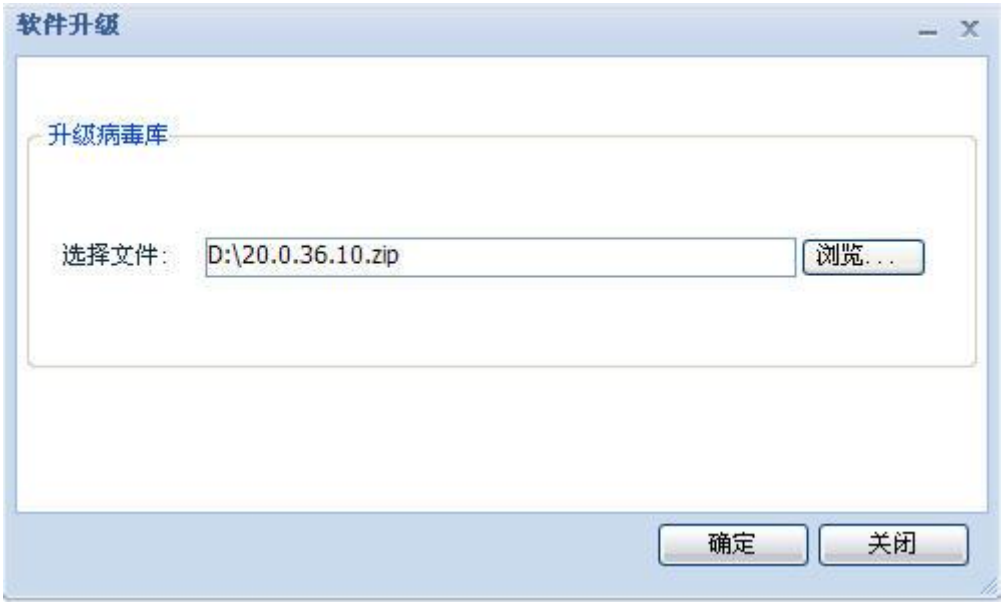


图 5.18 病毒库升级文件路径界面

6. 单击【确定】进行病毒库升级，单击【关闭】取消操作。

- **引擎信息查询**

在软件升级界面可以直接查看引擎信息，如图 5.19 所示

图 5.19 引擎信息提示界面

对引擎信息提示界面各字段我们做如下说明：

字段	说明
反病毒引擎版本	显示反病毒引擎当前版本
有效期	显示当前反病毒引擎的有效期限，若是反病毒引擎失效，将无法进行病毒库升级

表 5.3 引擎信息提示界面各字段说明

- **定时升级**

为了减少管理员的操作负担，瑞星防毒墙配备了定时升级的功能，管理员只需设置定时升级的时间，防毒墙将在设置的时间通过网络自动下载升级包对病毒库和引擎进行升级，定时升级还可以避免病毒库升级不及时导致防毒墙能力下降。

单击软件升级界面【定时升级】一行的设置图标，进入定时升级设置界面，如图 5.20 所示。

图 5.20 定时自动升级病毒库

单击启动左侧的复选框表示启动定时升级，输入定时升级时间，单击【确定】保存设置，单击【关闭】取消操作。管理员可以在软件升级板块直接查看定时升级是否启用，如图 5.21 所示。

图 5.21 查看定时升级是否启用界面

- **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 5.22 所示

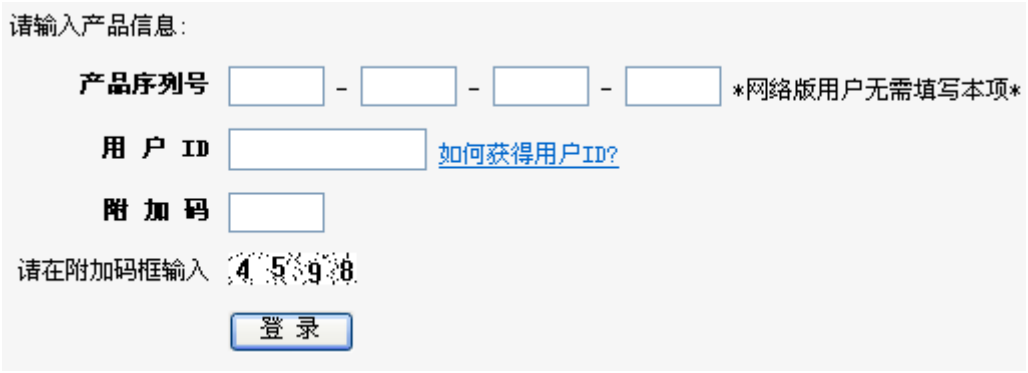


图 5.22 用户登录页面

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. 单击软件升级界面系统版本一行的设置图标，会弹出如图 5.23 所示的界面

图 5.23 选择系统升级包界面

5. 单击【浏览】即可浏览选择系统升级包，如图 5.24 所示

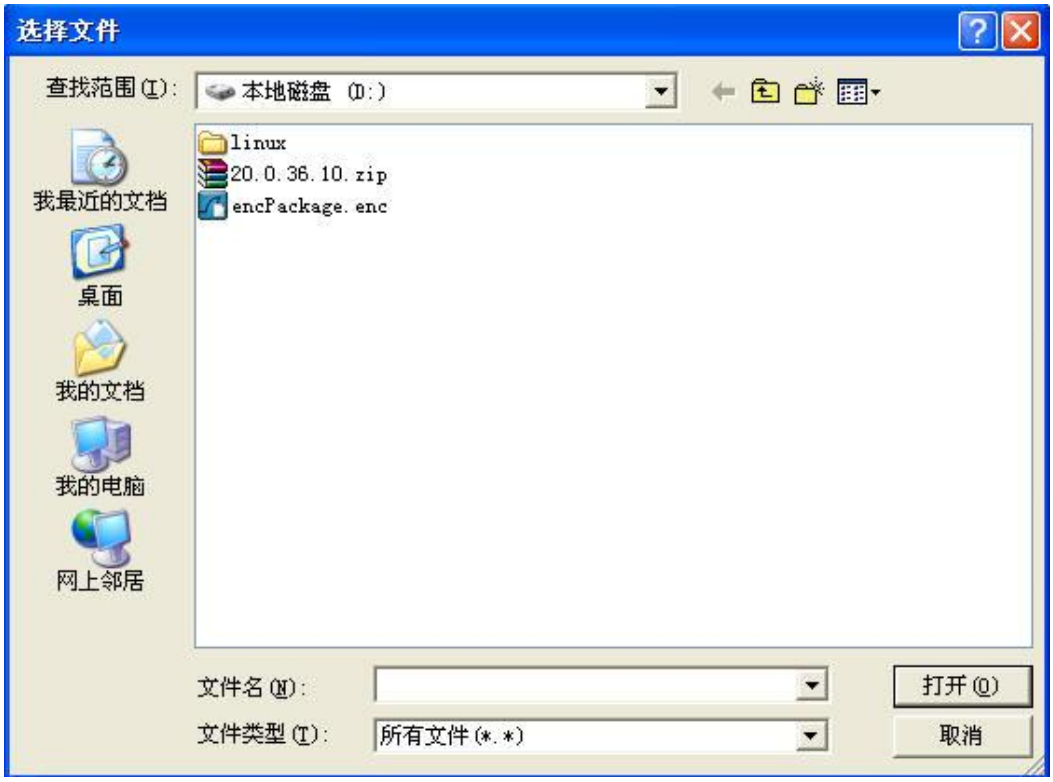


图 5.24 选择系统升级包界面

6. 选择系统升级包，单击【打开】选中升级包。

7. 在选择文件处显示被选取文件的详细路径，如图 5.25 所示

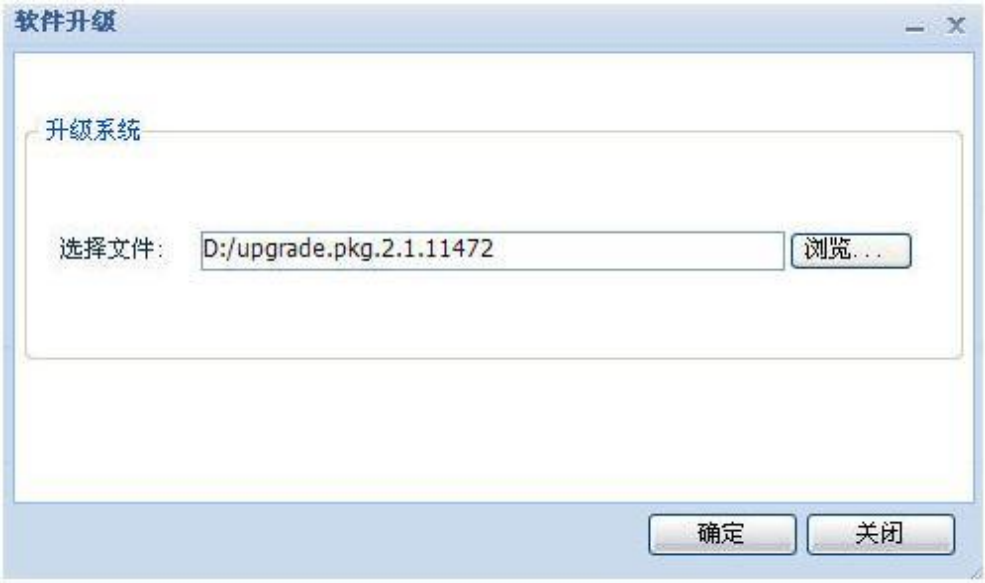


图 5.25 系统升级文件路径界面

8. 单击【确定】按钮开始系统升级，单击【关闭】按钮取消操作。

5.1.3 备份管理

当防毒墙因配置错误不能正常工作时，防毒墙备份管理功能可将防毒墙恢复到某个时间点的正确配置状态。 备份管理有立即备份和备份管理两种操作。管理员可以通过立即备份操作及时的对防毒墙系统设置

信息进行备份，管理员可以通过备份管理管理防毒墙的备份信息，例如下载、删除备份文件、用备份文件恢复系统、恢复出厂设置等。备份管理界面如图 5.26 所示。

图 5.26 备份管理主页面

- **立即备份**

为了备份当前的系统配置，用于日后恢复系统，用户可以执行立即备份操作。

1. 单击系统维护主页面的【立即备份】按钮，系统会弹出如图 5.27 所示的提示界面，给备份文件输入注释信息。

图 5.27 备份系统

提示：关于备份信息

输入信息主要为此次备份加一个注释，以便区分不同的备份，方便以后的管理。

2. 单击【确定】完成备份操作，系统弹出正在备份系统提示信息如图 5.28 所示；单击【取消】取消操作。

图 5.28 正在备份系统提示界面

注意：为节省存储空间，防毒墙存储 5 个备份记录，当备份记录超过 5 个时，系统会弹出如图 5.29 所示的提示信息，为了保护重要信息，用户应及时把重要的备份下载到本地保存。

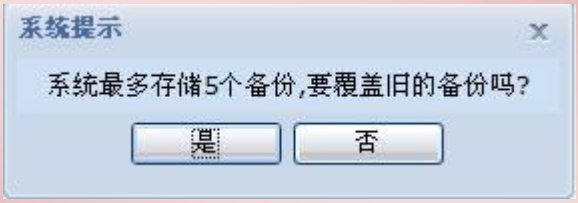


图 5.29 覆盖旧的备份提示

单击【是】按钮，继续进行备份操作，覆盖最早的备份，单击【否】取消操作。

- **备份管理**

单击备份管理主页面中的【备份管理】按钮，进入备份管理界面如图 5.30 所示的界面。

图 5.30 备份恢复界面

备份管理主要包括备份恢复、本地恢复和出厂恢复三个功能模块，以下我们将分别讲述这三个模块的功能及使用。

✓ **备份恢复**

单击备份管理界面中的【备份管理】按钮，即可进入备份恢复界面，如上图 5.30 所示，对于备份恢复界面各字段我们做以下说明：

字段	说明
序号	对备份文件根据时间进行排序
备份时间	显示该备份的时间
备份信息	显示备份时用户输入的备份信息
操作	用户可以对备份执行的操作包括【下载】备份到本地主机、【删除】备份和用备份【恢复】防毒墙设置

表 5.4 备份恢复界面各字段说明

- **备份文件的下载**

防毒墙系统最多可以存储五个备份文件信息，当系统已有五个备份文件的情况下，若是用户需要备份当前防毒墙配置，系统会采用覆盖最早备份的形式存储新的备份。所以用户应当及时的将备份文件下载到本地保存，这样既为新的备份提供了存储空间，又避免了重要备份信息的丢失。

1. 在备份恢复界面单击要下载的备份文件操作一列【下载】，进入备份文件下载界面，如图 5.31 所示

图 5.31 备份文件下载

2. 输入备份文件密码，为避免不法分子对防毒墙的恶意更改，在管理员用该备份文件进行系统恢复时，系统会要求管理员输入密码进行验证。

3. 单击【确定】，进入密码确认界面，如图 5.32 所示；单击【取消】按钮取消下载备份文件操作。

图 5.32 备份文件下载密码确认界面

4. 重复输入密码

5. 单击【确定】，进入文件下载界面，如图 5.33 所示

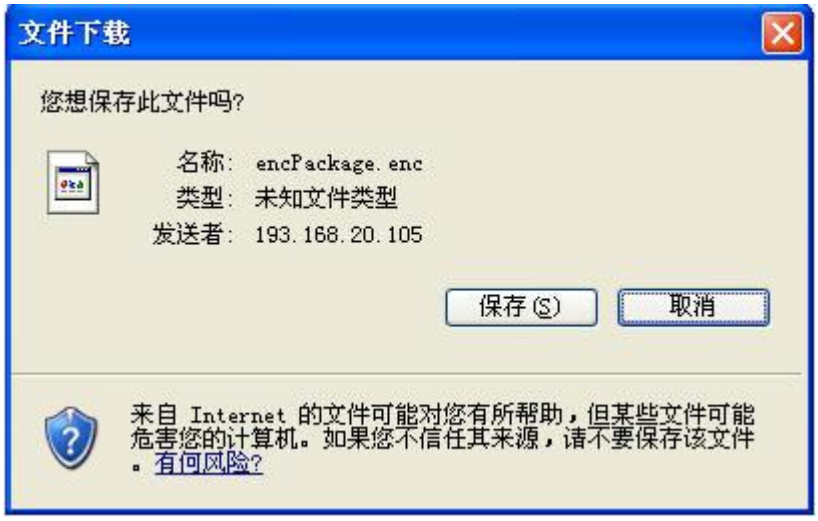


图 5.33 下载文件界面

6. 单击【保存】下载备份文件到本地，进入路径选择界面如图 5.34 所示。单击【取消】取消操作。

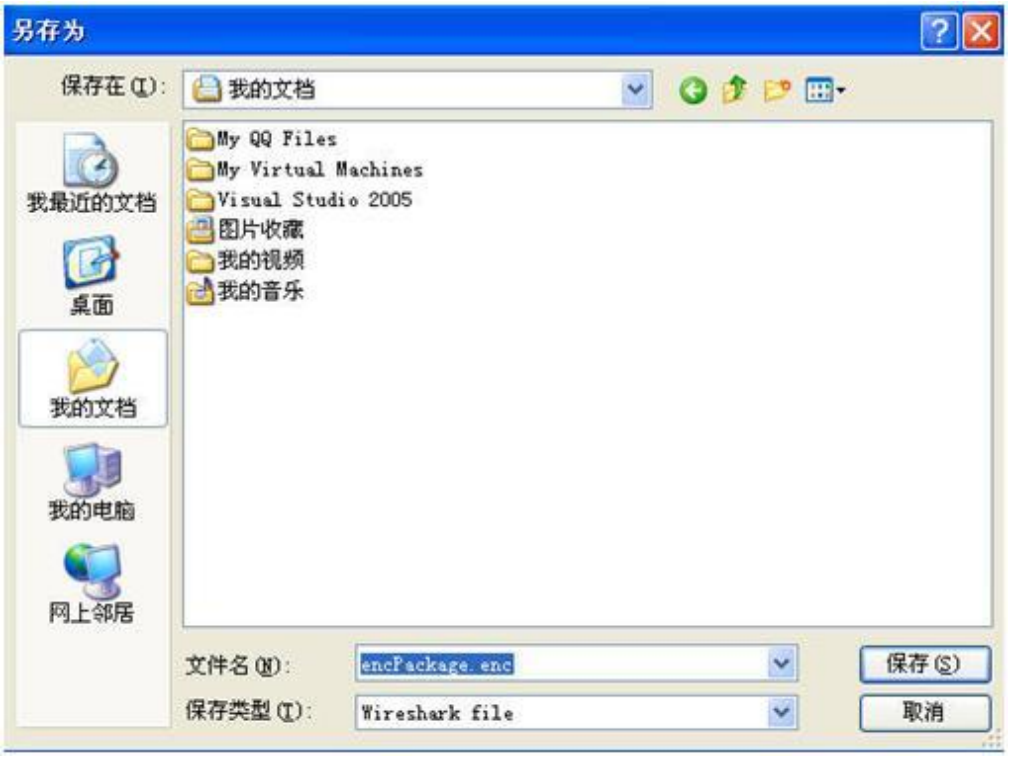


图 5.34 下载文件路径选择

7. 选择文件的保存路径，单击【保存】下载文件，单击【取消】取消操作。

下载完毕系统将会弹出下载完成提示信息，单击【关闭】下载备份文件操作完成。如图 5.35 所示。

图 5.35 下载备份完毕提示对话框

- **备份文件的删除**

如果用户觉得备份文件已没有意义，需要删除防毒墙上的备份文件，请按以下步骤进行操作：

1. 在备份恢复界面单击要删除的备份文件操作一列【删除】，进入备份文件删除界面，如图 5.36 所示。

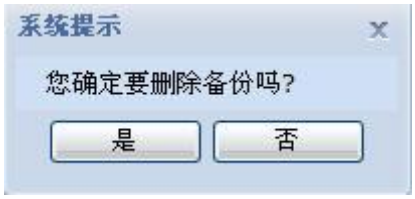


图 5.36 删除备份文件确认界面

2. 单击【是】删除备份文件，单击【否】取消操作。

- **备份文件的恢复**

如果用户需要用防毒墙系统上的备份文件恢复防毒墙系统设置，可以进行备份文件恢复，操作如下：

1. 在备份恢复界面单击用户需要用来恢复的备份文件操作一列【恢复】，进入如图 5.37 所示界面

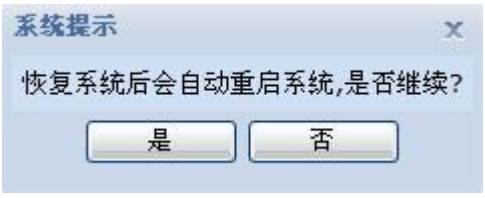


图 5.37 确认恢复界面

2. 单击【是】继续恢复操作，防毒墙重新启动，如图 5.38 所示。单击【否】取消操作。

图 5.38 系统重新启动提示界面

3. 防毒墙重新启动以后返回系统登录界面。

✓ **本地恢复**

如果用户想要将防毒墙配置恢复到以前某个时间点，并且当时的配置信息用户已备份并且下载保存在管理主机时，可以按照如下操作进行：

1. 在系统维护界面单击【备份管理】➔【本地恢复】，系统将进入如图 5.39 所示的界面。

图 5.39 选择下载到本地的备份文件进行恢复

2. 单击【浏览】按钮，选择从防毒墙下载到本地的备份文件，如图 5.40 所示

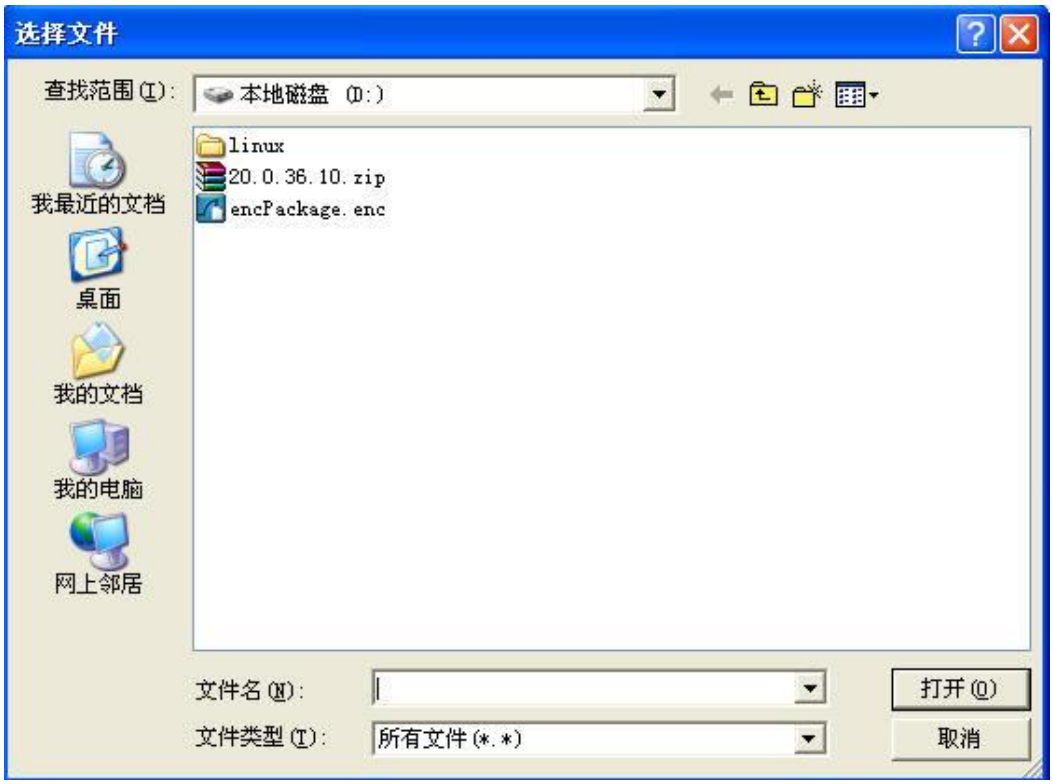


图 5.40 选择系统升级包界面

3. 单击选中备份文件，单击【打开】返回本地恢复界面，如图 5.41 所示。

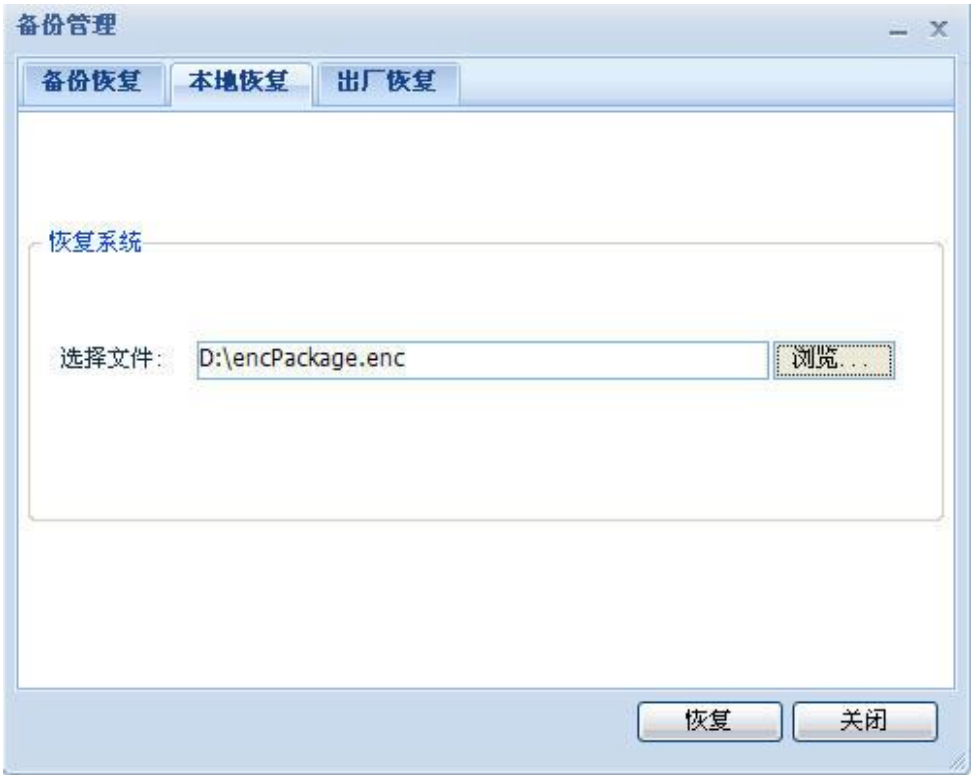


图 5.41 本地恢复文件路径界面

4. 单击【恢复】按钮，把防毒墙配置恢复到备份文件的设置，单击【关闭】按钮取消操作。

✓ **出厂恢复**

当用户对防毒墙作了过多的更改而备份恢复又不能满足用户的恢复需要时，可以选择出厂恢复。恢复到防毒墙出厂时的设置，用户可以根据用户手册对防毒墙重新设置。

1. 在系统维护界面单击【备份管理】➔【出厂恢复】，系统将进入如图 5.42 所示的界面。

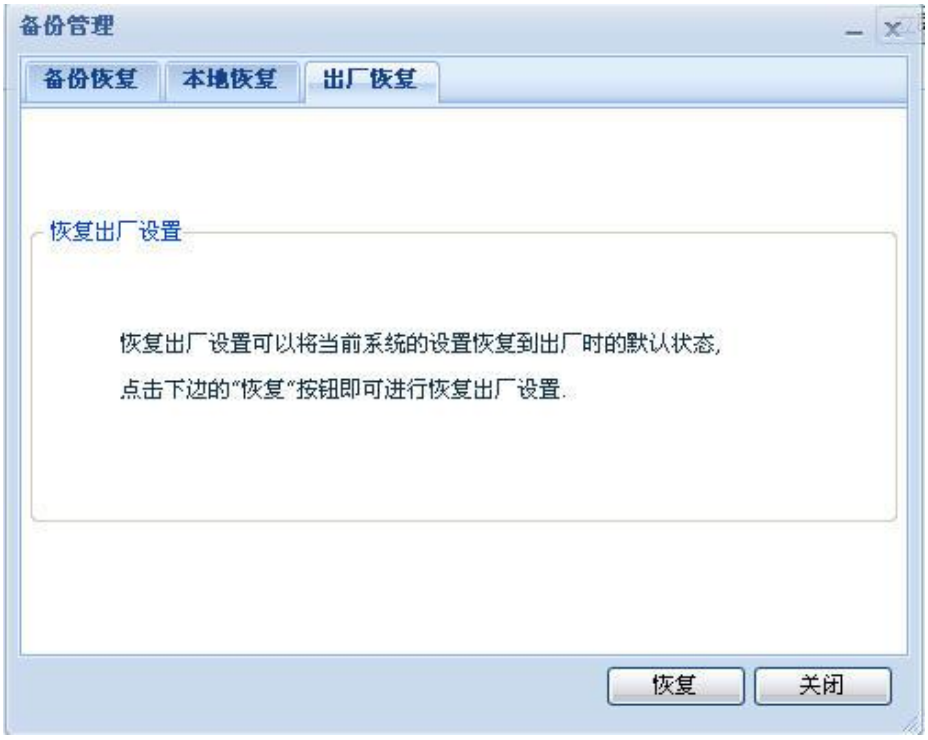


图 5.42 出厂恢复界面

2. 单击【恢复】，系统弹出确认提示界面，如图 5.43 所示

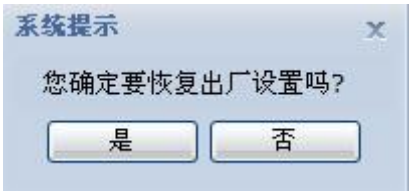


图 5.43 确认恢复出厂界面

3. 单击【是】即可使防毒墙设置恢复到出厂状态，单击【关闭】取消操作。

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。

5.1.4 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【系统维护】➔【系统维护】，SSL 证书管理如图 5.44 所示。

图 5.44 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【确定】按钮保存设置，系统弹出需要重新登录的对话框，如图 5.45 所示

图 5.45 系统 SSL 生成证书

3. 单击图 5.45 中的【是】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 5.46 所示

图 5.46 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 5.47 所示

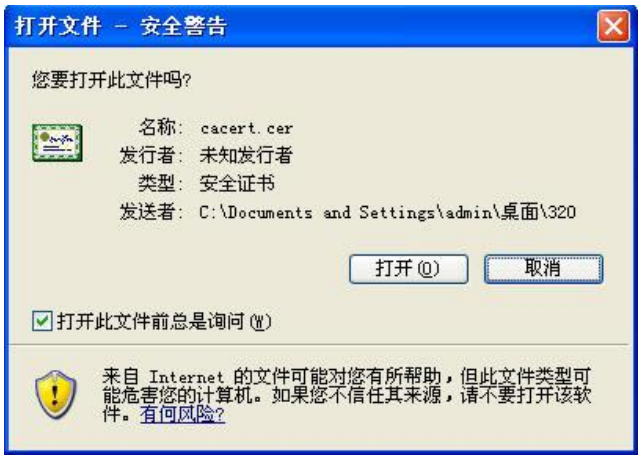


图 5.47 打开证书系统提示

6. 单击【打开】，如图 5.48 所示

图 5.48 防毒墙 SSL 证书

7. 选择【安装证书】，如图 5.49 所示

图 5.49 导入证书

8. 选择【下一步】，如图 5.50 所示

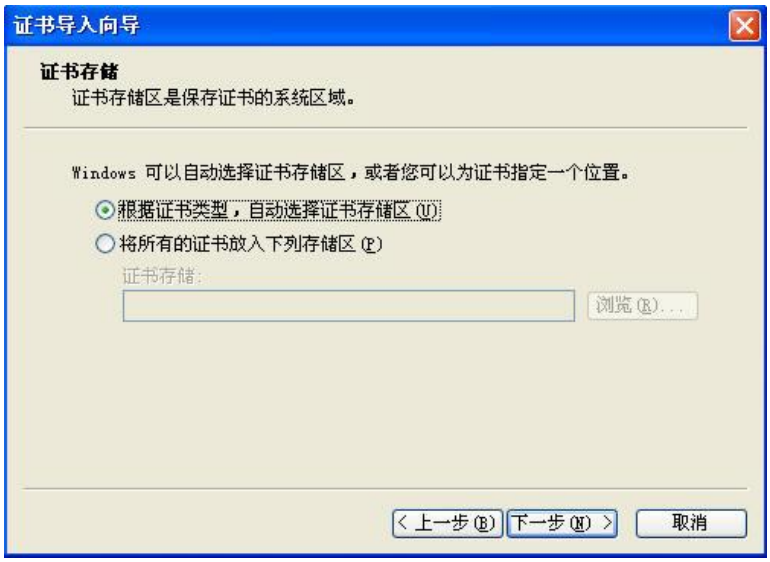


图 5.50 选择证书的存书类型

9. 选择【下一步】，如图 5.51 所示，单击【完成】按钮完成证书导入。

图 5.51 完成证书导入

10. 系统返回导入成功提示框，如图 5.52 所示

图 5.52 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。

5.2 帐号管理

企业存在多个管理员的情况下，管理员通过合法帐号登录防毒墙，并对用户帐号进行管理。单击【系统维护】➔【帐号管理】进入帐号管理界面，如图 5.53 所示

图 5.53 帐号管理界面

帐号管理界面各字段说明如下

字段	说明
增加管理员	单击可以进入增加管理员界面，可以增加防毒墙管理员
序号	将当前管理员以阿拉伯数字排序
状态	显示当前管理员的连接状态， 表示管理员在线， 表示管理员不在线， 表示管理员被锁定
管理员	显示当前登录的管理员用户名
允许登录 IP 范围	表示允许该管理员帐号可以从哪些 IP 登录到防毒墙。0.0.0.0/0 表示允许任何 IP 登录到防毒墙进行管理
已登录数	该帐号从不同地址登录的数量
	扩展图标，单击此图标可以查看在线管理员更多详细信息
操作	修改图标，单击此图标可以修改管理员帐号信息; 删除图标，单击此图标可以删除管理员帐号； 解锁图标，单击可以为锁定的用户解锁

表 5.5 帐号管理界面相关字段说明

提示：关于自动锁定管理员帐号和帐号的解锁

为保障防毒墙的使用安全，瑞星防毒墙设置了自动锁定帐号的功能，在当用户尝试登录超过系统默认的尝试登录次数后，而没有登录成功，系统将自动锁定帐号，默认的最大尝试登录次数为 4 次。用户帐号被锁定之后，除非用其他管理员帐号登录防毒墙进行解锁操作，否则该帐号将一直不可用。若是系统没有设置其它帐号而 admin 帐号被锁定，管理员可以通过串口模式登录防毒墙，若是用户以 admin 帐号在串口模式下登录成功，帐号将自动解锁。

5.2.1 添加新帐号

1. 在帐号管理界面单击【增加管理员】，弹出如图 5.54 所示的界面，新增帐号默认为管理员权限。

图 5.54 增加新帐号

2. 填写用户名：进行防毒墙系统登录的用户名（最多为 20 个字符）

3. 填写密码：登录密码（6-16 位），系统会提示密码强度

4. 重复密码：再次输入密码，防止误操作

5. 单击【确定】完成帐号的添加操作。

5.2.2 查看在线管理员信息

用户可以通过单击已登录数中的扩展图标，查看当前在线管理员信息，如图 5.55 所示。

图 5.55 查看当前登录用户

查看当前登录用户信息界面各字段说明

字段	说明
序号	将当前管理员以阿拉伯数字排序
访问方式	显示当前管理员访问防毒墙的方式 ，有 WEB、SSH 和 console 三种方式
访问 IP	管理员访问防毒墙使用的 IP 地址
空闲时间	管理员最近未对防毒墙执行任何操作的时间。用于在用户长时间脱离防毒墙时启用超时报警，需要管理员重新登录，以保障防毒墙本身的安全性
踢出	单击此按钮时，可以强行拒绝管理员访问防毒墙

表 5.6 查看当前登录用户界面各字段信息说明

5.2.3 修改帐号信息

防毒墙是企业的一座安全屏障，管理员可以通过用户帐号登录到防毒墙对防毒墙进行管理和设置，为了避免防毒墙的帐号被不法分子盗取对企业造成不必要的损失，建议用户不要设置过于简单的密码并且尽可能不要一个密码使用过长时间。管理员可通过修改帐号信息设置新密码。

1. 单击帐号一行操作选项中的修改图标，弹出如图 5.56 所示的界面

图 5.56 修改管理员信息界面

2. 填入新密码，若是管理员不需要修改密码，密码部分不填即可
3. 重复修改的密码，防止误操作
4. 修改允许地址/掩码（不修改则默认为原来的配置）
5. 单击【确定】完成修改帐号操作。

5.2.4 删除帐号

用户想删除管理员帐号时，单击用户帐号一行的删除图标，系统弹出确认提示对话框如图 5.57 所示。

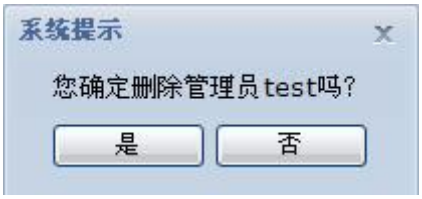


图 5.57 删除管理员确认提示界面

单击【是】删除帐号，系统弹出删除管理员帐号成功提示对话框，如图 5.58 所示；单击【否】取消操作

图 5.58 删除管理员成功

单击【确定】按钮，完成删除帐号操作。

5.3 网络诊断

单击【系统维护】➔【网络诊断】即可进入网络诊断界面。如图 5.59 所示。

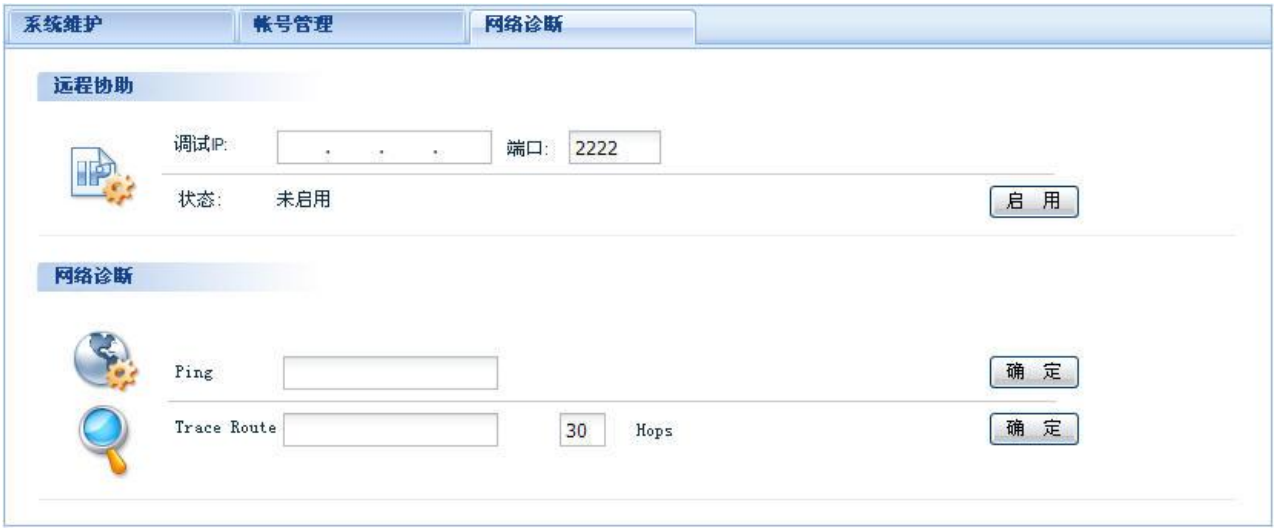


图 5.59 网络诊断界面

本节主要介绍以下两个模块的功能及使用：

- 远程协助：当瑞星防毒墙出现技术上的故障时，通过设置此部分内容获取瑞星工程师的技术支持
- 网络诊断：通过 Ping 和 Trace Route 命令来诊断网络

5.3.1 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【系统维护】➔【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【启用】，系统提示如图 5.60 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 5.60 远程协助界面

单击【停止】取消远程协助操作。

5.3.2 网络诊断

- Ping

在网络诊断界面，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：关于 ping 操作时的 IP 地址**
>
> 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【确定】开始网络诊断

3. Ping 测试的结果如图 5.61 所示

图 5.61 Ping 功能测试页面

- Trace Route

在网路诊断界面，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：关于 Trace Route 操作时的 IP 地址**
>
> 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，单击【确定】开始路由跟踪。跟踪路由示例如图 5.62 所示。

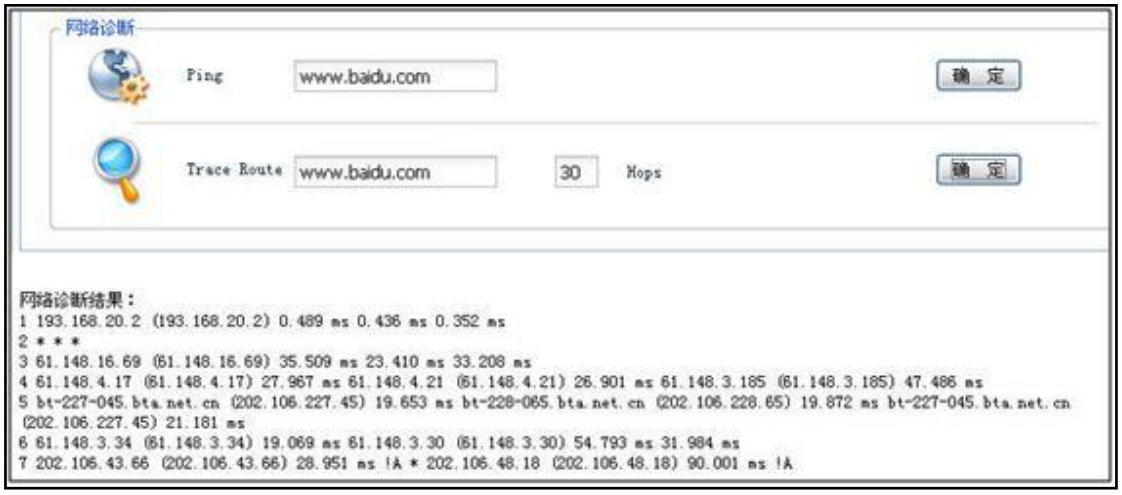


图 5.62 测试跟踪路由页面

提示：关于 HOPS 的解释

Trace Route 后面的 Hops 表示在网络诊断时追踪到的最远路由器数，即数据包最多经过多少个路由器转发到达目的 IP，若在规定的最大路由器转发数目内到不了，则认为不可达。

第六章 内网管理

本章主要介绍以下三个模块的功能和使用：

- 主机信息：进行内网主机相关信息的统计和管理，包括 MAC 绑定、流量控制、带宽管理、主机组管理和接口流量
- 主机历史：统计内网主机历史信息，管理员可根据需要按条件查询主机历史信息，防毒墙会对内网潜在的不安全信息发出警告，例如一个主机用多个 IP 接入网络或者不同主机用相同的 IP 接入网络时，会显示警告信息
- 端口映射：端口映射的作用是使互联网的用户能访问到局域网的服务器。

6.1 主机信息

主机信息主要用于当前内网主机相关信息的统计，管理员可以根据防毒墙提供的信息制定相应的管理方案。

6.1.1 主机信息的查看和修改

- **查看主机信息**

为方便管理员根据内网主机的实际使用情况适时的制定防毒墙管理策略，在主机信息界面可以查看内网主机的重要信息如主机 MAC 地址、IP 地址、名称等，还有主机流量信息的查看。下面我们分别介绍主机基本信息的查看和主机流量信息的查看。

✓ **查看主机基本信息**

单击【内网管理】➔【主机信息】进入内网管理中主机信息界面，此界面可以查看当前内网主机相关信息，如图 6.1 所示。

图 6.1 主机信息界面

提示：关于红色字体的解释

当内网主机 IP 和 MAC 地址冲突（即 IP 与 MAC 不一一对应）的时候字体会显示为红色，提醒管理员查看具体情况，核实 IP 与主机 MAC 的对应情况，将 IP 与 MAC 绑定，避免合法用户的 IP 被别人抢用，确保内网安全有序。

对于主机信息界面相关字段我们做如下说明：

字段	说明
【MAC 绑定】	单击进入 MAC 绑定相关界面，进行 MAC 绑定相关的管理
【流量控制】	单击进入流量控制界面，进行内网流量控制的管理
【带宽管理】	单击进入带宽管理界面，进行带宽管理
【主机组管理】	单击进入主机组管理界面，进行主机组管理相关设置
【接口流量】	单击可以进入接口流量查询界面
序号	按阿拉伯数字排序，便于统计主机数目及对相关主机的操作
名称	显示主机的名称，单击可以按字母表顺序将名称排序
MAC	显示主机的网卡物理地址，单击可以按 MAC 地址升序或降序显示
IP	显示主机 IP 地址，默认按主机 IP 地址升序显示，单击可以切换主机显示顺序按 IP 升序或是降序显示
接口	显示主机连接的防毒墙的接口，单击可以按接口序号升序或者降序排序显示
流量信息	经过该主机的信息流量统计值以及为主机配置的流量管理策略，单击可以按流量信息升序或者降序排序显示；单击主机对应的流量信息可以进入流量信息查看界面
带宽管理	显示管理员为主机设置的带宽控制信息以及为主机配置的带宽管理策略，单击可以按带宽控制信息升序或者降序排序显示
状态	显示当前用户状态，在线用户状态用 图标表示，不在线用 表示；当把鼠标悬停在状态图标上可以显示当前主机的状态信息，包括主机当前状态，是否在线和上线时间或是离线时间，例如：未锁定 当前在线 上线时间 14：00 为一条完整的提示信息
主机组	显示当前主机所属主机组信息，单击按主机组分组显示
操作	单击 图标（以下简称修改图标）可以修改主机信息

表 6.1 主机信息界面各字段说明

✓ **查看主机流量信息**

在主机信息查看界面单击所要查看【流量信息】一列的流量统计值，这里我们以查看 193.168.20.226 的流量信息为例。

单击主机 IP 为 193.168.20.226 一行的【流量信息】一列，进入如图 6.2 所示界面。

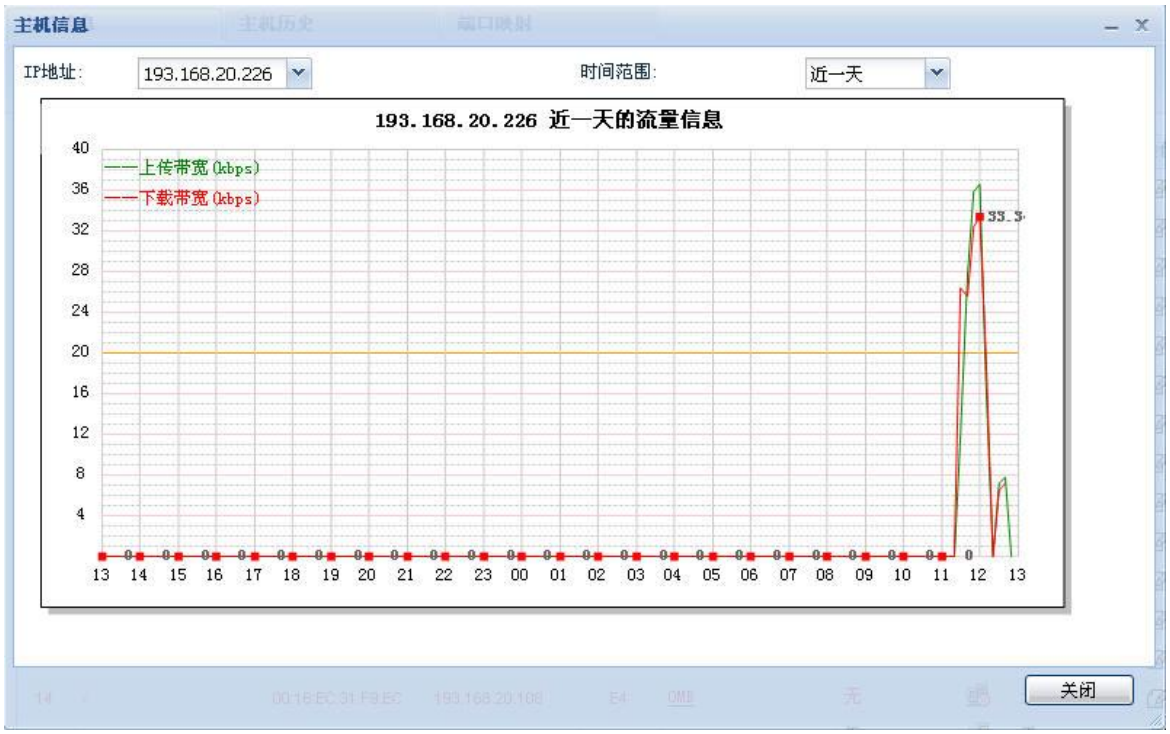


图 6.2 主机流量信息查看界面

对流量信息查看界面字段作如下说明：

字段	说明
IP 地址	当前显示的流量信息的主机 IP
时间范围	流量信息界面显示在时间范围内用户主机的流量信息 此处设置的时间范围有近一天和近一周两个选项，管理员可以选择不同的时间范围查看主机近一天或是近一周的上传、下载流量信息
上传带宽(kbps)	绿色曲线表示上传带宽
下载带宽(kbps)	红色曲线表示下载带宽
横坐标	显示选取的时间范围。若是选择近一天，取当前时间沿顺时针方向趋向的整点值，向前推 24 小时，例如：当前时间为 14：20，则近一天时间为昨天 15：00 到今天 15：00；若是选择近一周，时间坐标表示以今天为最后一天往前推算一周例如今天是 8 月 8 日，则时间坐标为 8 月 2 日到 8 月 9 日 0 点。
纵坐标	具体的时间对应的用户主机流量

表 6.2 主机流量信息查看界面说明

提示：关于修改查询条件

用户若是要查看其它内网主机用户的流量信息，可以单击 IP 地址栏后的下拉菜单，从中选择需要查询的用户主机 IP 地址，防毒墙会自动刷新显示界面。用户要更改查询时间范围，只需单击时间范围栏里的下拉菜单条选择时间范围即可。

- 修改主机信息

在主机信息界面，单击要修改的主机【操作】一列的修改图标，进入主机信息修改界面如图 6.3 所示。

图 6.3 修改主机信息界面

1. 填写主机名称
2. 选择主机组，如果有主机组的话，从下拉框中选择。防毒墙默认没有添加任何主机组，管理员为方便管理内部网络可以添加主机组，关于主机组的详细讲解请参看 6.1.5 主机组管理。

6.1.2MAC 绑定

为了规范企业内部网络环境，增加网络的安全性，防毒墙提供了 MAC 绑定的功能，将用户 IP 与主机 MAC 绑定，规定某一 IP 只对应于某一特定的网卡(每个网卡具有唯一的 MAC 地址)，即限定一个 IP 地址只能在一台指定的计算机上使用。当某台计算机通过防毒墙访问 Internet 时，防毒墙要检查其发出的数据中的 IP 以及 MAC 是否与防毒墙上的规定相符，如果相符就放行，否则不允许通过防毒墙。这样可大大方便网络的 IP 地址管理且可防止企业内部 IP 地址混乱的状态。在主机信息界面单击【MAC 绑定】进入 MAC 绑定设置界面，如图 6.4 所示。

图 6.4 MAC 绑定设置界面

对 MAC 绑定界面相关字段作如下说明：

字段	说明
【手动绑定】	单击进入 MAC 地址手动绑定界面
【全部绑定】	单击可以设置对当前内网中的所有在线主机的 MAC 绑定
【全部取消绑定】	单击可以设置取消内网中所有 MAC 绑定
【导出记录】	单击可以导出当前 MAC 绑定记录
【导入记录】	单击可以进入导入 MAC 绑定记录界面，可根据导入记录设置 MAC 绑定
序号	按阿拉伯数字进行排序，显示内网所有主机
名称	显示主机的名称，单击可以按字母表顺序将名称排序
MAC	显示主机的网卡物理地址，单击可以按 MAC 地址升序或降序显示
IP	显示主机 IP 地址，默认按主机 IP 地址升序显示，单击可以切换主机显示顺序按 IP 升序或是降序显示
操作	包括绑定、取消绑定和删除三种操作，单击 图标（以下简称绑定图标）执行 MAC 绑定操作，单击 图标（以下简称解除绑定图标）执行解除绑定操作。

表 6.3 MAC 绑定界面相关字段说明

- **手动绑定**

防毒墙提供两种方法进行手动绑定，一种是单击绑定图标进行绑定；另一种是手动输入 IP 地址和 MAC 地址信息，单击【绑定】进行绑定。

✓ **单击绑定图标进行绑定**

1. 在 MAC 绑定设置界面查找所要绑定的主机 MAC 地址及要绑定的用户 IP 地址，如图 6.5 所示界面。

图 6.5 MAC 地址绑定界面

2. 单击 图标执行 MAC 绑定操作，单击 图标执行解除绑定操作。

图 6.6 绑定成功提示界面

✓ **手动输入 IP 地址和 MAC 地址信息进行绑定**

1. 单击【主机信息】➔【MAC 绑定】➔【手动绑定】，进入手动绑定配置界面，如图 6.7 所示

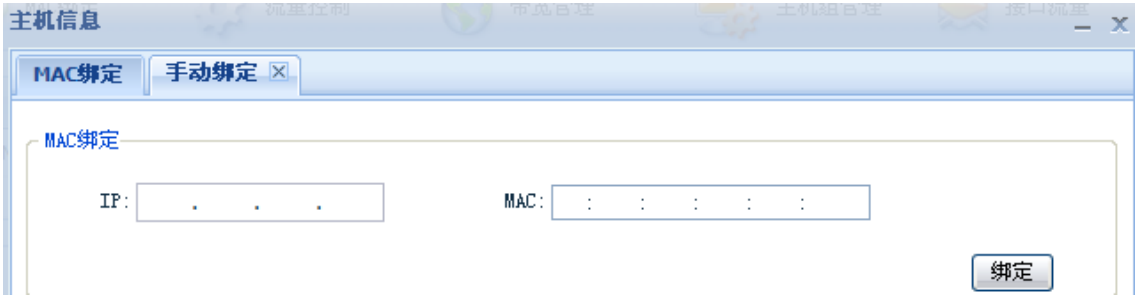


图 6.7 手动绑定界面

2. 填写执行 MAC 绑定的用户 IP 地址
3. 填写执行 MAC 绑定的主机 MAC 地址
4. 单击【绑定】，执行绑定操作。

✓ **取消绑定**

单击执行了 MAC 绑定操作的条目一行解除绑定图标，可以进行取消绑定的操作。

- **全部绑定**

1. 单击【主机信息】➔【MAC 绑定】➔【全部绑定】，进入全部绑定配置界面，如图 6.8 所示。

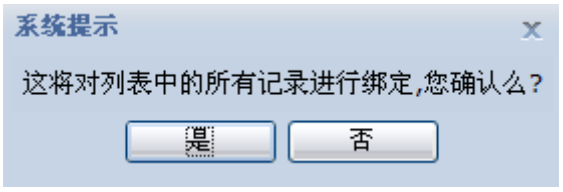


图 6.8 全部绑定系统提示

2. 单击【是】进行内网主机全部绑定操作，单击【否】取消操作。
3. 单击【是】按钮后，系统弹出绑定成功的提示框，如图 6.9 所示。

图 6.9 全部绑定成功

4. 单击【确定】按钮，完成全部绑定操作。

- **全部取消绑定**

1. 单击【主机信息】➔【MAC 绑定】➔【全部取消绑定】，进入全部取消绑定配置界面，如图 6.10 所示。

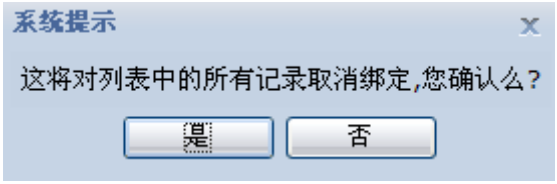


图 6.10 全部取消绑定系统提示

2. 单击【是】取消内网主机设置的全部 MAC 绑定，单击【否】取消操作。
3. 单击【是】按钮后，弹出全部取消绑定成功的提示框，如图 6.11 所示。

图 6.11 全部取消绑定执行成功

4. 单击【确定】按钮，完成全部取消绑定操作。

- **导出记录**

1. 单击【主机信息】➔【MAC 绑定】➔【导出记录】，导出系统当前内网 MAC 绑定信息，如图 6.12 所示。

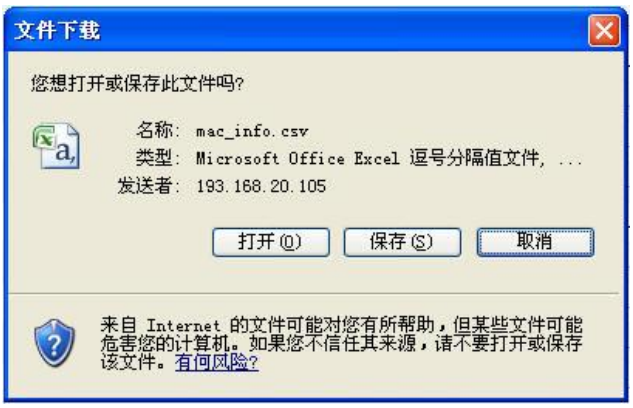


图 6.12 保存导出记录

2. 单击【打开】可以查看当前 MAC 绑定信息；单击【保存】，将进入如图 6.13 所示界面，选择记录要保存的位置；单击【取消】取消操作。

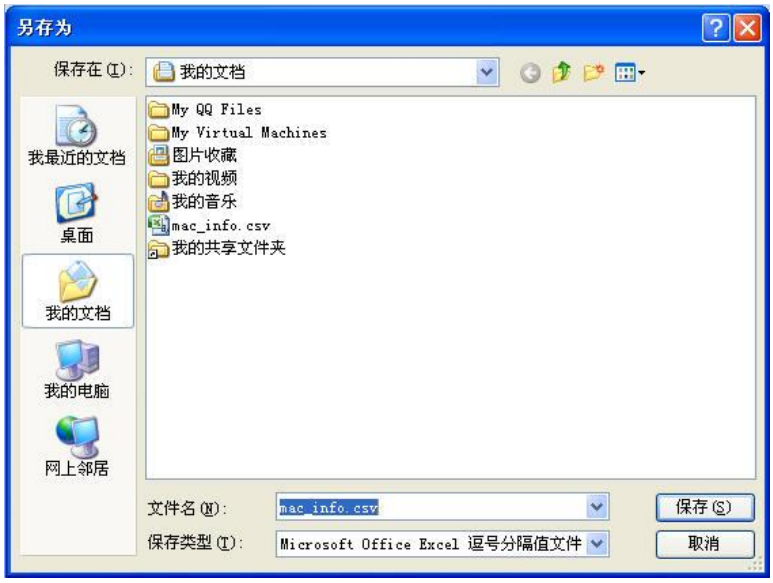


图 6.13 保存界面

3. 单击【保存】按钮，完成导出记录的操作。

- **导入记录**

1. 单击【主机信息】➔【MAC 绑定】➔【导入记录】，防毒墙可根据导入信息进行 MAC 绑定。如图 6.14 所示。

图 6.14 导入 MAC 信息备份文件

2. 单击【浏览】，进入 MAC 信息备份文件选择界面，如图 6.15 所示。

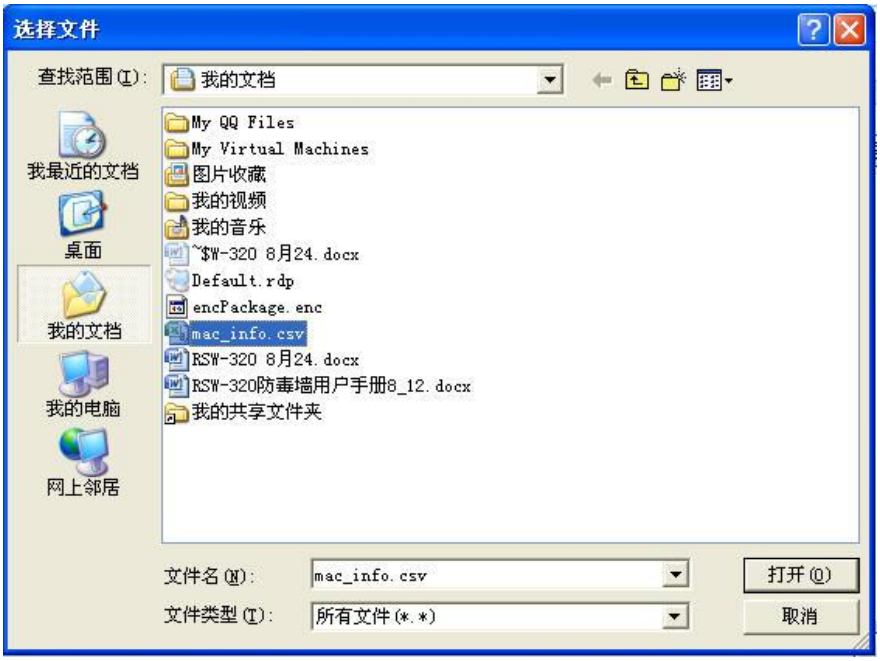


图 6.15 选择导入记录路径

3. 选中保存的 MAC 记录，单击【打开】按钮确认导入文件，如图 6.16 所示。

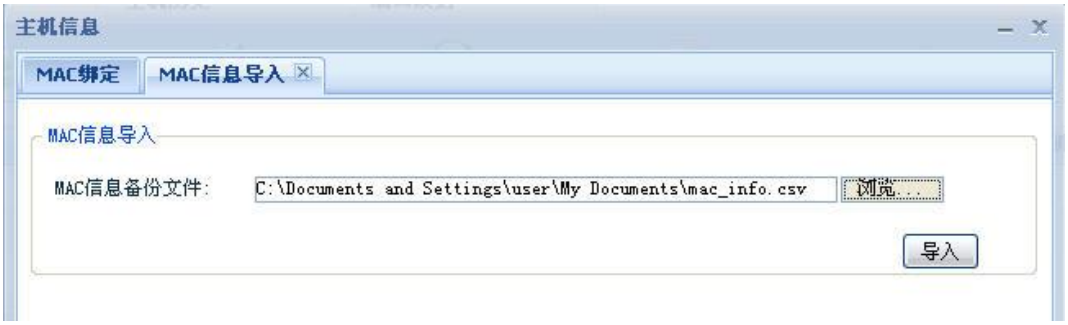


图 6.16 上传导入文件

4. 单击【导入】，若是 MAC 信息备份文件无误则成功导入，弹出提示框如图 6.17 所示。

图 6.17 导入 MAC 记录成功

5. 单击图 6.17 中的【确定】按钮，完成 MAC 记录的导入操作。

- **删除 IP 地址与 MAC 地址的对应暂存表项**

若是管理员要删除 MAC 条目。可以单击 MAC 绑定界面中操作一列的删除图标可以删除该项 MAC 记录。

6.1.3 流量控制

流量控制功能可针对内网某一固定 IP 或网段在单位时间内的数据流量进行控制，流量控制功能方便管理员控制内网主机的上传和下载流量，进行流量管理和流量分析。单击【内网管理】➔【主机信息】➔【流量控制】进入流量控制界面，如图 6.18 所示。

图 6.18 流量控制界面

对流量控制界面各字段作如下说明：

字段	说明

【增加控制】	单击进入增加流量控制界面
序号	按照阿拉伯数字排序
地址/主机组	设置流量控制所控制的网络范围
控制	流量控制所设置的流量上限值
周期	设置控制周期，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。
状态	有已生效和未生效两种状态
操作	有修改和删除两种操作，单击 图标进行流量控制规则的修改操作，单击 图标可以删除设置的流量控制规则

表 6.4 流量控制界面各字段说明

- **增加流量控制**

1. 单击【内网管理】➔【主机信息】➔【流量控制】进入流量控制界面如图 6.19 所示。

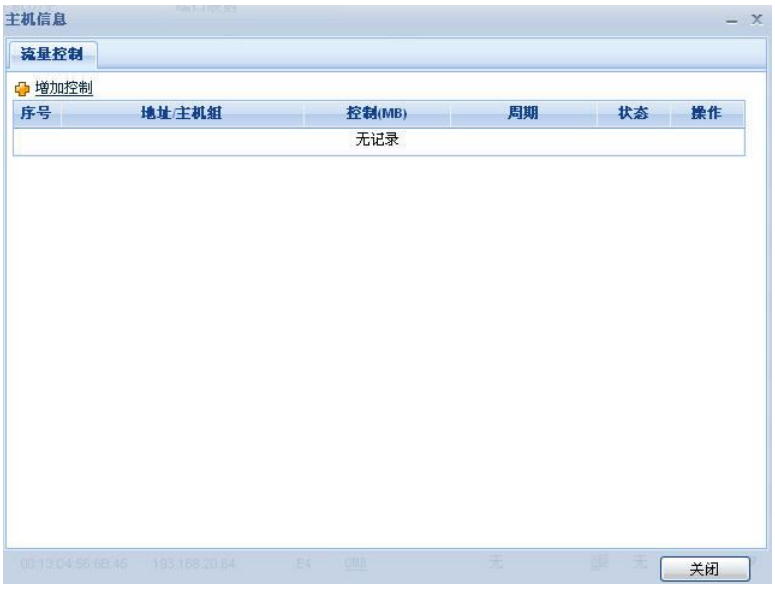


图 6.19 流量控制界面

2. 单击【增加控制】，进入增加流量控制界面如图 6.20 所示。

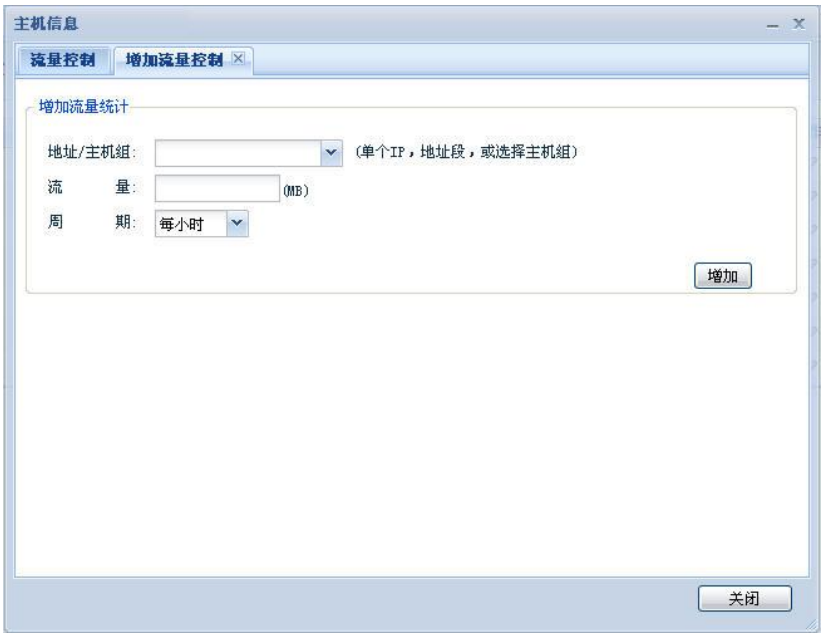


图 6.20 增加流量控制界面

3. 填写流量控制适用的地址或是主机组

> **提示：关于地址和地址组的选择**
>
> 用户可以直接在地址/地址组一栏采用 IP/掩码的形式输入单个主机的 IP 地址或是一个网段，也可以直接以 193.168.20.226-193.168.20.229 的网段输入形式输入。还可以单击地址/地址组后面的下拉框选择主机组。如果用户选择的是主机组，例如：测试部，则设置的流量控制策略对属于测试部的所有主机均有效。

4. 填写控制流量
5. 选择统计周期
6. 单击【增加】保存设置，单击【关闭】取消操作。

> **提示：关于流量控制**
>
> 1. 对主机组进行流量控制之后，还可以对主机组内单个主机设置流量控策略，先定义的策略具有较高的优先级。对单个主机设置了控制策略后，也可以对主机所在的主机组添加控制策略，先添加的策略具有较高的优先级。
> 2. 流量值应该为 1-1000000 之间的整数。

- **修改流量控制**

1. 单击【内网管理】➔【主机信息】➔【流量控制】，进入流量控制信息查看界面如图 6.21 所示。

图 6.21 流量控制查看界面

2. 单击操作一列的修改图标，进入修改界面如图 6.22 所示。

图 6.22 修改流量控制界面

3. 重新写入要修改的流量信息，单击【修改】完成修改操作，单击【关闭】取消操作。

- **删除流量控制**

1. 单击【内网管理】➔【主机信息】➔【流量控制】，进入流量控制查看界面如图 6.23 所示。

图 6.23 流量控制查看界面

2. 单击操作一列的删除图标，系统弹出提示框如图 6.24 所示。

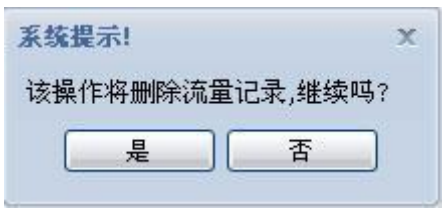


图 6.24 系统提示是否要删除流量控制记录

3. 单击【是】按钮删除记录，单击【否】按钮取消操作。

6.1.4 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主机或是网段上设置不同的带宽策略控制分配网络流量。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，管理员可以给各部门分配不同的网段，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。

单击【内网管理】➔【主机信息】➔【带宽管理】进入带宽管理界面，如图 6.25 所示

图 6.25 带宽管理界面

对于带宽管理界面各字段我们做以下说明：

字段	说明
【增加带宽管理 】	单击进入增加带宽管理设置界面
序号	按照阿拉伯数字排序
地址/主机组	设置带带宽控制的网络范围
服务	可以选择对不同的服务设置带宽
下载带宽	设置最大下载带宽
上传带宽	设置最大上传带宽
控制	控制类型为整个网段或每个 IP
操作	有修改和删除两种操作，单击 图标进行带宽管理规则的修改操作，单击 图标可以删除设置的带宽管理规则

表 6.5 带宽管理界面字段说明

- **增加带宽管理**

1. 在带宽管理界面单击【增加带宽】，进入如图 6.26 所示界面

图 6.26 增加带宽管理

2. 填写带宽管理适用的地址或是主机组
3. 选择服务类型，服务类型界面如图 6.27 所示

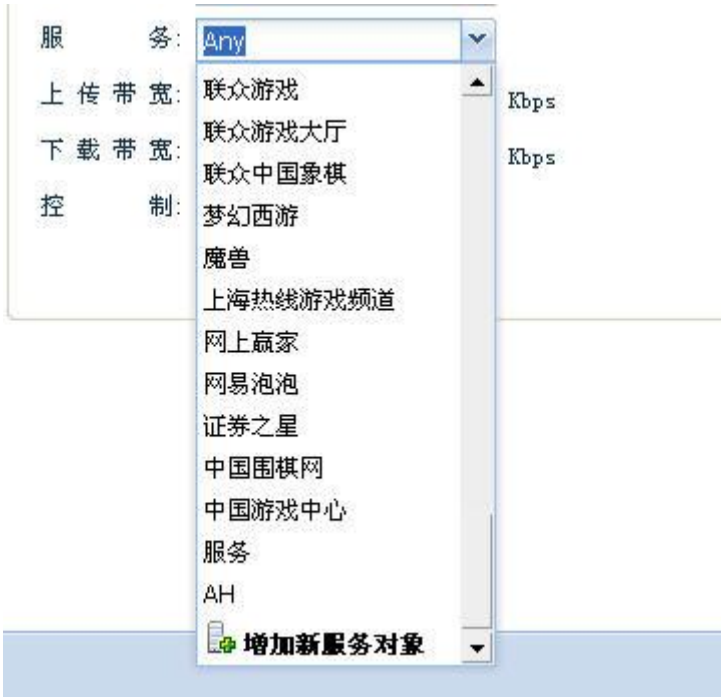


图 6.27 服务类型

关于服务类型的选择，可以参看服务对象的设置部分。

4. 输入下载带宽和上传带宽
5. 设置控制类型：整个网段或是每个 IP

提示：关于控制类型的选择

带宽管理设置中的控制类型有整个网段和每个 IP 两种。整个网段是指设置的上传带宽和下载带宽是对于整个网段内所有主机的上传带宽之和及下载带宽之和而言的；每个 IP 是指上传带宽和下载带宽的限制是针对网段内的每台主机而言。

6. 单击【增加】，增加带宽管理策略。单击【关闭】取消操作。

- **服务对象的设置**

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。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。

✓ **增加新的服务对象**

1. 在增加带宽管理界面服务选项下展开下拉菜单，如图 6.28 所示：

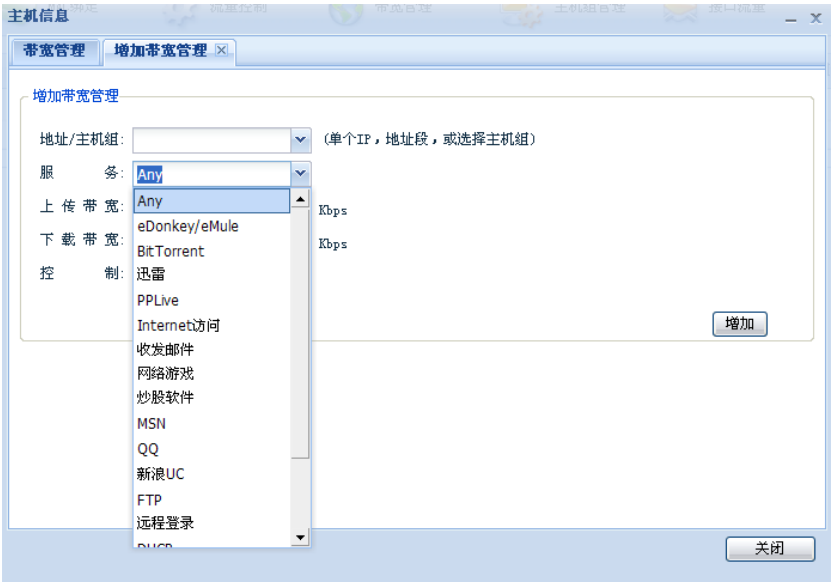


图 6.28 选择增加新服务对象界面

对各服务作以下说明：

协议	说明
Edonkey/ Emule	Edonkey/ Emule 使用的协议
BtTorrent	BT 使用的协议
迅雷	迅雷使用的协议
PPLive	用于互联网上大规模视频直播的免费软件
Internet 访问	客户端进行 internet 访问必须的几个标准 tcp 端口组合服务
收发邮件	客户端进行收发邮件必须的几个标准 tcp 端口组合服务

网络游戏	常见网络游戏网络通讯传输端口的组合服务
炒股软件	常见炒股软件网络通讯传输端口的组合服务
MSN	MSN 的标准网络通信传输端口的组合服务
QQ	QQ 的标准网络通信传输端口的组合服务
新浪 UC	新浪 UC 的标准网络通信传输端口的组合服务
FTP	FTP 协议标准网络通信传输端口的组合服务
远程登录	常用远程登录通信传输端口组合服务
DHCP	DHCP 标准通讯协议
VPN	VPN 传输使用的标准通讯协议
SNMP	简单网络管理协议

表 6.6 服务说明

2. 单击【增加新的服务对象】，进入如图 6.29 所示增加新服务对象设置界面

图 6.29 增加新服务对象界面

3. 填写服务名称（为便于设置最好填写便于识别意义的协议名称）

4. 选择协议

关于协议我们做以下详细说明，防毒墙提供了 4 种定义协议的方式

- TCP/UDP 对于这两种常用的三层协议，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 6.30 所示

图 6.30 TCP/UDP 的设置

- ICMP 用户可以指定 ICMP 协议的类型域，如图 6.31 所示

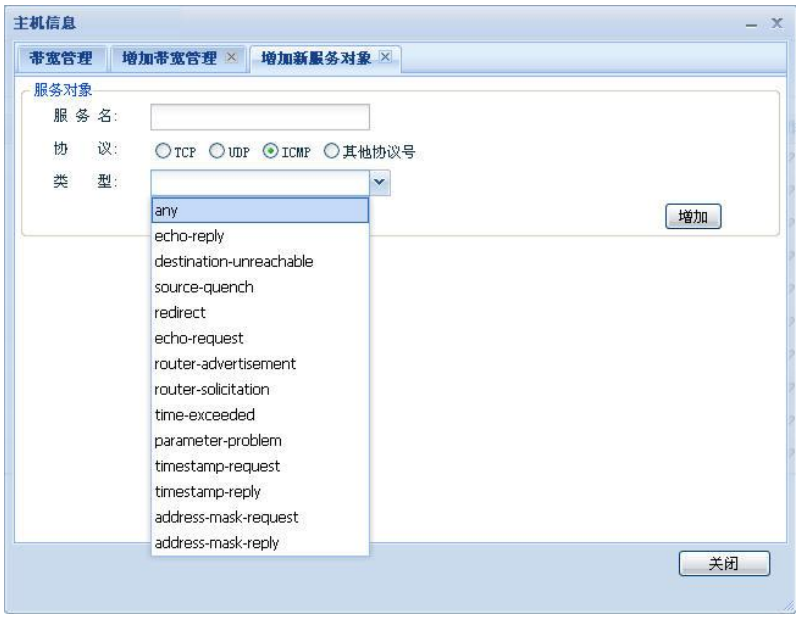


图 6.31 ICMP 的配置

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 6.7 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定义未在防毒墙上列出的协议，如图 6.32 所示

图 6.32 自定义协议号

5. 设置完成后，单击【增加】按钮保存设置，结果如图 6.33 所示；单击【关闭】取消操作。

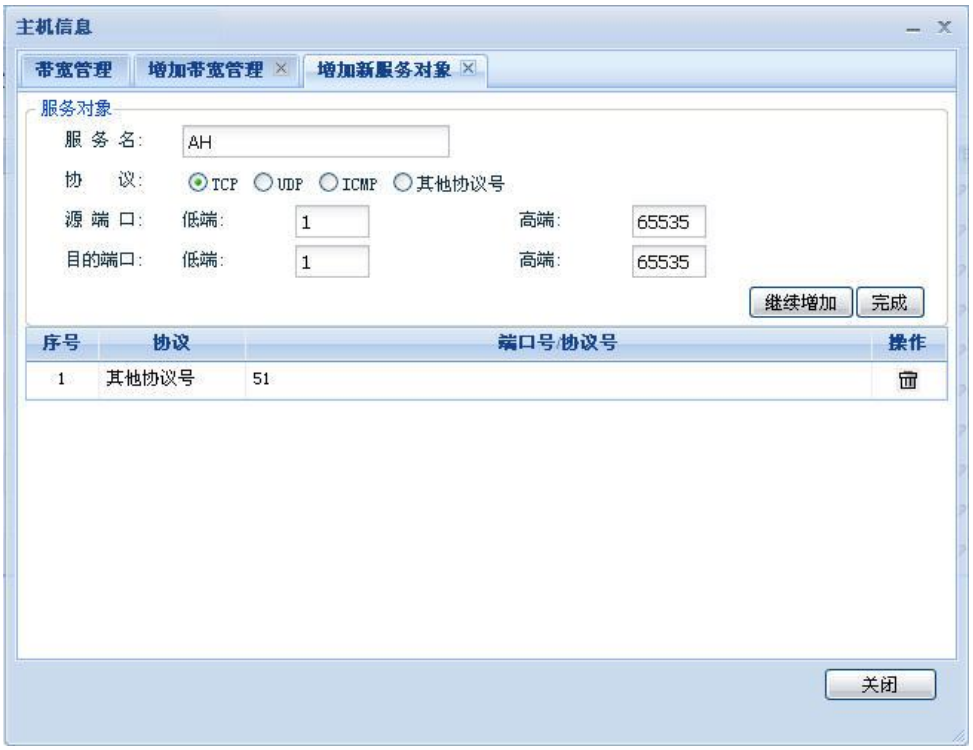


图 6.33 增加一个新服务对象后增加服务对象界面

图 6.33 界面下方显示了服务配置的详细信息，即服务使用的协议、端口号等。单击【继续增加】可以为一个服务对象设置多组协议组合。单击【完成】返回上个界面（在不同的模块中上个界面不同）。

✓ **修改服务设置**

如果需要修改某个服务对象，在增加带宽控制界面服务选项中选中该服务对象，单击其右侧的修改图标进入修改服务对象页面进行修改。如图 6.34 所示。

图 6.34 修改服务对象

修改方式见增加服务对象中的说明。

✓ **删除服务对象设置**

如果需要删除某个服务对象，在增加带宽控制界面服务选项中选中该服务对象，单击其右侧的删除图标进行删除操作。

- **修改带宽管理**

如果随着企业业务的拓展或是员工工作的调整，已经设置的带宽管理策略不能适应企业的需求，管理员可以修改带宽管理策略以更好的控制分配网络流量。单击【内网管理】➔【主机信息】➔【带宽管理】进入带宽管理界面，如图 6.35 所示。

图 6.35 带宽控制查看界面

1. 单击要修改网段的操作一列的修改图标，进入修改界面，如图 6.36 所示。

图 6.36 修改带宽控制界面

2. 重新填入带宽管理设置信息，单击【修改】系统弹出修改成功提示对话框，修改带宽控制完成。也可单击服务一行的修改操作进入具体服务的修改，如图 6.37 所示

图 6.37 修改服务对象界面

提示： 对于具体服务对象的修改，参见本节服务对象的设置部分

- **删除带宽管理**

如果用户要删除设置的带宽控制策略，可以按照以下步骤进行：

1. 单击【内网管理】➔【主机信息】➔【带宽管理】进入带宽管理界面，如图 6.38 所示：

图 6.38 带宽控制查看界面

2. 单击所要删除网段操作一列的删除图标，系统弹出提示框如图 6.39 所示。

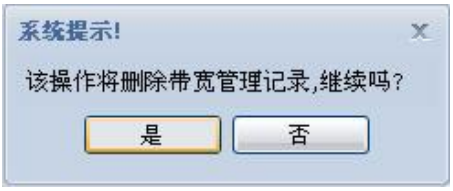


图 6.39 删除带宽控制成功界面

3. 单击【是】按钮删除带宽管理记录，单击【否】按钮取消操作。

6.1.5 主机组管理

主机组管理是为了便于企业的管理而设计的，对于企业而言，可能有多个部门，利用防毒墙主机组管理功能将企业各个部门分类，便于管理员的统一管理。单击【内网管理】➔【主机信息】➔【主机组管理】进入如图 6.40 所示界面。

图 6.40 主机组管理界面

对主机组管理各字段说明如下：

字段	说明
增加主机组	单击进入增加主机组操作界面
序号	按照阿拉伯数字排序

组名称	设置的主机组名称
操作	有修改和删除两种操作，单击 图标进行主机组设置的修改操作，单击 图标可以删除主机组

表 6.8 主机组管理界面字段说明

- **增加主机组**

1. 单击主机组管理界面中的【增加主机组】，进入如图 6.41 所示界面。

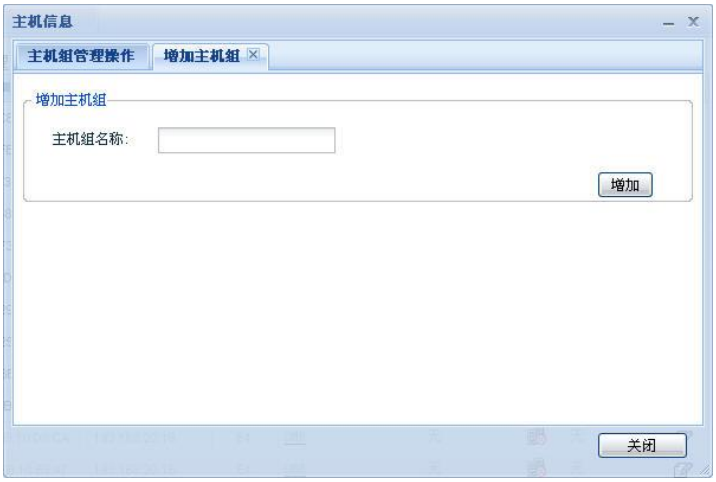


图 6.41 增加主机组界面

2. 填写主机组名称

3. 单击【增加】保存设置，完成主机组的添加操作；单击【关闭】取消操作。

- **修改主机组**

1. 单击【内网管理】➔【主机信息】➔【主机组管理】进入如图 6.42 所示界面

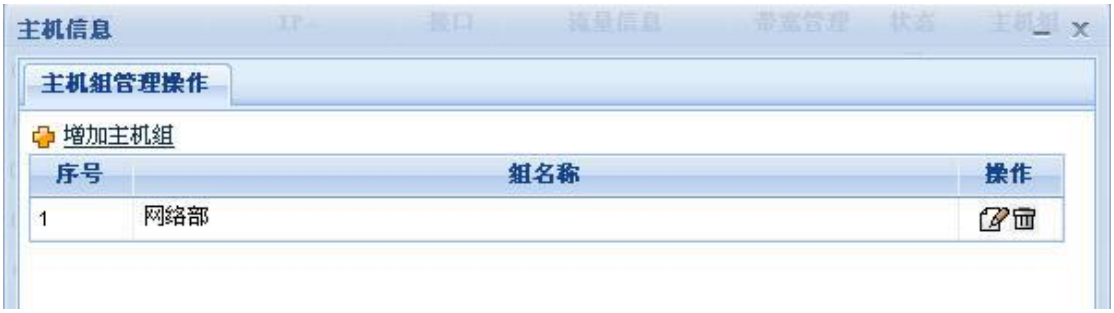


图 6.42 主机组设置查看界面

2. 单击所要修改主机组一行的修改图标，进入修改界面如图 6.43 所示。

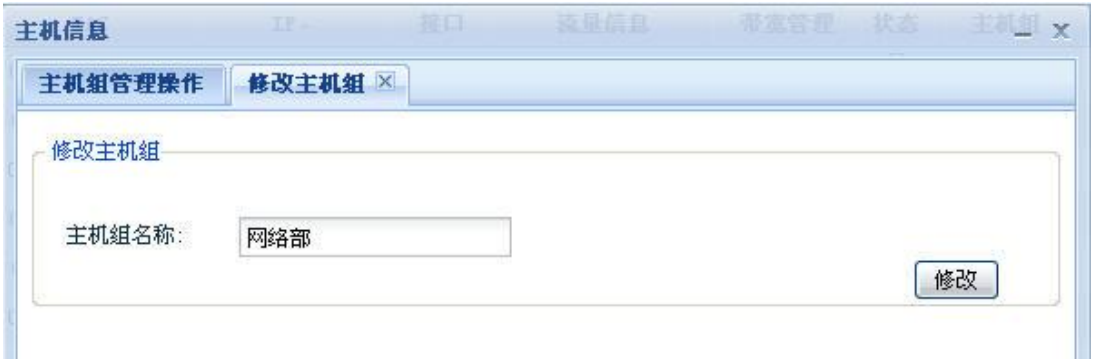


图 6.43 主机组修改界面

3. 单击【修改】保存设置，单击【关闭】取消操作。

- **删除主机组**

1. 单击【内网管理】➔【主机信息】➔【主机组管理】进入删除界面如图 6.44 所示。

图 6.44 主机组设置查看界面

2. 单击操作一列中删除图标，系统弹出如图 6.45 所示提示框。

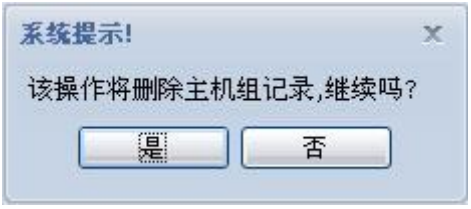


图 6.45 系统提示是否删除主机组界面

3. 单击【是】按钮，完成主机组的删除操作；单击【否】按钮取消操作。

6.1.6 接口流量

瑞星防毒墙有 E0、E1、E2、E3、E4 五个接口，接口流量功能模块的设置是为了便于管理员查看已连通的各接口的近一小时的流量信息，单击【内网管理】➔【主机信息】➔【接口流量】进入接口流量查看界面，如图 6.46 所示。

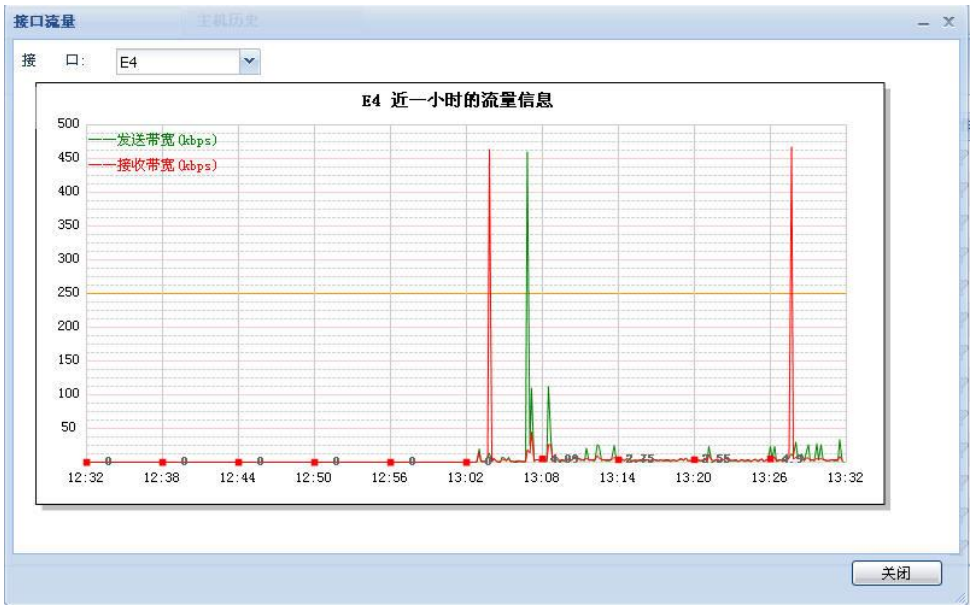


图 6.46 接口流量查看界面

接口流量信息显示当前连通的接口近一小时的流量信息，要查看其它接口时，只需单击界面上端接口下拉框选择接口即可，如图 6.47 所示。

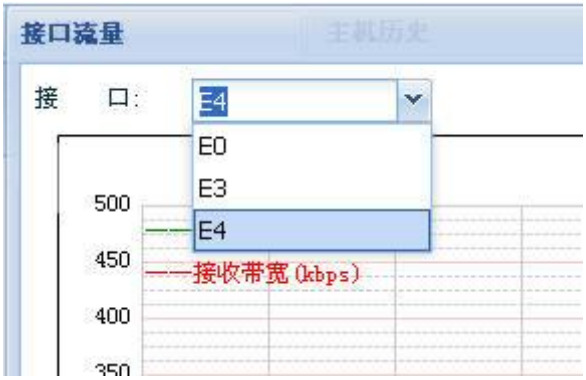


图 6.47 接口选择界面

6.2 主机历史

为了便于管理员更好的管理企业内部网络，瑞星防毒墙提供主机历史查询的功能，管理员可设置适当的查询条件查询内网主机在一个时间段内的上线信息。还会对内网 IP 地址或是 MAC 地址的冲突发出告警。单击【内网管理】➔【主机历史】进入主机历史界面，如图 6.48 所示。

图 6.48 主机历史界面

主机历史界面各个字段说明：

字段	说明
警告	如果一个主机用多个 IP 接入网络或者多台主机用一个 IP 接入网络，防毒墙会发出警告信息，管理员可根据警告信息查看具体情况，核实 IP 与主机的对应情况，将 IP 与 MAC 绑定，避免合法用户的 IP 被别人抢用，确保内网安全有序。
	单击可以隐藏警告信息
当前查询条件	显示当前查询主机信息的条件，刚开始进入界面为防毒墙的默认条件：查询当天局域网内所有主机的状态
更改查询条件	单击此按钮可以进入更改查询条件界面
序号	主机信息按照阿拉伯数字排序
时间	主机发生动作（上线或者离线）的时间
MAC	主机网卡的 MAC 地址
IP	主机的 IP 地址
接口	通过防毒墙的哪个接口获取的主机信息
状态	主机的状态，有上线和离线

表 6.9 主机历史界面字段说明

6.2.1 更改查询条件

瑞星防毒墙为用户提供了按条件查询主机历史的功能，管理员可以根据不同的查询需要选择不同的查询条件。单击【更改查询条件】进入查询条件界面，填写信息如图 6.49 所示。

图 6.49 主机历史查询条件界面

主机历史查询条件界面各个字段说明：

字段	说明
IP 地址	填入要查询的主机的 IP 地址
MAC 地址	填入要查询的主机的 MAC 地址，IP 和 MAC 只需填一个即可
时间	查询主机信息在一定时间的动作信息
接口	主机动作通过的防毒墙的接口，选择全部代表查询全部的接口
状态	有上线、离线和全部

表 6.10 主机历史查询条件界面说明

主机历史查询条件的填写可以按照以下操作进行：

1. IP 地址，填写要查询的主机的 IP 地址
2. MAC 地址，填写要查询的主机的 MAC 地址
3. 时间，选择要查询的主机在某段时间的状态集合，单击日历图标可设置起始时间和结束时间，结束时间不可早于起始时间
4. 接口，选择主机使用的接口，全部代表所有的接口
5. 状态，可以根据需要选择上线、离线或者全部

提示：也可输入上述条件的某一条或几条进行模糊查询。

填写完内容后，单击【确定】进行查询，查询结果将在主机历史界面上显示出来，如图 6.50 所示。单击【关闭】按钮取消操作。

图 6.50 主机历史查询结果

6.3 端口映射

端口映射的作用是使互联网的用户能访问到局域网的服务器，具体实现技术是在瑞星防毒墙上做一个转发装置，当互联网用户要访问本局域网内服务器的时候将公网 IP 映射为要访问的服务器的内网 IP，此时服务器为其提供服务，该功能可保护对外提供服务的计算机安全运行。如图 6.51 所示，当一个响应数据包从公网送进防毒墙时，NAT 服务（Network Address Translation 可译为网络地址转换）会把目的地址由公网 IP 地址转换为内网服务器的私有 IP 地址后，再传送给局域网内服务器主机。例如用户想访问瑞星公司（www.rising.com.cn）的网站服务器，首先经过瑞星公司的防毒墙，防毒墙将其外网接口的 IP 地址转换为瑞星公司内的网站服务器的地址，用户的请求就可以到达网站服务器，然后用户就可以进行下载新的病毒库等操作。

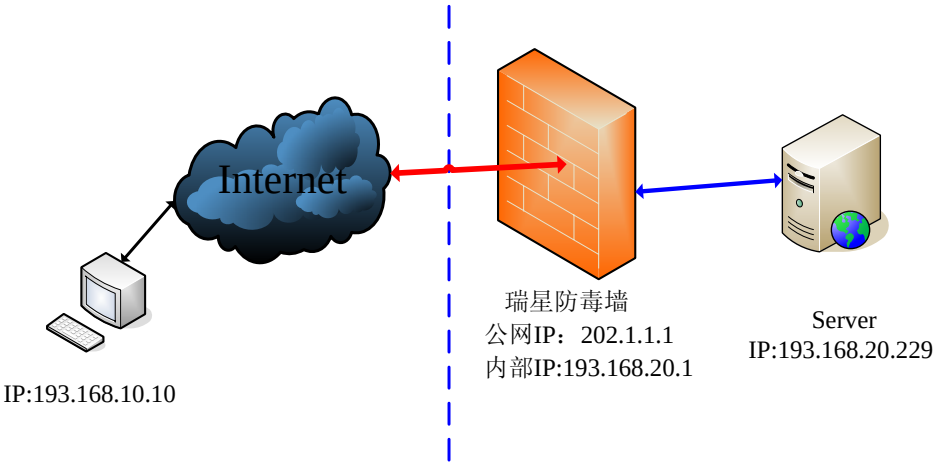


图 6.51 端口映射转换示意图

提示：防毒墙在透明模式下没有此功能

在透明模式下没有端口映射菜单项，所以用户只有在选择防毒墙工作模式为宽带模式时才需配置。若是用户配置防毒墙工作在透明模式下，则可跳过端口映射的配置。

单击【内网管理】➔【端口映射】进入端口映射主界面，如图 6.52 所示

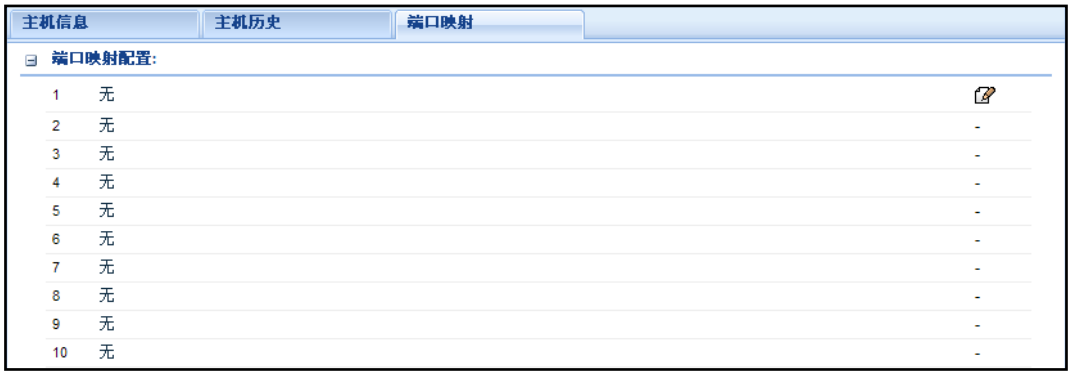


图 6.52 端口映射主界面

6.3.1 增加端口映射

防毒墙默认最多可以配置十组端口映射。单击端口映射界面的修改图标进入增加端口映射界面，如图 6.53 填写端口映射信息。

图 6.53 增加端口映射

增加端口映射界面各字段说明如下：

字段	说明
外部	外网用户访问内部服务器时使用防毒墙接口的IP地址和端口,若是防毒墙外网接口设置为静态IP接入方式或是其他ISP接入方式但是已经分配IP地址，则可以在下拉框中直接选择IP地址
内部	内部服务器的IP地址和提供服务所用的端口
协议	服务使用的协议，有TCP和UDP两种
上传带宽	内部服务器允许外网用户上传文件的最大速率
下载带宽	内部服务器允许外网用户下载文件的最大速率

表 6.11 端口映射名词解释

提示：如果界面上外部后下拉框没有 IP 可以选择

需要按如下操作进行：进入【网络配置】➔【接口配置】，把外网接口（E0、E1 或 E2）配置为静态 IP 接入方式并添加 IP 地址或者将外网口配置为动态 IP 方式或 PPPoE 方式。具体配置操作参见外网口接口设置部分。

防毒墙增加端口映射的配置操作可以按照以下步骤进行：

1. 选择外部，从下拉框中选择一个 IP 地址，冒号(:)后面的框中填入服务使用的端口
2. 选择内部，填入转换成内部的 IP 地址，即外网要访问的内部服务器地址，冒号(:)后面的框中填入服务使用的端口
3. 选择协议，默认服务使用 TCP 协议，可以从下拉框中选择 UDP 协议
4. 选择上传带宽，填写上传带宽速率（1-1000000）
5. 选择下载带宽，填写下载带宽速率（1-1000000）

填写好相关内容后，单击【修改】按钮保存修改内容，单击【关闭】按钮取消操作。当向防毒墙增加一条端口映射记录后，端口映射配置的记录会在端口映射主界面上显示出来，如图 6.54 所示。

图 6.54 端口映射配置

6.3.2 修改端口映射

若用户需要对存在的端口映射进行修改，可以单击该条记录后面的修改图标进行修改，如图 6.55 所示。

图 6.55 修改端口映射

修改防毒墙端口映射的操作可以按照以下步骤进行：

1. 选择外部，从下拉框中选择一个 IP 地址进行修改，如图 6.55 有两个 IP 地址可供选择，端口也可以进行修改
2. 选择内部，修改成要转换的内部服务器的 IP 地址，端口也可以进行修改
3. 选择协议，可以更改协议类型，有 TCP 和 UDP 可以选择
4. 选择上传带宽，填入一个数字（1-1000000），修改最大上传速率
5. 选择下载带宽，填入一个数字（1-1000000），修改最大下载速率

填写好相关内容后，单击【修改】按钮保存修改，单击【关闭】按钮取消修改操作。

6.3.3 删除端口映射

若要删除一个端口映射，直接单击该条端口映射后面的删除图标，弹出系统提示如图 6.56 所示。

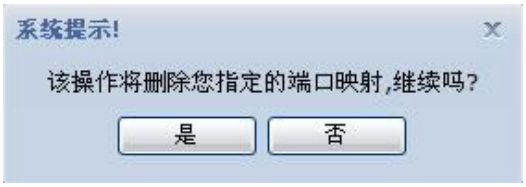


图 6.56 系统提示是否删除端口映射

单击【是】按钮确认删除，单击【否】按钮取消删除操作。单击【是】按钮后系统弹出删除成功提示框如图 6.57 所示。

图 6.57 删除端口映射成功

第七章 上网控制

瑞星防毒墙提供了上网控制功能，用户可以通过配置防毒墙的上网控制策略对局域网内的主机进行管理，本章将从以下四个方面介绍防毒墙的上网控制功能：

- 安全策略：通过设置防毒墙安全策略保证企业内部与外部网络的通讯安全
- 连接管理：查看通过防毒墙建立的连接信息
- URL 过滤：进行防毒墙 URL 过滤设置
- IP 黑名单：对一些经常制造网络威胁的地址进行过滤

7.1 安全策略

本小节将介绍以下两个方面的内容：特权 IP 和安全策略。

单击防毒墙功能菜单的【上网控制】进入安全策略页面，如图 7.1 所示。

图 7.1 安全策略页面

7.1.1 特权 IP

特权 IP 可以不受上网控制条件（例如流量限制）的约束，管理员可以根据需要设置内网某些主机的 IP 为特权 IP。

- **增加特权 IP**

单击安全策略页面的【单击此处增加特权 IP】按钮，进入增加特权 IP 界面，如图 7.2 所示。

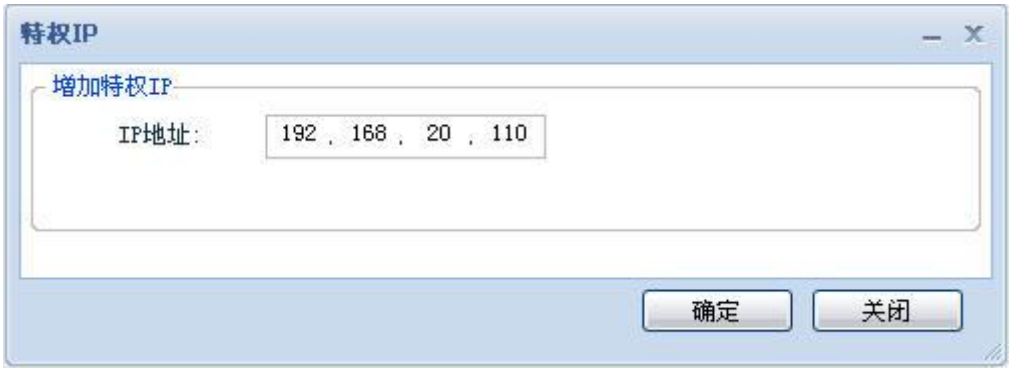


图 7.2 增加特权 IP

填写完 IP 地址后，单击【确定】按钮添加一个特权 IP，单击【关闭】按钮取消操作。单击【确定】按

钮后，系统弹出增加特权 IP 成功的提示框如图 7.3 所示。

图 7.3 特权 IP 增加成功提示框

单击中的【确定】按钮，完成特权 IP 的增加操作。

提示：添加特权 IP 的注意事项

1. 不允许添加已经存在的特权 IP（即不允许重复添加）；
2. 不允许添加存在于 IP 黑名单中的 IP 地址为特权 IP，如果管理员确实要添加这个 IP 为特权 IP，可先进入【IP 黑名单】删除黑名单 IP，然后再添加特权 IP，删除黑名单 IP 的操作可以参看 7.4.3 节的删除黑名单 IP 部分。

添加一个特权 IP 后，该条记录会在安全策略页面上显示出来，如图 7.4 所示。

图 7.4 特权 IP 记录

特权 IP 记录各字段说明：

字段	说明
【单击此处增加特权 IP】	单击此按钮进入增加特权 IP 页面添加特权 IP
（当前已设置）1 个特权 IP	显示特权 IP 记录条数，单击此处可以隐藏显示的特权 IP 记录
	隐藏信息图标，单击可以隐藏特权 IP 记录
	修改图标，单击可以进入修改特权 IP 界面，进行特权 IP 的修改操作
	删除图标，单击可以删除特权 IP 记录

表 7.1 特权 IP 记录界面说明

- **修改特权 IP**

若要修改特权 IP，单击该条特权 IP 记录后面的修改图标，弹出修改界面如图 7.5 所示。

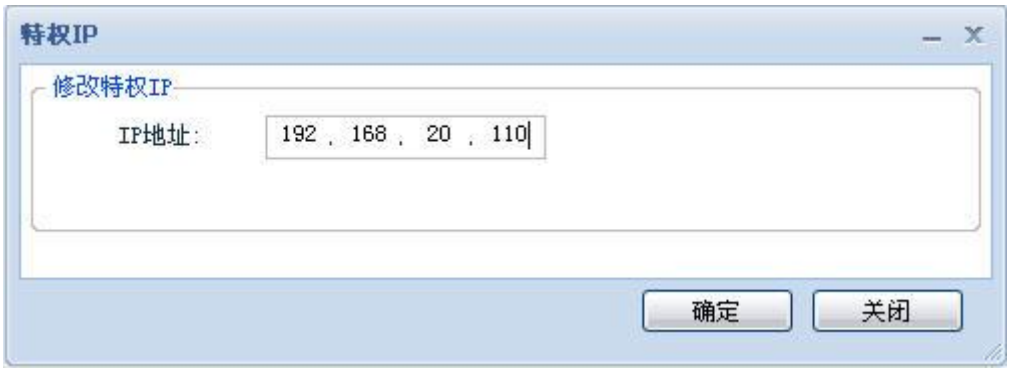


图 7.5 修改特权 IP

在 IP 地址后输入要修改的特权 IP 地址，单击【确定】按钮完成修改操作，单击【关闭】按钮取消修改操作。单击【确定】按钮后，系统弹出修改成功的提示框，如图 7.6 所示。

图 7.6 特权 IP 修改成功

单击【确定】按钮，完成特权 IP 的修改操作。

- **删除特权 IP**

若要删除某个特权 IP，单击该条记录后面的删除图标，弹出系统提示如图 7.7 所示

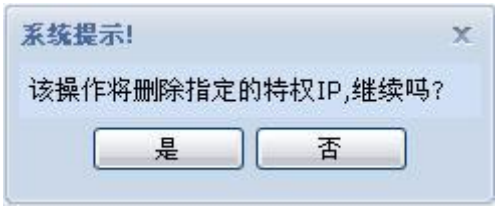


图 7.7 特权 IP 的提示对话框

单击【是】按钮删除特权 IP，单击【否】按钮取消操作。

7.1.2 安全策略

瑞星防毒墙集成了防火墙功能，对请求与防毒墙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。安全策略界面如图 7.8 所示。

图 7.8 策略界面

提示：防火墙默认情况下网络全通，保证在接入防毒墙后就能为用户提供防护。

安全策略界面各个字段说明：

字段	说明
【增加安全策略】	单击此按钮可以进入安全策略管理界面，添加安全策略
序号	策略按照阿拉伯数字排序
	表示当有数据包命中该安全策略时动作为允许即允许数据包通过
	表示当有数据包命中该安全策略时动作为拒绝即拒绝数据包通过
策略名称	策略的名称
时间	策略的适用时间
【设为拒绝】	表示当数据包命中策略时防毒墙允许数据包通过，单击该按钮后防毒墙将拒绝命中策略的数据包，同时该按钮变为【设为允许】
	修改图标，单击可以进入修改策略界面，进行修改操作
	删除图标，单击可以删除此策略

表 7.2 安全策略界面说明

- **增加安全策略**

单击安全策略界面的【增加安全策略】，进入安全策略管理界面，填写信息如图 7.9 所示。

图 7.9 安全策略管理

安全策略管理各个字段说明：

字段	说明
策略名	填写要增加的策略的名称
入口	通过防毒墙的数据流的入口，有防毒墙启用的接口和 PPTP 可以选择， PPTP 代表 VPN 通道

	接口
出口	通过防毒墙的数据流的出口
源地址	通过防毒墙数据流的源地址
目的地址	通过防毒墙数据流的目的地址
服务	该策略要检查何种服务内容
时间	该策略的适用时间
动作	表示当数据包命中该安全策略时防毒墙执行的策略。有允许和拒绝两种动作：允许表示允许数据包通过；拒绝表示拒绝数据包通过
日志记录	当数据包命中该安全策略时是否需要进行相应的网络日志的记录。关于网络日志的相关信息用户可参看 11.1.5 网络日志
	修改图标，单击可以进入修改界面对服务或时间对象进行修改操作
	删除图标，单击可以删除策略使用的对象
	警告信息，当选择地址为主机组地址时，不可对该地址进行操作，请到内网管理的主机组管理里进行操作。

表 7.3 安全策略管理界面说明

增加安全策略的操作可以按照以下步骤进行：

1. 策略名处输入唯一的策略名称，方便管理员进行识别
2. 选择数据流的入口
3. 选择数据流的出口
4. 在源地址处选择地址对象或在下拉框中单击【增加新地址对象】，进入增加新地址对象界面，如图 7.10 所示。

提示：主机组对象的修改和删除操作

如果在【内网管理】➔【主机信息】➔【主机组管理】中添加了主机组，这里可以选择使用，但是无法对该地址对象进行修改和删除操作，如果要修改和删除，请参见 6.1.5 节主机组管理。

图 7.10 增加新地址对象

1) 地址名称：用来表示该地址对象的友好名称

2) 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：192.168.0.1
- ✓ 增加一个网段，例如：192.168.0.1/24
- ✓ 增加一段地址，例如：192.168.0.1-192.168.0.10

设置完成后，单击【增加】按钮保存设置，单击【关闭】取消操作。

如果建立的策略要控制不连续的地址，可以单击【继续增加】按钮继续添加地址 IP，例如再添加一个网段，界面如图 7.11 所示。

图 7.11 继续增加地址对象

3) 添加地址对象完成后，单击【完成】按钮返回增加安全策略界面继续添加安全策略。

提示：关于单击【关闭】按钮的说明

现在只完成了策略中地址对象的配置，如果单击【关闭】按钮则返回了安全策略界面，中止了安全策略的增加操作，用户还得重新进行前面增加安全策略操作的步骤，所以这里不要单击【关闭】按钮。

5. 在目的地址处选择地址对象或在下拉框中单击【增加新地址对象】，进入增加新地址对象界面添加地址对象。关于增加新地址对象的详细操作，可参见增加新地址对象部分。

6. 在服务处选择服务对象或在下拉框中单击【增加新服务对象】，进入增加服务对象界面添加新服务对象。关于增加新服务对象详细操作，可参见服务对象的设置部分。

7. 在时间处选择时间对象或在下拉框中单击【增加新时间对象】，进入增加新时间对象界面添加新时间对象。关于增加新时间对象的详细操作，可参见时间对象的设置部分。

8. 在策略处选择允许或拒绝，表示当数据包命中安全策略时允许数据包通过还是拒绝数据包通过。

9. 在日志记录一栏单击记录或是不记录前的单选框，表示当数据包命中该安全策略时是否记录网络日志。

填写完内容后，单击【确定】按钮增加安全策略，单击【关闭】按钮取消操作。添加了一条策略后，该策略会在安全策略界面上显示出来，如图 7.12 所示。

图 7.12 安全策略记录

- **移动安全策略顺序**

瑞星防毒墙安全策略是有顺序性的，当有数据包通过防毒墙时按照策略顺序处理数据包。为了达到良好的效能，适时的调整策略的次序是必要的。应该把限制条件多的策略移动到前面。如果要调整某条安全策略的顺序，可以用鼠标单击该策略不放，将其拖到某条策略之前或者之后，系统会提示确认移动操作，单击【是】按钮完成移动，单击【否】取消移动。移动安全策略的顺序后，如图 7.13 所示。

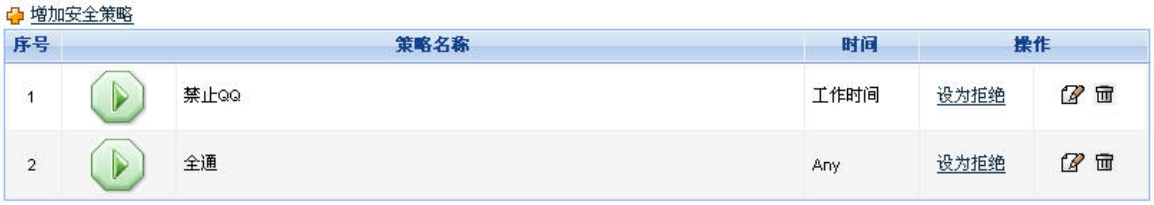
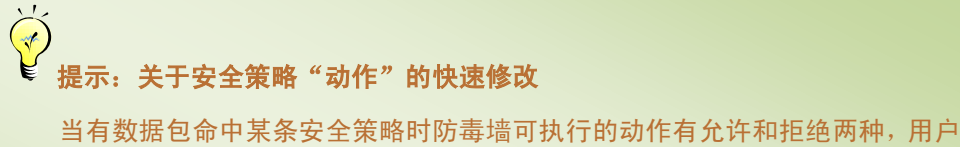


图 7.13 交换安全策略的顺序

- **修改安全策略**

当用户想修改某一安全策略时，单击该条策略一行的修改图标，修改操作与增加安全策略步骤类似，具体操作可参看增加安全策略。



提示：关于安全策略“动作”的快速修改

当有数据包命中某条安全策略时防毒墙可执行的动作有允许和拒绝两种，用户可以对该动作进行快速修改。在安全策略界面单击要修改的策略条目一行操作栏【设为允许】或【设为拒绝】文字，如图 7.14 所示。

图 7.14 修改安全策略

- **删除安全策略**

当用户想删除某条安全策略时，单击该策略一行的删除图标，弹出如图 7.15 所示的系统提示对话框。

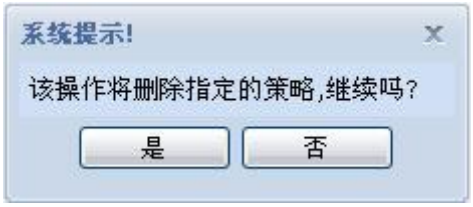


图 7.15 删除策略提示框

单击【是】按钮删除策略，单击【否】取消操作。

7.2 连接管理

防毒墙连接管理显示了当前系统连接的状态信息，管理员可据此查询局域网内主机的连接信息。单击安全策略界面的【连接管理】进入连接管理界面，如图 7.16 所示。

图 7.16 连接管理界面

连接管理界面各字段说明：

字段	说明
【开始统计】	单击该按钮统计连接信息
【更改查询条件】	单击该按钮进入更改查询条件的界面
序号	连接信息按照阿拉伯数字排序
协议	采用何种协议进行通信，包括TCP、UDP和ICMP三种协议，单击可以切换显示顺序（按协议分组显示）
源地址	连接的来源IP地址，单击可以切换显示顺序按源地址升序或是降序显示
目的地址	连接的目的IP地址，单击可以切换显示顺序按目的地址升序或是降序显示
端口对	源地址通过防毒墙连接目的地址所使用的端口，*代表任意端口，单击可以切换显示顺序按端口对升序或是降序显示
上传字节数/包	从源地址流向目的地址的字节数，单击可以切换显示顺序按上传字节数升序或是降序显示
下载字节数/包	从目的地址流向源地址的字节数，单击可以切换显示顺序按下载字节数升序或是降序显示
在线秒数	从建立连接后一共运行了多长时间，单击可以切换显示顺序按在线时间升序或是降序显示
空闲秒数	建立连接后该连接的空闲时间，单击可以切换显示顺序按空闲时间升序或是降序显示
连接数	当前建立的连接的数量，单击可以切换显示顺序按连接数升序或是降序显示

表 7.4 连接管理界面说明

7.2.1 开始统计

连接管理界面显示了防毒墙统计信息的总体情况及其统计时间等信息。如图 7.17 所示。

图 7.17 开始统计

单击【开始统计】按钮，按照防毒墙默认的查询条件或管理员最近一次设置的查询条件查询当前主机的连接信息并将统计结果显示在界面上。

7.2.2 更改查询条件

连接管理界面上显示了当前的查询条件，如图 7.18 所示。

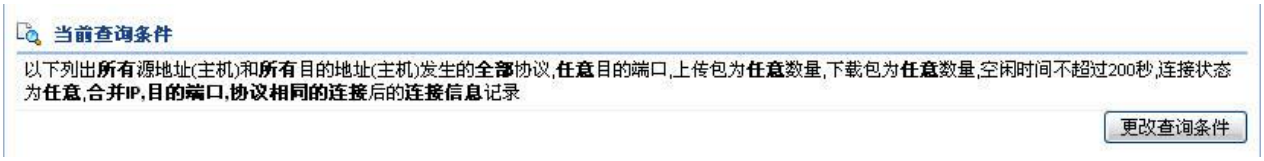


图 7.18 当前查询条件

默认查询所有的信息，如果管理员想查询更加详细的信息，单击【更改查询条件】按钮进入更改查询条件界面，如图 7.19 所示。

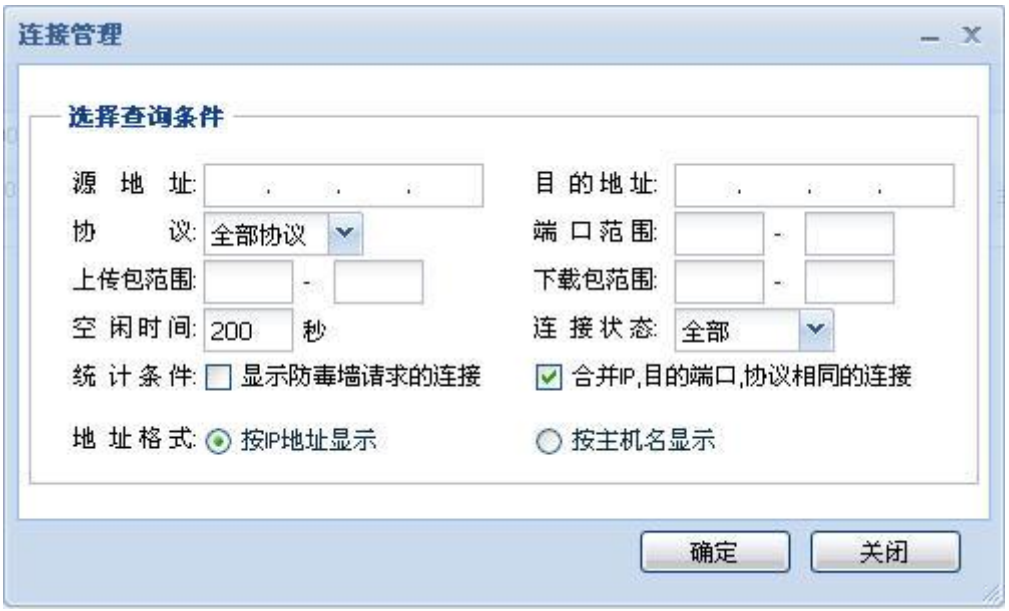


图 7.19 更改查询条件

更改查询条件各个字段说明：

字段	说明
源地址	经过防毒墙的数据包的来源地址
目的地址	经过防毒墙的数据包的目的地址
协议	使用的协议类型，有 TCP、UDP 和 ICMP，全部协议则代表以上三种全部协议
端口范围	主机连接进行通信使用的端口范围
上传包范围	上传的数据包的大小范围，为空时忽略此条件
下载包范围	下载的数据包的大小范围，为空时忽略此条件
空闲时间	建立连接后该连接的空闲时间，为空时忽略此条件
连接状态	正常表示正常的数据通信，不正常表示数据为单方向传输，全部包括正常和不正常
统计条件	单击显示防毒墙请求连接前的复选框表示显示防毒墙内部满足条件的连接。单击合并 IP，目的端口，协议相同的连接前的复选框表示查询结果上将 IP、目的端口和协议相同的连接合并为一行显示
地址格式	查询结果的显示方式，有按 IP 地址显示和按主机名显示

表 7.5 更改查询条件界面说明

更改查询条件的操作可以按照以下步骤进行：

1. 源地址，填写经过防毒墙的数据包的源地址

2. 目的地址，填写经过防毒墙的数据包的目的地址
3. 协议，选择连接使用的协议，TCP、UDP、ICMP 或者默认的全部
4. 端口范围，填写主机连接进行通信时使用的端口的范围，默认为全部
5. 上传包范围，填写主机进行连接时上传的数据包的范围大小，起始值不能大于结束值
6. 下载包范围，填写主机进行连接时下载的数据包的范围大小，起始值不能大于结束值
7. 空闲时间，填写空闲时间，即主机连接后未进行任何操作的时间
8. 统计条件，单击统计条目前的复选框，方便显示统计信息
9. 地址格式，选择查询结果的显示方式

填写完以上内容后，单击【确定】按钮保存查询条件并查询，单击【取消】按钮取消操作。

提示：也可输入上述条件的某一条或几条进行模糊查询。

保存查询条件后，防毒墙按照设置的查询条件查询并将结果显示在连接管理界面上，如图 7.20 所示。

当前查询条件

以下列出**所有**源地址(主机)和**所有**目的地址(主机)发生的**全部**协议,**任意**目的端口,上传包为**任意**数量,下载包为**任意**数量,空闲时间不超过200秒,连接状态为**任意**,**显示防毒墙请求的连接、合并IP,目的端口,协议相同的连接**后的**连接信息**记录

更改查询条件

序号	协议	源主机	目的主机	端口对	连接数	上传字节/包	下载字节/包	在线秒数	空闲秒数
1	tcp	127.0.0.1	127.0.0.1	* - 8888	13	4197/84	3830/84	4	0
2	tcp	127.0.0.1	127.0.0.1	* - 3306	1	3077/37	1890/21	2950	187
3	tcp	net	193.168.20.105	* - 443	1	1009/7	849/7	0	0
4	tcp	net	193.168.20.105	* - 443	10	8968/70	7963/64	4	0
5	tcp	192.168.1.1	65.74.168.210	* - 80	1	52/1	0/0	2	2
6	tcp	192.168.1.1	213.52.240.240	* - 80	1	104/2	0/0	5	2
7	tcp	徐长明	193.168.20.105	* - 22	2	58916/1006	195656/785	2749	160
8	tcp	193.168.20.105	SERVER	* - 1976	2	104/2	0/0	50	20

当前 1 /1页(每页 10 条) 当前显示第1-8条记录(共8条)

图 7.20 查询结果

7.3 URL 过滤

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。单击安全策略界面的【URL 过滤】进入 URL 过滤界面，如图 7.21 所示。

图 7.21 URL 过滤界面

7.3.1 增加 URL 过滤

单击 URL 过滤界面的【增加 URL 过滤策略】按钮，进入 URL 策略管理界面，填写内容如图 7.22 所示。

图 7.22 增加 URL 过滤

增加 URL 过滤的操作可以按照以下步骤进行：

1. 在策略名处输入 URL 过滤策略的名称
2. 在源地址处选择地址对象或在下拉框中单击【增加新地址对象】，进入新地址对象增加界面添加新地址对象。关于增加地址对象的详细操作，可参看增加新地址对象部分
3. 在时间处选择时间对象或在下拉框中单击【增加新时间对象】，进入增加新时间对象界面添加新时间对象。关于增加时间对象的详细操作，可参见时间对象的设置部分
4. 选择过滤的类型
5. 填写过滤的内容，选择要过滤的类型前面的单选框后，在界面右下角会提示相应的输入格式

填写好相关内容后，单击【确定】按钮保存设置，单击【关闭】按钮取消操作。向防毒墙增加一条 URL 过滤规则后，URL 过滤规则记录会在 URL 过滤界面上显示出来。如 7.23 所示。

图 7.23 URL 过滤记录

URL 过滤记录各个字段说明如下：

字段	说明
序号	URL 过滤记录按照阿拉伯数字排序
策略名称	策略的名称
源地址	该策略过滤的数据的来源地址
时间	策略的适用时间
过滤类型	过滤的类型，有网站名、网站地址和文件类型
过滤内容	过滤的具体内容
	修改图标，单击此图标可以进入修改界面修改该策略
	删除图标，单击此图标可以删除该策略

表 7.6 URL 过滤记录界面说明

7.3.2 修改 URL 过滤

若要修改某条 URL 过滤记录，单击该条记录后面的修改图标进入修改界面，填写要修改的内容如图 7.24 所示。

图 7.24 修改 URL 过滤记录

修改 URL 过滤操作和增加 URL 过滤操作相同，用户可参看增加 URL 过滤部分。

修改完成后，单击【确定】按钮保存修改内容，单击【关闭】按钮取消操作。

7.3.3 删除 URL 过滤

若要删除某条 URL 过滤记录，单击该记录后面的删除图标，弹出系统提示如图 7.25 所示。

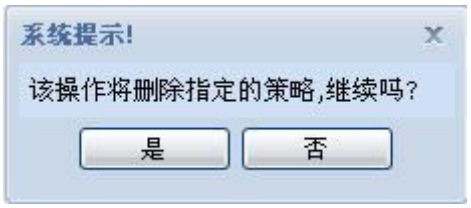


图 7.25 删除 URL 过滤记录

单击【是】按钮删除记录，单击【否】按钮取消操作。单击【是】按钮后，系统弹出删除成功的提示框如图 7.26 所示。

图 7.26 URL 过滤记录成功删除

单击【确定】按钮，完成 URL 记录的删除操作。

7.4 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。

单击安全策略界面的【IP 黑名单】进入 IP 黑名单界面，如图 7.27 所示。

图 7.27 IP 黑名单界面

7.4.1 增加黑名单 IP

单击【增加黑名单 IP】进入增加 IP 黑名单界面，如图 7.28 所示。

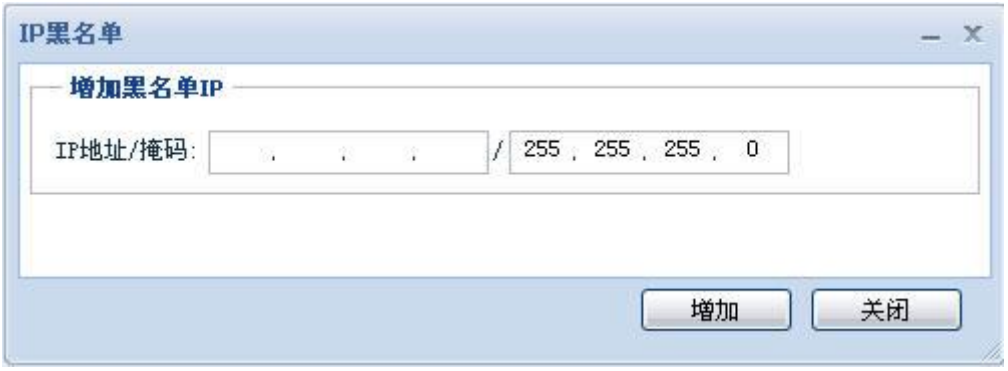


图 7.28 增加 IP 黑名单

输入黑名单形式为 IP 地址/掩码，填入 IP 地址后，可以在掩码栏手动填写子网掩码，当掩码为 255.255.255.255 时，代表单个 IP。

输入已经确认是恶意 IP 的地址或地址段，单击【增加】按钮保存设置，单击【关闭】按钮取消操作。分别添加一个网段 192.168.20.0/255.255.255.0 和单个 IP：192.168.10.20/255.255.255.255 后的 IP 黑名单如图 7.29 所示。

图 7.29 IP 黑名单

提示：添加 IP 黑名单的注意事项

1. 不允许添加已经存在于黑名单中的 IP（即不允许重复添加）；
2. 不允许添加管理员当前使用的管理主机的 IP；
3. 不允许添加特权 IP（如果要添加存在于特权 IP 中的 IP 地址为黑名单 IP，可以先删除特权 IP，然后再进行添加，删除特权 IP 可以参看 7.1.1 节的删除特权 IP 部分。

7.4.2 修改黑名单 IP

若要修改某个黑名单 IP，单击该条记录后面的修改图标，进入修改页面，如图 7.30 所示。

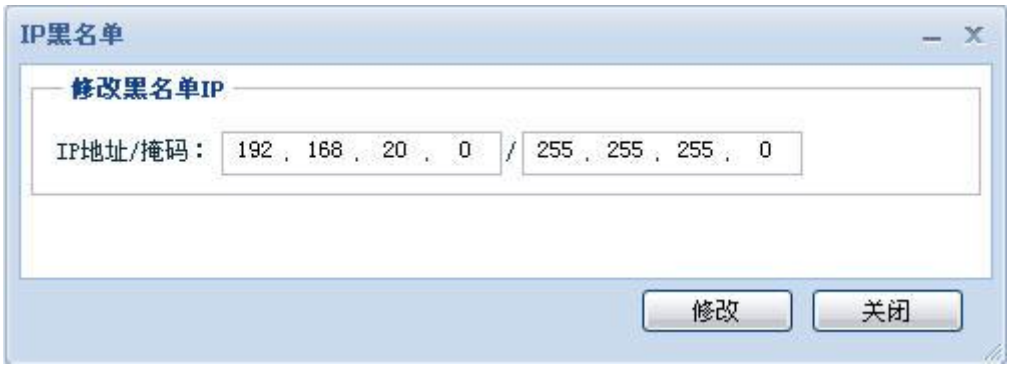


图 7.30 修改黑名单 IP

输入要修改的黑名单 IP，输入格式和增加黑名单 IP 时相同。可参看增加黑名单 IP 部分。

填写好修改的 IP 地址后，单击【修改】按钮保存修改操作，单击【关闭】按钮取消操作。

7.4.3 删除黑名单 IP

若要删除某个黑名单 IP，可以单击该条记录后面的删除图标，弹出系统提示如图 7.31 所示。

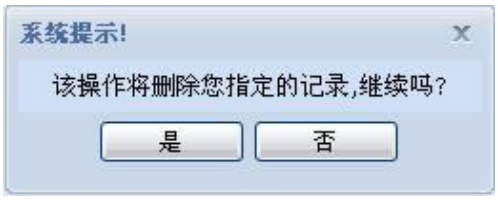


图 7.31 系统提示是否删除记录

单击【是】按钮删除记录，单击【否】按钮取消操作。

第八章 虚拟专网

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。

本节从以下两个方面介绍瑞星防毒墙的虚拟专网的功能：

- PPTP VPN 通道：建立远程用户和内部网的连接通道。例如在外出差的员工和公司之间。
- IPSec VPN 通道：建立两个内部网络之间的连接通道。例如总公司和异地分公司或是地理位置不同的两个分公司之间。

8.1 PPTP VPN 通道

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【虚拟专网】进入虚拟专网主界面，如图 8.1 所示。

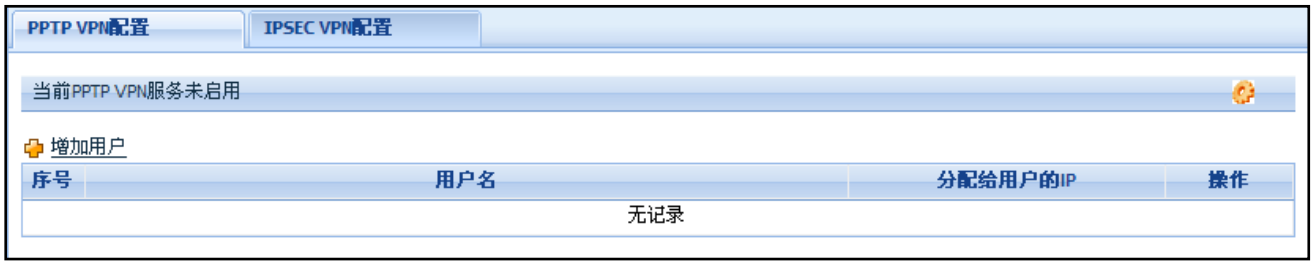


图 8.1 虚拟专网主界面

8.1.1 PPTP VPN 服务

PPTP VPN 服务有两种状态：启用和停用。

- **启用 PPTP VPN 服务**

在虚拟专网主界面上查看 PPTP VPN 服务状态，防毒墙默认停用 PPTP VPN 服务。若要启用该服务，单击设置图标进行设置，弹出窗口如图 8.2 所示。

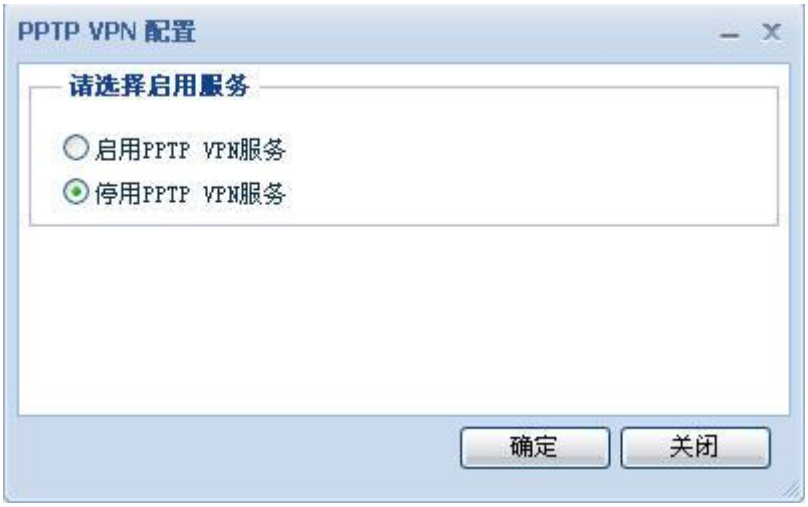


图 8.2 PPTP VPN 配置

单击启用 PPTP VPN 服务前面的单选框启用 PPTP VPN 服务，启用 PPTP VPN 服务后的界面如图 8.3 所示。当启用 PPTP VPN 服务后，弹出隐藏的 PPTP VPN 的详细设置界面。

图 8.3 启用 PPTP VPN 服务

PPTP VPN 设置界面各字段说明如下：

字段	说明
认证方式	包含四种认证方式，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；MS-CHAP V2加密可以提供交互身份验证，在发送和接收数据时使用不同的加密密钥；

接口地址	从下拉框中选择一个内部接口的IP地址，该IP将会成为分配给客户端的网关地址
起始地址	当外部用户拨入后，防毒墙分配给客户端的内网IP段的起始IP地址
终止地址	当外部用户拨入后，防毒墙分配给客户端的内网IP段的终止IP地址
配置内部DNS	当外部用户拨入后，防毒墙分配给PPTP客户端的内部域名解析服务器地址
配置内部WINS	当外部用户拨入后，防毒墙分配给PPTP客户端的内部网际名称服务器地址

表 8.1 PPTP VPN 服务说明

当启用 PPTP VPN 服务后，配置 PPTP VPN 的详细信息可按照以下步骤进行：

1. 选择一种认证方式
2. 选择一个内网接口地址
3. 填写起始地址，用于分配给 PPTP 客户端的起始 IP 地址
4. 填写终止地址，用于分配给 PPTP 客户端的 IP 的结束地址，必须大于起始地址
5. 配置内部 DNS，填写用于分配给 PPTP 客户端的内部域名解析服务器地址
6. 配置内部 WINS，填写用于分配给 PPTP 客户端的内部网际名称服务器地址

填写好相关内容后，单击【确定】按钮启用 PPTP VPN 服务，系统弹出启用成功提示界面，如图 8.4 所示。单击【取消】按钮取消操作。

图 8.4 启用 PPTP VPN 服务成功提示界面

提示：PPTP VPN 服务的使用前提

启用了 PPTP VPN 服务以后，还需要在【网络配置】里把外网口（E0、E1 或 E2）高级设置里的 PPTP 服务开启，该 VPN 服务才可以使用。具体操作参看外网口接口设置部分。

启用了 PPTP VPN 服务后，虚拟专网主界面会显示当前 PPTP VPN 服务已启用，如图 8.5 所示。

图 8.5 PPTP 服务为启用状态

- **停用 PPTP VPN 服务**

若要停用 PPTP VPN 服务时，单击 PPTP VPN 服务状态后面的设置图标，进入 PPTP VPN 配置界面如图 8.6 所示。

图 8.6 PPTP 的服务状态

单击停用 PPTP VPN 服务前面的单选框停用 PPTP 服务，如图 8.7 所示。

图 8.7 停用 PPTP 服务

单击【确定】按钮保存 PPTP VPN 设置，停用 PPTP VPN 通道服务，单击【取消】按钮取消操作。单击【确定】按钮后，系统弹出成功提示界面如图 8.8 所示；

图 8.8 停用 PPTP VPN 服务成功提示界面

停用了 PPTP VPN 服务后，虚拟专网主界面会显示当前 PPTP VPN 服务未启用，如图 8.9 所示

图 8.9 PPTP 服务为停用状态

8.1.2 PPTP VPN 用户

防毒墙的 PPTP VPN 服务是为了使远程用户能够通 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，在通道建立之前，远程用户需要首先拥有防毒墙 PPTP VPN 用户身份，这可以通过添加 PPTP VPN 用户实现。

- **增加用户**

单击虚拟专网主界面中的【增加用户】进入添加 PPTP VPN 用户页面，如图 8.10 填写用户信息。

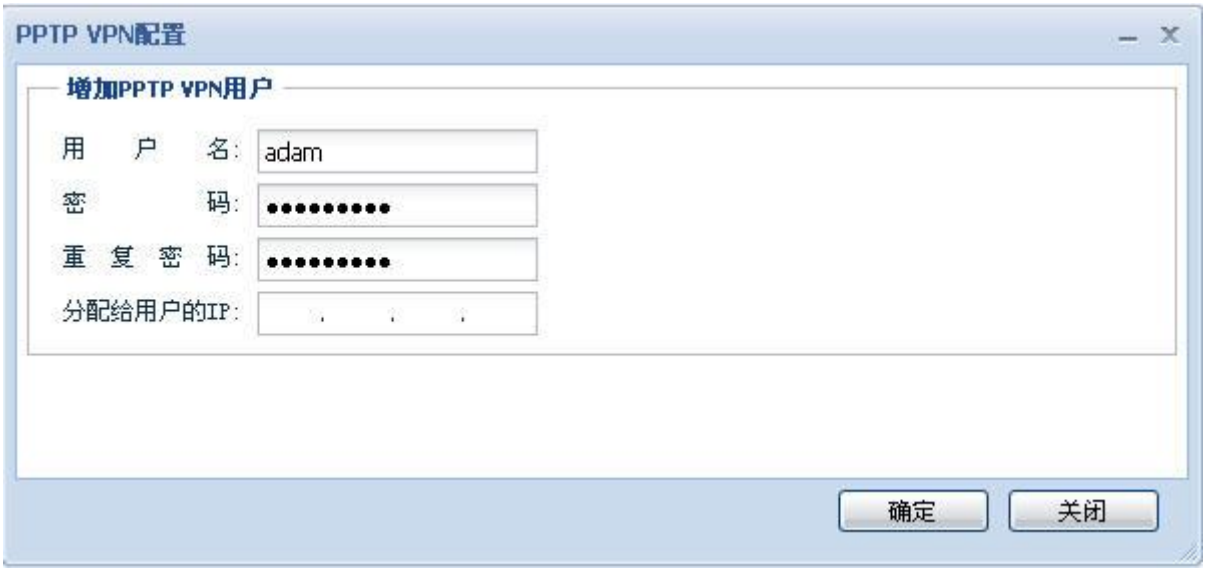


图 8.10 增加 PPTP VPN 用户

增加用户界面的各字段说明：

字段	说明
用户名	用户的名称
密码	为用户设置一个访问密码
重复密码	再次输入密码
分配给用户的IP	当外部用户拨入后，防毒墙分配的用户使用的内部IP地址

表 8.2 增加用户界面说明

提示：关于分配给用户 IP 地址

如果不填写 IP 地址的话，防毒墙会自动分配给 VPN 用户一个内部 IP 地址；如果人为为客户端分配 IP，填写的 IP 必须在启用 PPTP 服务的时候填写的地址范围之内。

增加用户的操作步骤可以按照如下步骤进行：

1. 在用户名处输入远程用户使用的用户名
2. 在密码和重复密码处输入密码
3. 输入分配给用户的 IP 地址

填完内容后，单击【确定】按钮保存设置，单击【关闭】按钮取消操作。单击【确定】按钮后系统弹出成功添加用户的提示框，如图 8.11 所示。

图 8.11 添加用户成功

单击【确定】按钮完成添加用户操作。

当向防毒墙增加一条用户信息后，该记录会在虚拟专网主界面上显示出来，如图 8.12 所示。

图 8.12 PPTP VPN 用户信息

- **修改用户**

当需要修改用户信息时，单击该用户信息后面的图标，进入修改页面，如图 8.13 所示。

图 8.13 修改用户信息

修改用户信息的操作可以依照如下步骤进行：

1. 在用户名处填写要修改的用户名
2. 在密码和重复密码处输入要修改的密码，如果不填写，则不更改密码
3. 输入要分配给用户的 IP 地址

单击【修改】按钮保存修改操作，单击【关闭】按钮取消操作。单击【修改】按钮后系统弹出修改成功的提示框，如图 8.14 所示。

图 8.14 修改用户成功

单击【确定】按钮，完成修改用户的操作。

- **删除用户**

若要删除某个用户记录，单击该用户信息后面的删除图标，系统弹出是否要删除用户的提示框，如图 8.15 所示。

图 8.15 是否要删除 VPN 用户

单击【是】按钮删除用户，单击【否】取消操作。

8.2 IPSEC VPN 通道

IPSec 是一套比较完整成体系的 VPN 技术，它可以提供访问控制、无连接完整性、数据源鉴别、载荷机密性和有限流量机密等安全服务，弥补由于 TCP/IP 协议体系自身带来的安全漏洞。单击虚拟专网主界面上的【IPSec VPN 配置】进入 IPSec VPN 通道主界面，如图 8.16 所示。

图 8.16 IPSec VPN 通道主界面

8.2.1 IPSec 通道操作

- **增加 IPSec 通道**

在 VPN 通道配置主界面上单击【增加 IPSec 通道】，进入 VPN 通道增加页面，再单击【高级】展开高级选项，如图 8.17 所示。

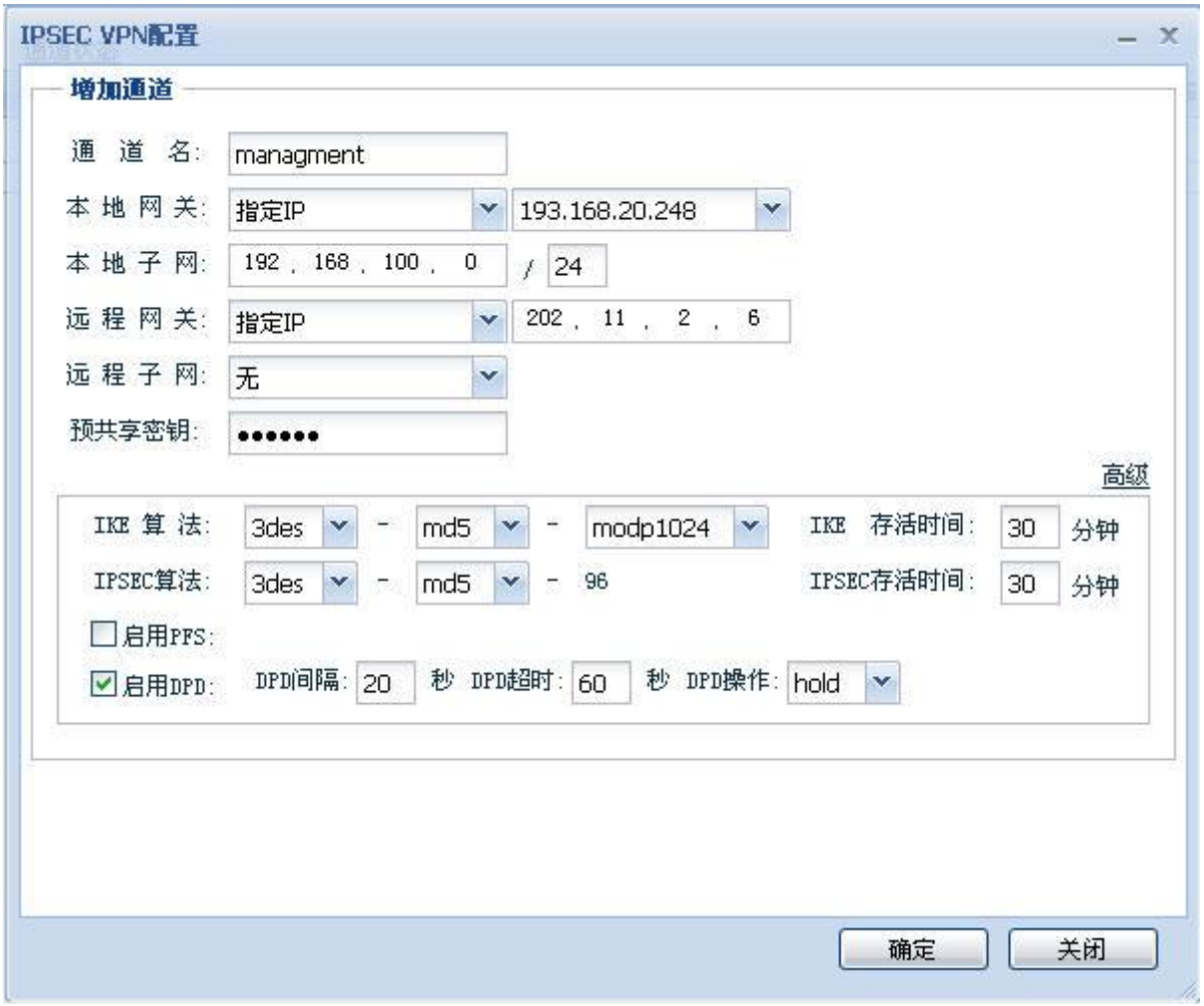


图 8.17 增加 IPSEC 通道

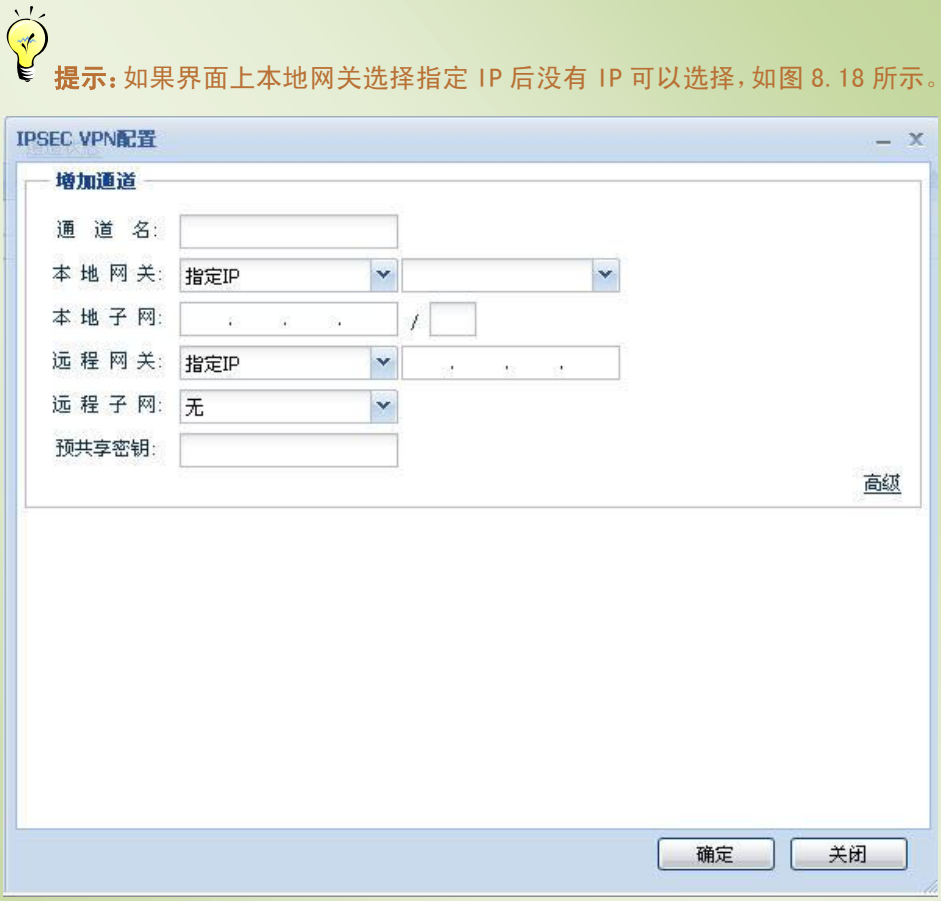


图 8.18 没有指定 IP 可以选择

提示：如果界面上本地网关选择指定 IP 后没有 IP 可以选择，如图 8.18 所示。

遇到这种情况，可以有两种选择：

1. 本地网关后面选择指定设备 ID；
2. 进入【网络配置】➔【接口配置】，把外网接口（E0、E1 或 E2）中接入方式配置为静态 IP、动态 IP 或者 PPPOE 并且在【高级设置】里将 VPN 服务复选框勾选上。具体设置参看外网口的接口设置。

增加 IPSEC 通道的操作可以按照如下步骤进行：

1. 填写通道名称
2. 在本地网关中，“指定 IP”为指定本地的网关地址；“使用设备 ID”则通过瑞星防毒墙唯一的设备 ID 号查询本地网关的公网 IP 地址
3. 本地子网中填写本地局域网的一个网段
4. 远程网关可以选择指定 IP 或者指定设备 ID，“指定 IP”时需要输入远程网关的 IP；“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 VPN 隧道另一端网络中的子网地址。“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. 预共享密钥中填入一个不少于 8 位的自定义的密码

7. 选择协商密钥的加密方式和协商超时时间
8. 选择数据传输密钥的加密方式和加密传输超时时间
9. 是否启用 PFS，此功能为可选配置，启用该功能后，向前保密加密传输数据，防止攻击者破解密钥
10. 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。

填好相关内容后，单击【确定】按钮确认添加通道，单击【关闭】按钮取消操作。单击【确定】按钮后，系统弹出添加通道成功提示界面，如图 8.19 所示

图 8.19 添加通道成功提示界面

单击【确定】后添加了一个通道，添加通道成功后可以在 IPSEC VPN 主界面查看通道配置信息，

如图 8.20 所示：

图 8.20 通道配置

通道配置的各字段的说明如：

字段	说明
通道名称	IPSEC VPN通道的名字
本地网关	本地的网关地址
本地子网	本地的子网地址组
远程网关	远程的网关地址
远程子网	远程的子网地址组
	通道启用的标志，单击它可以停用通道，图标变为  ，再单击可以开启通道
	修改图标，单击可以进入通道修改界面对通道进行修改
	删除图标，单击可以删除通道

表 8.3 通道配置名词解释

- **修改 IPSec 通道**

若要修改通道，单击要修改的通道配置一行右侧的修改图标，进入通道设置修改界面，如图 8.21 所示。

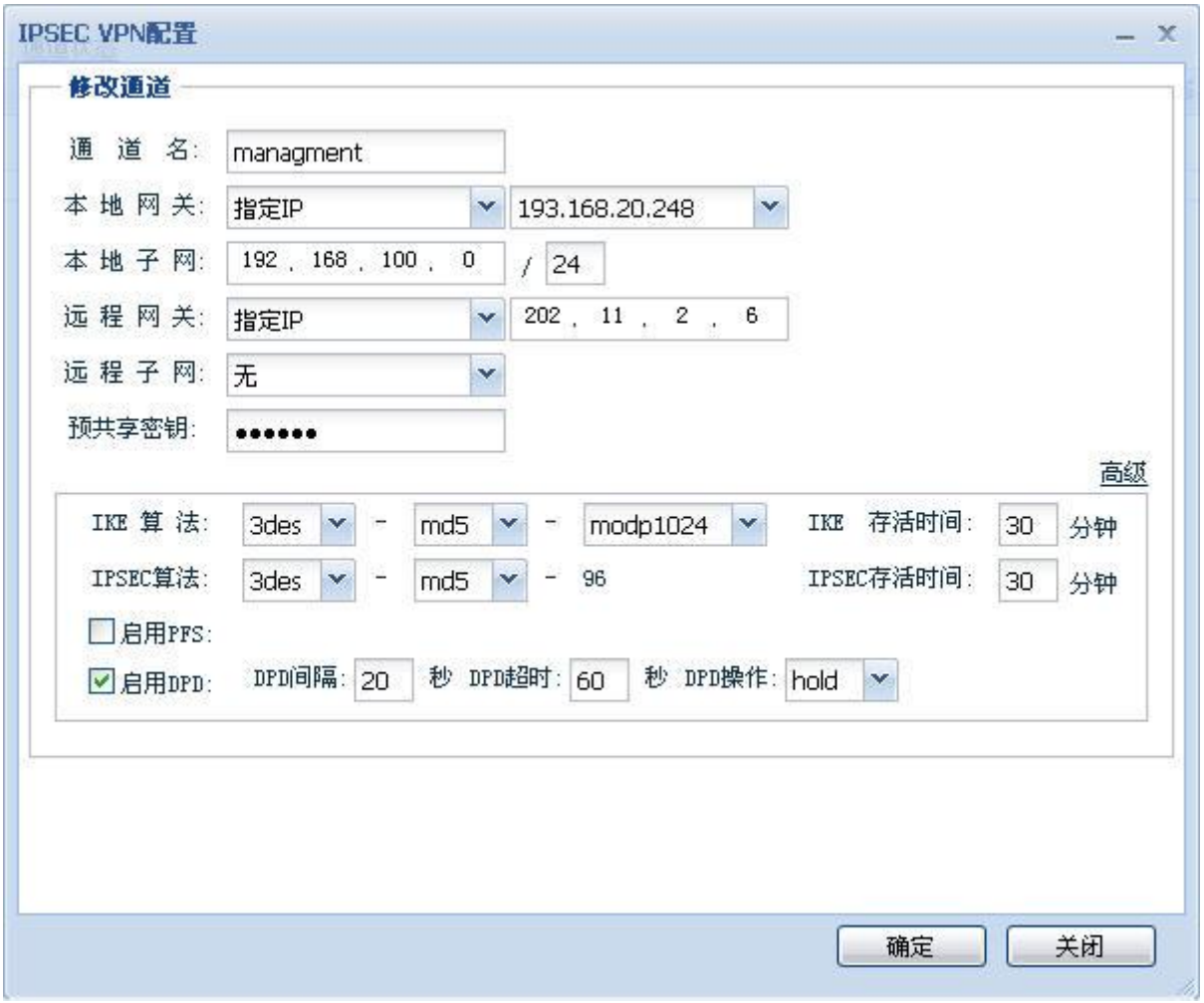


图 8.21 修改通道配置界面

填写要修改的通道信息，具体操作可参看增加 IPSEC VPN 通道部分。

修改完后，单击【确定】按钮保存设置，单击【关闭】取消操作。单击【确定】按钮后，系统弹出修改成功提示界面，如图 8.22 所示。

图 8.22 修改通道成功提示界面

- **启用与停用 IPSec 通道**

  IPSec VPN 通道有两种状态：启用与停用。当通道为启用状态时，单击该通道后面的图标停用正在启用的通道，图标由变为，停用通道成功。当通道为停用状态时，单击停用图标可以启用通道，图标变为同时系统提示启用通道成功。

- **删除 IPSec 通道**

当要删除通道时，单击该通道后面的删除图标，系统会弹出删除成功的提示框，如图 8.23 所示。

图 8.23 删除通道成功

单击【确定】按钮，完成删除通道操作。

8.2.2 IPSec 通道状态

单击 IPSec VPN 通道主界面上的【通道状态】进入通道状态界面，如图 8.24 所示

图 8.24 通道状态

通道状态各字段说明如下：

字段	说明
序号	通道按照阿拉伯数字排序
通道名称	IPSEC VPN通道的名字
本地网关	VPN通道的本地网关的地址
本地子网	VPN通道的本地子网
远程网关	VPN通道远端网关的地址
远程子网	VPN通道远端的子网地址
状态	有两种，connected为连接状态， waiting为等待状态

表 8.4 通道状态界面名词解释

单击【刷新】按钮可以刷新防毒墙的 VPN 通道状态，单击【关闭】按钮关闭通道状态页面。

第九章　防病毒

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 5.1.2 软件升级部分。

用户可以从以下两个方面进行防毒墙的防病毒配置：

- 防毒配置：对使用一些常见协议进行传输的数据进行病毒查杀
- 瑞星网络版联动配置：瑞星防毒墙与瑞星杀毒软件网络版协同工作。

9.1 防毒配置

防毒墙进行防毒配置后，如果指定端口用相关协议进行数据传输，防毒墙将对数据进行杀毒操作。单击【防毒配置】进入防毒配置的主界面，如图 9.1 所示。

图 9.1 防毒配置主界面

防毒配置主界面各字段说明如下。

字段	说明
默认端口	协议使用的默认端口
特殊配置	如果服务器不使用默认端口，更换为别的端口，可以在这里添加端口
源地址不杀毒	默认都杀毒，如果添加一个源地址IP，则从此IP传输的数据经过防毒墙将不进行杀毒
目的地址不杀毒	默认都杀毒，如果添加一个目的地址IP，则传送到此IP的数据经过防毒墙将不进行杀毒

表 9.1 防毒协议的名词解释

防毒配置中协议的启用与停用可以通过单击协议名称前面的复选框来实现。所有的协议都默认设置为启用状态，如上图 9.1 所示，可以单击协议名称前面的复选框停用协议，同时该项字体颜色变灰表示该协议为停用状态，如图 9.2 所示。

图 9.2 防毒墙支持的协议

- HTTP 协议

HTTP 协议的默认端口为 80，并开启 HTTP 协议的杀毒服务，防毒墙对使用 HTTP 协议传输的数据包都进行杀毒处理。用户可以根据需要在确认源地址或目的地址安全的情况下设置源地址 IP 不杀毒或是目的地址 IP 不杀毒，减少防毒墙的性能开销。

✓ 特殊配置

单击【特殊配置】后面带有下划线的文字（这里的【无】）进行特殊配置，有的服务器提供服务时不用默认的端口而用其他的端口，在这里可以添加服务器用的其他端口或者 IP 地址:端口的形式。添加内容如图 9.3 所示。

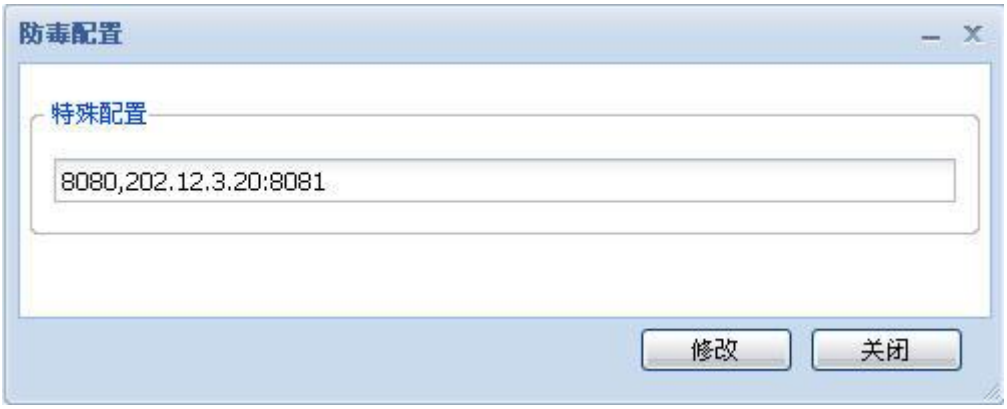


图 9.3 HTTP 协议的特殊配置

单击【修改】按钮保存配置，单击【关闭】按钮取消操作。单击【修改】按钮后，系统弹出修改成功提示框，如图 9.4 所示。

图 9.4 修改 HTTP 特殊配置成功

✓ 源地址不杀毒

默认所有用 HTTP 协议传输的数据都进行杀毒处理，单击【源地址不杀毒】后面带有下划线的文字进入源地址不杀毒列表界面，添加 IP 则从此 IP 传输的数据经过防毒墙时不进行杀毒操作，添加内容如图 9.5 所示。

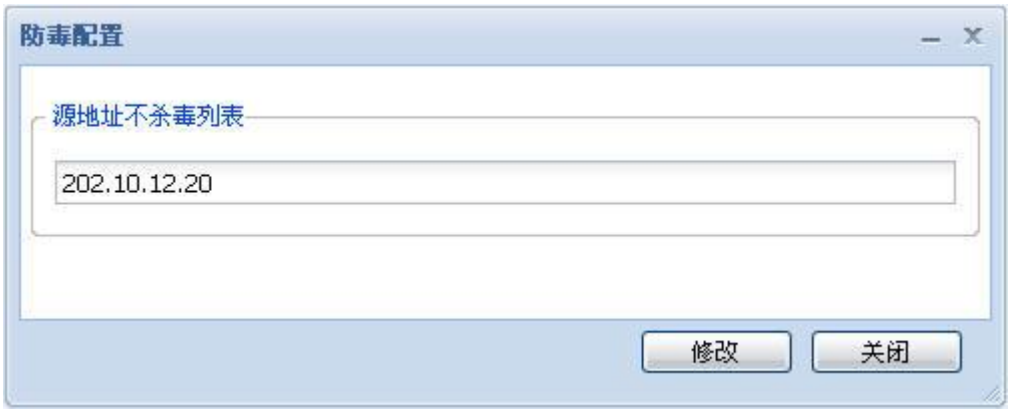


图 9.5 源地址不杀毒列表

单击【修改】按钮保存配置，单击【关闭】按钮取消操作。单击【修改】按钮后，系统弹出修改成功的提示框，如图 9.6 所示。

图 9.6 修改 HTTP 源地址不杀毒列表成功

✓ 目的地址不杀毒

默认经过防毒墙使用该协议的数据都进行杀毒，如果添加一个目的 IP，则传送到此 IP 的数据防毒墙不进行杀毒操作，单击【目的地址不杀毒】后面带有下划线文字进入目的地址不杀毒列表，添加内容如图 9.7 所示。

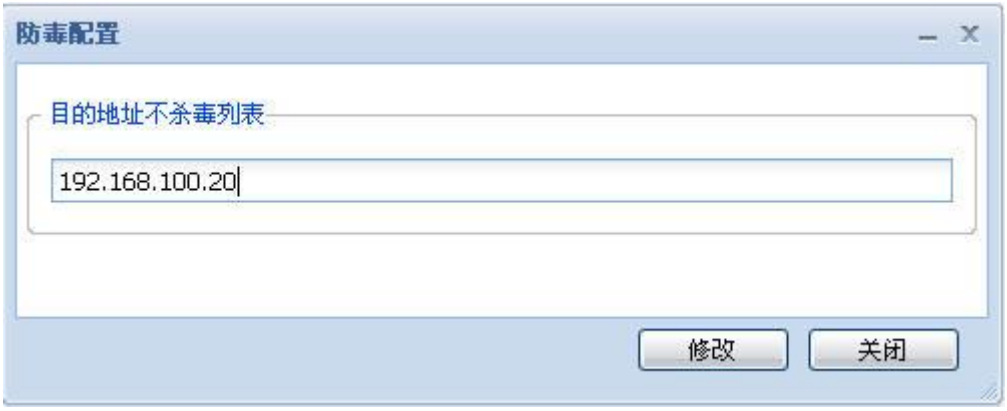


图 9.7 目的地址不杀毒列表

单击【修改】按钮保存配置，单击【关闭】按钮取消操作。单击【修改】按钮后，系统弹出修改成功的提示框，如图 9.8 所示。

图 9.8 修改 HTTP 目的地址不杀毒列表成功

设置完成后，有关 HTTP 协议的杀毒设置结果会在界面上显示出来，如图 9.9 所示。

图 9.9 HTTP 协议的设置结果

- FTP 协议，与前面防毒协议里 HTTP 协议的设置过程一样，可参见 HTTP 协议的设置步骤
- SMTP 协议，与前面防毒协议里 HTTP 协议的设置过程一样，可参见 HTTP 协议的设置步骤
- POP3 协议，与前面防毒协议里 HTTP 协议的设置过程一样，可参见 HTTP 协议的设置步骤
- MSN 协议， 因为该协议是微软公司开发的协议，使用固定端口 1863，所以不需要其他的配置
- IMAP4 协议，与前面防毒协议里 HTTP 协议的设置过程一样，可参见 HTTP 协议的设置步骤

提示：关于协议的停用说明

由于每个协议有三个配置选项（MSN 协议除外），如果停用部分配置，单击配置后面带有下划线的文字（参见 HTTP 协议的配置），将配置的内容删除即可。如果要停用协议，单击协议名称前面的复选框不选中协议即可。

9.2 防毒配置高级

单击扩展图标或者高级展开高级选项可以进行进一步的杀毒配置，选项前面的复选框选中代表启用了相应的功能，如图 9.10 所示。

图 9.10 防毒配置的高级界面

高级设置分以下三部分进行介绍：杀毒基本配置、HTTP 协议设置和 FTP 协议设置。

9.2.1 杀毒基本配置

- **设置最大查杀毒文件**

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。用户可以指定查杀毒文件的大小，若传输的文件超过指定的大小防毒墙将不做查杀。单击【查杀文件最大】后面带有下划线文字进入设置最大查杀文件大小的界面，指定最大查杀文件大小（范围为 1 到 10），填写内容如图 9.11 所示。

图 9.11 设置最大查杀文件大小

单击【修改】按钮保存配置结果，单击【关闭】按钮取消操作。单击【修改】按钮后，系统弹出修改成功的提示框，如图 9.12 所示。

图 9.12 成功修改最大查杀文件大小

单击【确定】按钮，完成设置最大查杀文件大小的操作。

- **设置最大压缩文件层数**

当文件被压缩时，指定防毒墙可以识别的压缩层数（最多可以解压缩 100 层，但不建议用户设置太多的压缩层数，因为层数越大，防毒墙进行病毒查杀花费的时间越多）。单击【压缩文件层数最大】后面带有下划线的文字进入设置查杀层数界面，指定最大查杀层数，如图 9.13 所示。

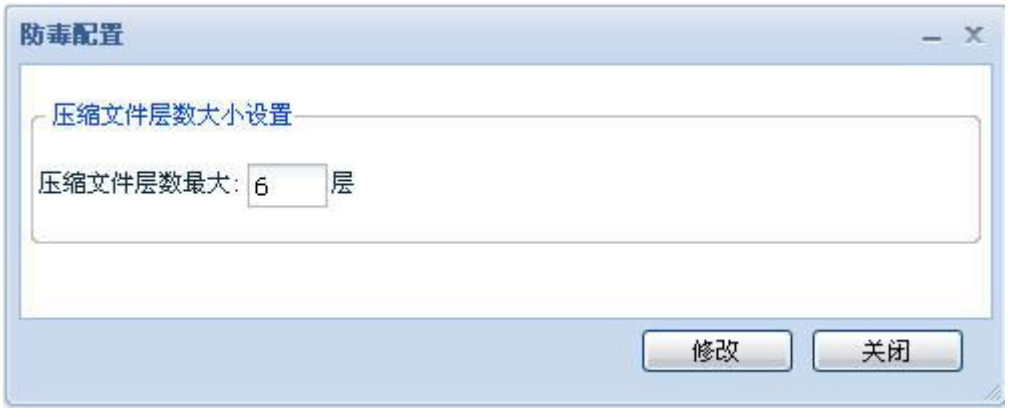


图 9.13 设置最大查杀层数

单击【修改】按钮保存配置结果，单击【关闭】按钮取消操作。单击【修改】按钮后，系统弹出修改成功的提示框，如图 9.14 所示。

图 9.14 成功修改压缩文件层数

单击【确定】按钮，完成设置压缩文件层数的操作。

- **设置禁止传输的文件类型**

单击【禁止传输的文件类型】后面带有下划线的文字进入禁止传输文件类型设置页面，系统默认禁止传输一些出现问题几率比较大的文件类型，这样会使您的网络更加安全，如图 9.15 所示；

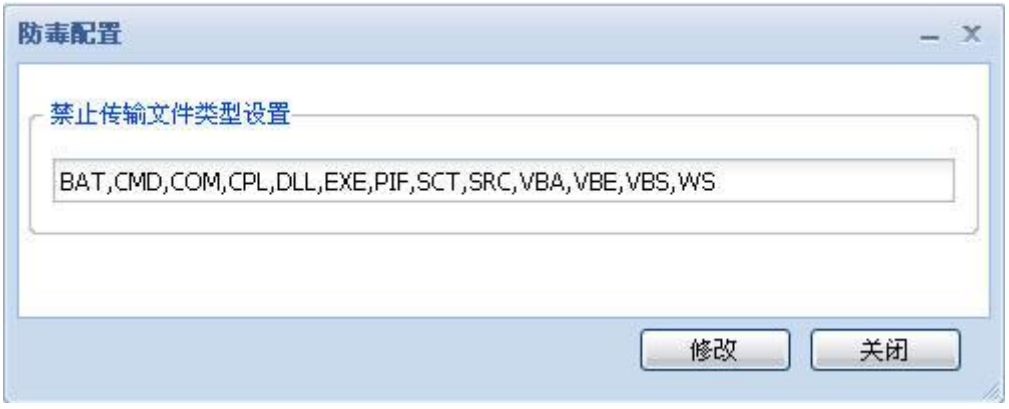


图 9.15 设置禁止传输文件类型

单击【修改】按钮保存配置结果，单击【关闭】按钮取消操作。单击【修改】按钮后，系统弹出修改成功提示框，如图 9.16 所示。

图 9.16 成功修改禁止文件传输类型

单击【确定】按钮，完成设置禁止传输的文件类型操作。

- **设置不查杀的文件类型**

用户可以将某些潜在危险较小的文件类型设置为不查杀文件类型，对其不进行杀毒操作，提高防毒墙性能。单击【设置不查杀的文件类型】后面带有下划线的文字进入不查杀的文件类型设置页面，指定不查杀的文件类型，如 RAR，如图 9.17 所示。

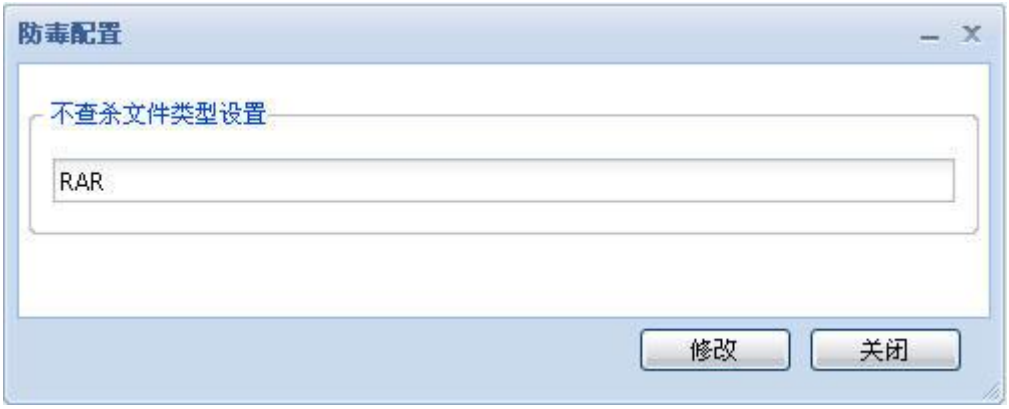


图 9.17 设置不查杀文件类型

单击【修改】按钮保存配置结果，单击【关闭】按钮取消操作。单击【修改】按钮后，系统弹出修改成功提示框，如图 9.18 所示。

图 9.18 成功修改不查杀文件类型

单击【确定】按钮，完成设置不查杀文件类型的操作。

- 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：防毒墙对内网用户浏览的网页有选择的病毒查杀，提高用户的上网速度
- 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
- 查杀图片病毒：对图片文件进行查杀处理
- 检查可疑脚本：对可疑脚本进行检测并阻断
- 隔离病毒文件：把含有病毒的文件隔离

9.2.2 HTTP 协议配置

- 禁用下级 HTTP 代理：通过防毒墙后的数据不能是指向一个外部代理服务器的数据
- 禁用非标准 HTTP 协议：防毒墙进行 HTTP 协议杀毒操作时，杀毒基本配置里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：启用此功能将过滤防毒墙已经分析出来的恶意网站和病毒 URL 地址，防毒墙将对此列表不断更新
- 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，单击【启用 SQL 注入防护】后面带有下划线的文字进入设置页面，输入内部服务器的地址，如图 9.19 所示。

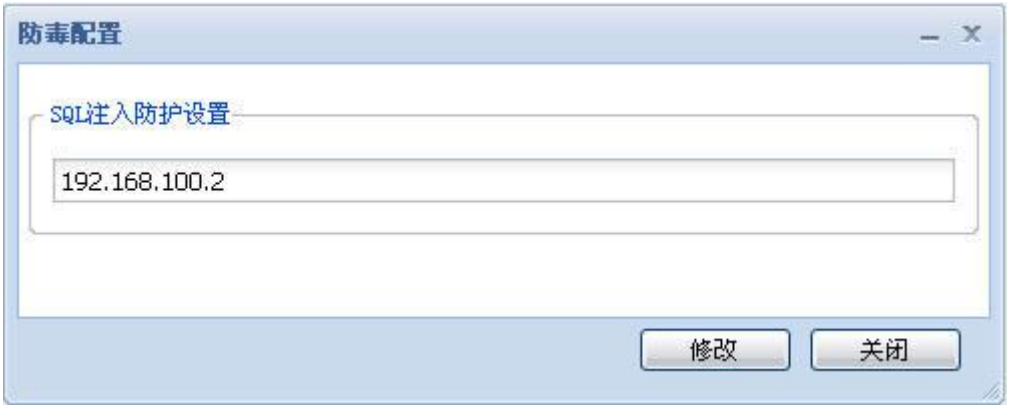


图 9.19 SQL 注入防护

单击【修改】按钮保存配置结果，单击【关闭】按钮取消操作。单击【修改】按钮后，系统弹出修改成功提示框，如图 9.20 所示。

图 9.20 成功修改内部 HTTP 服务器配置

单击【确定】按钮，完成修改内部 HTTP 服务器配置操作。

9.2.3 FTP 协议配置

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。

9.3 瑞星网络版联动配置

内网主机安装瑞星杀毒软件网络版后，其系统中心负责监控内网主机的瑞星杀毒软件网络版的配置情况并将信息传送给防毒墙，防毒墙可以根据主机的配置情况对其进行相关的控制操作，例如阻止不安全主机访问网络。使用瑞星网络版联动功能，防毒墙可以与瑞星杀毒软件网络版相辅相成地管理着内部网络，

使网络更加安全。

9.3.1 联动功能配置

联动功能配置功能主要用于启用或是停止防毒墙与瑞星杀毒软件网络版的联动功能，在联动功能配置部分，单击【启用与网络版杀毒联动功能】前的复选框选择启用此项功能，如图 9.21 所示：

图 9.21 联动功能配置界面

若想停用联动功能，只需再次单击复选框，将其置为未选中状态即可。

9.3.2 瑞星网络版中心配置

瑞星网络版中心配置界面如图 9.22 所示。

图 9.22 瑞星网络版中心配置界面

瑞星网络版中心配置各个字段说明：

字段	说明
系统中心信息	初始状态为无，单击“无”，在弹出配置对话框进行配置系统中心地址及通讯端口
查询间隔	防毒墙和瑞星杀毒软件网络版系统中心通信的时间间隔，单击“30分钟”，在弹出配置对话框，填入瑞星杀毒软件网络版系统中心与防毒墙协商间隔时间
客户端安装包路径	瑞星杀毒软件网络版客户端安装包文件路径，单击“无”，在弹出配置对话框填入瑞星杀毒软件网络版客户端安装包文件路径

表 9.2 瑞星网络版中心配置界面说明

9.3.3 对不安全主机的控制策略

防毒墙根据管理员制定的内网安全性定义对不安全主机可以采取相应的控制策略，如图 9.23 所示。

图 9.23 防毒墙对不安全主机的控制策略

防毒墙对不安全主机的控制策略界面字段说明：

字段	说明

阻断用户访问	防毒墙禁止不安全主机访问网络，单击“阻断所有访问”弹出配置对话框，阻断方式有两种，第一种仅阻断WEB访问，第二种阻断所有的访问，管理员可以根据需要选择阻断方式。
发送WEB告警信息	防毒墙自动对不安全主机发送WEB告警信息，单击“发送标题”，该项功能启用后，对于未满足内网主机安全性定义的主机，在浏览网页时会在指定的周期内在WEB页面发出不安全提示警告信息。
发送客户端控制台信息	该项功能启用后，防毒墙对不安全主机客户端控制台发送告警信息。
发送管理员邮件警告	该项功能启用后，对于未满足内网主机安全性定义的主机，防毒墙会指定的时间向管理员发送邮件告警。单击时间处，在弹出的对话框中配置发送警告的时间。

表 9.3 防毒墙对不安全主机的控制策略说明

9.3.4 内网主机安全性定义

内网主机安全选项界面如图 9.24 所示。用户可以根据需要制定相应的安全策略，可以选中几条或者不选，为了使内部网络更加安全，建议用户全部选中。定义了内网主机安全性之后，控制中心认为未满足条件的内网主机是不安全的，可以发信息给防毒墙，防毒墙可以对不安全主机增加控制策略，对不安全主机的控制策略将在 9.3.3 节对不安全主机的控制策略中详细说明。

图 9.24 内网主机的安全性定义界面

内网主机安全性定义各个字段说明：

字段	说明
安装瑞星网络版客户端	勾选此选项对内网主机安全定义为安装瑞星杀毒软件网络版软件的计算机属于安全主机
开启文件监控	勾选此选项对内网主机安全定义为瑞星杀毒软件网络版软件开启文件监控属于安全主机
升级到最新版本	勾选此选项对内网主机安全定义为瑞星杀毒软件网络版软件已经升级到最新版本属于安全主机
启用瑞星网络版防火墙	勾选此选项对内网主机安全定义为启用瑞星网络版防火墙软件的计算机属于安全主机
没有高危漏洞	勾选此选项对内网主机安全定义为瑞星杀毒软件网络版未发现操作系统中存在高危漏洞属于安全主机

表 9.4 内网主机安全性定义界面说明

第十章 入侵防御

把已经发现的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。当外部主机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【入侵防御】进入入侵防御设置界面，如图 10.1 所示。

图 10.1 入侵防御设置界面

10.1 查看入侵防御规则

瑞星 RSW-320 防毒墙提供了七种类型的入侵防御，分别是蠕虫病毒入侵防御、Web 服务器入侵防御、FTP 服务器入侵防御、Database 服务器入侵防御、Mail 服务器入侵防御、Windows 系统入侵防御、其他入侵防御。每种类型列举了常见的漏洞作为入侵防御规则。

单击入侵防御界面各类型入侵防御规则前的展开图标，可以查看具体的入侵防御规则，以查看病毒蠕虫类的入侵防御规则为例。如图 10.2 所示。

图 10.2 入侵防御规则的查看界面

单击收缩图标可以隐藏入侵防御具体信息。

提示：关于入侵防御规则的解释

在如图 10.2 所示界面，单击带有下划线的入侵防御规则可以进入瑞星的网站查看入侵防御规则的详细解释。例如：单击 2003蠕虫王 false(Worm.NetKiller.2003) 可以进入 http://it.rising.com.cn/Channels/Service/2006-07/1153196673d22647.shtml 查看该条防御规则的具体信息。

10.2 入侵防御规则的启用与停用

瑞星防毒墙默认不启用这些规则，管理员可根据实际情况有选择性的启用这些规则。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规则。

提示：关于开启入侵防御前的准备工作

使用入侵防御时，用户需在【网络配置】➔【接口配置】中开启接口的 IPS 服务，关于接口服务相关内容请参看接口服务设置部分。

- **启用入侵防御规则**

入侵防御规则的启用有两种方式，一种方式是单击各类型前的当选框启用入侵防御规则，这种情况下该类型中列举的具体防御规则都被启用。例如：单击蠕虫病毒入侵防御，将启用病毒蠕虫类中的所有入侵防御规则，如图 10.3 所示。

图 10.3 启用蠕虫病毒入侵防御所有入侵防御规则

另一种方式是由选择性的启用规则，我们以病毒蠕虫类为例介绍这种方式下的入侵防御规则的启用。

1. 在入侵防御设置界面，单击病毒蠕虫类前的展开图标，展开病毒蠕虫类的具体规则（默认全部停用，颜色全部为灰色），如图 10.4 所示。

图 10.4 蠕虫病毒入侵防御规则列表

2. 单击病毒蠕虫列表下各具体规则前的复选框（可多选），选中用户想要启用的入侵防御规则，如图 10.5 所示。

图 10.5 选择性启用入侵防御规则

- **停用入侵防御规则**

  若要停用某些规则，单击需要停用的入侵防御规则前面的复选框即可。

第十一章 日志审计

本章我们主要从以下两个方面了解防毒墙日志审计的详细设置：

- 日志审计：查看防毒墙日志记录的详细信息
- 日志统计：查看防毒墙日志记录的统计信息

11.1 日志审计

单击防毒墙功能菜单【日志审计】进入日志审计的主界面，防毒墙默认显示病毒日志的内容或者用户最近查看的日志内容，如图 11.1 所示。

图 11.1 日志审计主界面

日志审计主界面上各字段文字详细说明如下：

字段	说明
当前查询条件	当前查询日志的条件
更改查询条件	单击此按钮可以更改日志的查询条件

表 11.1 日志审计界面名词解释

用户可以单击【更改查询条件】按钮更改日志类型及其条件。日志类型共有以下五种：

- 病毒日志：防毒墙过滤的病毒日志
- 隔离文件：防毒墙隔离的病毒文件
- 管理日志：防毒墙管理员进行防毒墙管理操作日志
- 系统日志：防毒墙系统日志
- 网络日志：防毒墙网络安全日志
- 入侵日志：查看防毒墙入侵防御日志

11.1.1 病毒日志

单击日志审计主界面上的【更改查询条件】按钮进入查询日志条件界面，可以选择日志类型，默认为病毒日志，病毒日志为防毒墙的病毒查杀日志，如图 11.2 所示。

图 11.2 病毒日志查询界面

病毒日志查询界面各个字段说明：

字段	说明
协议	病毒通过哪种协议进行传播，有HTTP、FTP、SMTP、POP3、IMAP、MSN和全部协议
源地址，目的地址	病毒的来源和目的IP地址
按时间段	可以单击后面的日历图标选择开始时间和结束时间
病毒名	填写要查询的病毒名字
地址格式	病毒日志的显示方式，有按IP地址显示和按主机名显示两种，默认为按IP地址显示

表 11.2 病毒日志查询界面说明

提示：按主机名显示

若选择地址格式按主机名显示，则病毒日志查询界面有变动，源地址、目的地址一行为源主机、目的主机，用户可以选择内网内的主机。默认的 ALL 表示所有的主机。

查询病毒日志的操作可以按照以下步骤进行：

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. 在源地址处输入查询的来源 IP 地址

3. 在目的地址处输入查询的目的 IP 地址

4. 在按时间查询处选择查询的时间范围（后者的时间不可早于前者）

5. 在病毒名处输入病毒的名称信息

6. 单击单选按钮选择病毒日志的显示方式，有按 IP 显示和按主机名显示两种可以选择

以上内容可以不全填，如果不填的话，防毒墙默认将病毒日志的内容全部显示出来。单击【确定】按钮保存查询条件，同时在日志审计主界面会出现病毒日志的记录，如图 11.3 所示。

图 11.3 病毒日志查询结果

病毒日志查询结果各字段文字详细说明如下：

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），单击可以改变记录排序按时间升序或降序排列
协议	通过何种协议进行传播，单击可以改变记录的显示方式按照协议的顺序显示
源地址	数据包发送IP地址，单击可以使记录按照源地址IP升序或者降序的顺序排列
目的地址	数据包目的IP地址，单击可以使记录按照目的地址IP升序或者降序排列
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 11.3 病毒日志界面名词解释

单击病毒日志查询结果界面右下角的【下载日志】，病毒日志将以 XLS 格式文件下载到本地计算机，供管理员日后分析。

11.1.2 隔离文件

当防毒墙判定某些文件有危险时，会将其放入隔离区同时将该信息记录在隔离文件里。单击日志审计主界面上的【更改查询条件】按钮进入查询日志条件界面，选择日志类型为隔离文件，显示隔离文件的查询界面，防毒墙的隔离文件日志功能可按协议、源地址、目的地址和文件信息对检测到的文件进行分类记录，如图 11.4 所示。

图 11.4 隔离文件查询界面

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 和全部协议，全部协议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. 在地址格式处选择日志显示方式

填写完以上查询条件内容后，单击【确定】按钮保存查询条件，同时在日志审计主界面会出现用户查询的隔离文件记录的详细信息，如图 11.5 所示。

图 11.5 隔离文件查询结果部分界面

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
源地址	发送文件的IP地址
目的地址	接收文件的IP地址
描述	隔离文件信息的详细描述
文件	可以单击【另存】将防毒墙隔离的文件以TGZ格式下载到本地供管理员详细分析
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 11.4 隔离文件日志名词解释

单击隔离文件查询结果界面右下角的【下载日志】，隔离文件将以 XLS 格式文件下载到本地计算机，供管理员日后分析。

11.1.3 管理日志

单击日志审计主界面上的【更改查询条件】按钮进入查询日志条件界面，选择日志类型为管理日志，显示管理日志的查询界面，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 11.6 所示。

图 11.6 管理日志查询界面

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. 在按时间段处选择查询的时间范围
3. 在按操作处输入管理员对防毒墙所进行的操作
4. 在按结果处选择按成功、失败或全部结果进行查询
5. 在地址格式处选择日志显示方式

填写完以上查询条件内容后，单击【确定】按钮保存查询条件，同时在日志审计主界面会出现用户查询的管理日志记录的详细信息，如图 11.7 所示。

图 11.7 管理日志查询结果

管理日志各字段信息文字说明：

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），单击可以改变日志记录按照时间升序或者降序排列
管理员	管理员的名称
登录来源	管理员登录防毒墙进行管理时使用的IP地址
操作	防毒墙管理员进行的管理操作

表 11.5 防毒墙管理日志名词解释

单击管理日志查询结果界面右下角的【下载日志】，系统日志将以 XLS 格式文件下载到本地计算机，供管理员日后分析。

11.1.4 系统日志

单击日志审计主界面上的【更改查询条件】按钮进入查询日志条件界面，选择日志类型为系统日志，显示系统日志的查询的界面，系统日志包含任何关于瑞星防毒墙系统的操作信息，如图 11.8 所示。

图 11.8 系统日志查询界面

查询系统日志：

1. 选择系统日志的级别
2. 在按进程名处输入需要查询的进程
3. 在按操作处输入防毒墙进行的系统操作
4. 在按时间段处选择查询的时间范围

填写完以上查询条件内容后，单击【确定】按钮保存查询条件，同时在日志审计主界面会出现用户查询的系统日志记录详细信息，如图 11.9 所示。

图 11.9 系统日志查询结果

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），单击可以改变日志条目按照时间升序或者降序排序
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 11.6 防毒墙系统日志名词解释

单击系统日志查询结果界面右下角【下载日志】，系统日志将以 XLS 格式文件下载到本地计算机，供管理员日后分析。

11.1.5 网络日志

单击日志审计主界面上的【更改查询条件】按钮进入查询日志条件界面，选择日志类型为网络日志，显示网络日志的查询界面，防毒墙的网络日志功能可按协议、操作、规则名、端口、入口、出口、源地址、目的地址和时间进行分类记录，如图 11.10 所示。

图 11.10 网络日志查询界面

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 和全部协议，全部协议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类型进行查询，分为安全策略、入侵防御和全部，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规则的规则名称
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. 在地址格式处选择显示方式

填写完以上查询条件内容后，单击【确定】按钮保存查询条件，同时在日志审计主界面会出现用户查询的网络日志记录详细信息，如图 11.11 所示。

图 11.11 网络日志查询结果部分界面

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
源地址	发起网络连接的IP地址
目的地址	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 11.7 网络日志名词解释

单击网络日志查询结果界面右下角【下载日志】，网络日志将以 XLS 格式文件下载到本地计算机，供管理员日后分析。

11.1.6 入侵日志

单击日志审计主界面上的【更改查询条件】按钮进入查询日志条件界面，选择日志类型为入侵日志，显示入侵日志的查询界面，防毒墙的入侵日志功能可按协议、端口、源地址、目的地址、时间段和地址格式进行分类记录，如图 11.12 所示。

图 11.12 入侵日志查询界面

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 和全部协议，全部协议则代表包含上述三种协议
2. 在规则名处输入进行查询自定义规则的规则名称
3. 在端口处输入需要查询的端口范围
4. 在源地址处输入进行查询的来源 IP 地址
5. 在目的地址处输入进行查询的目的 IP 地址
6. 在按时间查询处选择查询的时间范围
7. 在地址格式处选择显示方式

填写完以上查询条件内容后，单击【确定】按钮保存查询条件，同时在日志审计主界面会出现用户查询的入侵日志记录详细信息。

11.2 日志统计

对已检测到的内网主机病毒事件进行分析汇总，按照主机所产生事件比例进行排序，让管理员通过日志统计界面直观的了解企业内部网络病毒威胁，快速处理出现问题的网络节点，保证企业网络的正常运行。单击日志审计主界面上的【日志统计】进入日志统计的主界面，日志统计对防毒墙记录的病毒事件进行全局的统计，如图 11.13 所示。

图 11.13 日志统计主界面

日志统计主界面各字段说明如下：

字段	说明
当前查询条件	显示当前日志统计的查询条件
【更改查询条件】	单击该按钮进入更改查询条件界面，管理员可以更改查询日志的条件
主机	发生病毒事件的内网主机的IP地址和主机名信息 ;事件所占比例表示该主机发生的病毒事件占所有主机发生的总病毒事件的百分比
事件数	显示内网主机访问网络时被防毒墙拦截的病毒总数和用户使用何种协议访问网络时被防毒墙拦截的病毒数以及占总病毒数的百分比。病毒事件用饼状图表示，并根据协议的不同用不同颜色进行区分。当主机病毒事件仅为一种协议进行传播时，不显示饼形图。

表 11.8 日志统计界面名词解释

11.2.1 更改查询条件

单击日志统计主界面的【更改查询条件】按钮，进入更改查询条件界面，如图 11.14 所示。

图 11.14 更改查询条件界面

更改查询条件界面的字段说明如下：

字段	说明
协议	内网用户访问外部网络时使用何种协议时遇到的病毒事件 ,有HTTP、FTP、SMTP、POP3、IMAP、MSN和全部协议
源地址	传输病毒的发起端
目的地址	接收病毒的最终网络节点
按时间段	可以单击后面的日历图标选择开始时间和结束时间；也可手工输入查询日期，格式为：年-月-日
病毒名	填写要查询的病毒名字
地址格式	可以选择按病毒事件的源地址或者目的地址显示

表 11.9 更改查询条件界面说明

查询病毒日志的操作可以按照以下步骤进行：

1. 在协议处选择用户使用何种协议访问外部网络时防毒墙拦截到的病毒，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. 在源地址处输入查询的来源 IP 地址
3. 在目的地址处输入查询的目的 IP 地址
4. 在按时间查询处选择查询的时间范围（后者的时间不可早于前者）
5. 在病毒名处输入病毒的名称信息
6. 单击单选按钮选择病毒日志的显示方式，有按源地址和按目的地址两种可以选择

以上内容可以不全填，如果不填的话，防毒墙默认将病毒日志的内容全部显示出来。单击【确定】按钮保存查询条件，同时在日志统计主界面会显示更改条件后的查询结果，例如更改地址格式为按目的地址显示，结果如图 11.14 所示。

图 11.14 更改查询条件的日志统计

按源地址和按目的地址两种不同的格式显示搜索结果，目的是为了让管理员通过日志统计功能快速解决内网病毒安全问题，并利用防毒墙安全策略保障企业网络安全。通过这两种方式，可以快速封堵互联网不安全的节点和定位内网问题较严重的主机。

11.2.2 查看详细的病毒事件

具体协议病毒事件的查看步骤类似，这里以 FTP 病毒事件查看为例进行说明。

单击日志统计主界面某主机的 FTP 病毒事件前的展开图标展开 FTP 病毒事件的具体信息，如图 11.15 所示。

图 11.15 FTP 病毒事件

单击图 11.15 中的【查看更多事件…】进入日志审计界面的病毒日志查询界面，可以查看当前主机 FTP 病毒事件的详细信息，如图 11.16 所示。

图 11.16 FTP 病毒事件的详细信息

关于 FTP 病毒事件详细信息的各个字段说明可参见 11.1.1 节的病毒日志查询结果部分。

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
bypass      bypass
dns        configure DNS
exit       exit shell
help       show command list
```

```
hwaddr      display hardware address of the gateway
hwcode      Show HWCODE
ipaddr      interface IP address management
netmode     display or configure network mode
network     network setting
ping        Send ICMP ECHO_REQUEST packets to network hosts
reboot      reboot machine
reportsc    Enable or disable service center
reset       reset to default setting.
route       static route configure
service     interface service management
showsn      show device ID and serial No.
shutdown    shutdwon machine
time        display of set system time
user        user administration
version     display version
wanmode     show or configue system topology
```

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]$ time ?
time
time set <YYYY-MM-DD[_hh:mm:ss]>       (year between 1970 and 2037)
time sync <ntpserver>
time zone {CST|UTC}
```

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: XXXXXXXXXXX
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
```

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) 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 工作模式

a) 查看接口工作模式

命令格式：netmode

示例：

```
[RsShell]$ netmode
broadband
```

b) 设置接口的工作模式

```
命令格式：netmode {transparent|broadband}
```

示例：设置接口工作模式为网桥模式

```
[RsShell]$ netmode transparent
```

A1.12 服务管理

c) 查看端口服务

```
命令格式：service <iface>
```

示例：

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

d) 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
```

A1.13 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
E3 192.168.100.244 255.255.255.0
E4 192.168.2.1 255.255.255.0
```

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]$ ipadrr del E2
```

A1.14 查看端口硬件地址

```
命令格式：hwaddr
```

示例：

```
[RsShell]$ hwaddr
E0 00:90:FB:11:DC:20
E1 00:90:FB:11:DC:1F
E2 00:90:FB:11:DC:1E
E3 00:90:FB:11:DC:1D
E4 00:90:FB:11:DC:1C
```

A1.15 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
0 193.168.20.0 255.255.255.0 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 193.168.20.1
```

d) 添加防毒墙默认路由

```
命令格式： route add default-gw <gateway>
```

示例：

```
[RsShell]$ route add default-gw 193.168.20.1
```

e) 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
```

f) 删除防毒墙默认路由

```
命令格式： route del default-gw
```

示例：

```
[RsShell]$ route del default-gw
```

A1.16 查看 DNS 设置

```
命令格式： dns
```

示例：

```
[RsShell]$ dns
1st=202.106.2.20
2nd=202.106.46.151
```

A1.17 设置 bypass 功能

a) 显示当前 bypass 功能状态

```
命令格式： bypass
```

示例：

```
[RsShell]$ bypass
Bypass enable 4
```

b) 设置 bypass 功能生效时间

```
命令格式： bypass enable <second>
```

示例：

```
[RsShell]$ bypass enable 5
```

c) 停用 bypass 功能

```
命令格式： bypass disable
```

示例：

```
[RsShell]$ bypass disable
```

A1.18 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
```

A1.19 查看防毒墙产品类型

```
命令格式:hwcode
```

示例：

```
[RsShell]$ hwcode
HWCODE=HW2090
```

A1.20 开启系统中心

是否开启与瑞星公司防毒墙系统中心的连接。

```
命令格式：reportsc
```

示例：

开启与瑞星公司防毒墙系统中心连接

```
[RsShell]$ reportsc enable
```

关闭与瑞星公司防毒墙系统中心连接

```
[RsShell]$ reportsc disable
```

1.21 外网口模式设置

当外网口处于禁用状态时，配置外网口接口工作模式。

```
命令格式：wanmode
```

示例

修改 E0 接口工作模式为 DHCP

```
[RsShell]$ wanmode E0 DHCP
```

1.22 防毒墙 tcp 高级选项

当防毒墙需要修改特定参数与其他网络设备协商时，使用该功能进行配置。

```
命令格式：network
```

示例 关闭 windows scaling

```
[RsShell]$ network setting disable tcp_window_scaling
```

APPENDIX 2 专业术语表

A

安全套接层（SSL）

SSL 为 Secure 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。

B

Bypass

Bypass 主要保护防止各类网络串接网关设备因意外失效（如硬件故障、电源故障、软件死锁等）而成为单点故障，避免了因网络手工切换带来的时间延误和网络运维管理困难。

D

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。

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。

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。

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

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。

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朴结构。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。

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 瑞星网络安全硬件产品质保服务说明

A3.1 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，产品即可获得病毒代码升级服务与保修服务。用户可通过登录瑞星网站查询产品的“升级服务截止日期”与“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
- 如无特殊说明和协议约定，瑞星公司提供的病毒代码升级服务期与保修服务期均为一年；
- 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。

A3.2 免费服务

A3.2.1 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。

A3.2.2 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 A3.3.2 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 A3.1 瑞星提供的免费技术咨询服务

A3.2.3 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。

瑞星公司为用户提供每天至少一次的病毒代码升级。用户可以采用网络或者本地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“A3.3.4 产品升级服务”部分。

A3.2.4 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
服务激活网址	http://reg.rising.com.cn/enterprise/hardware/hdregindex.aspx
用户产品信息查询网址	http://reg.rising.com.cn/enterprise/hardware/index.aspx

表 A3.2 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。

A3.3 有偿服务

A3.3.1 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；

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损坏相关责任。

- 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；

A3.3.2 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；

A3.3.3 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%）；

A3.3.4 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损坏相关责任。

A3.4 服务标准

A3.4.1 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；

A3.4.2 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；

A3.4.3 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

A3.4.4 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；

A3.5 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。

APPENDIX 4 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://hardware.rising.com.cn