# 防火墙实验

**【实验目的】**

(1)过实验深入理解防火墙的功能和工作原理；

(2)通以“瑞星”防火墙为例熟悉配置个人防火墙；

**【实验仪器】**

 针对“瑞星”个人防火墙在Windows 2000\2003\XP操作系统下，安装“瑞星”防火墙的计算机。

**【实验内容及步骤】**

实验步骤一：瑞星个人防火墙

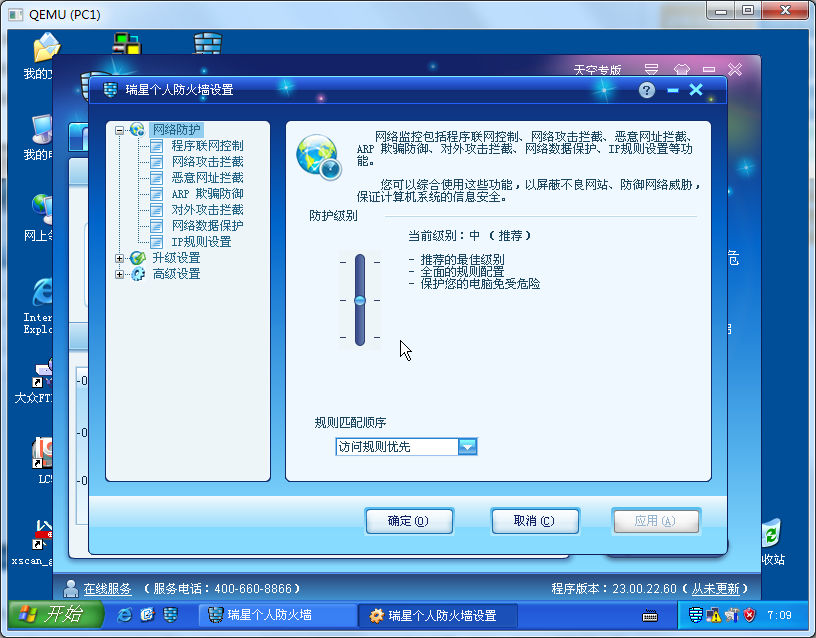
 1. 对应用程序的安全设置

 单击“瑞星”防火墙（如图7-5所示）右上方的“设置”按钮，将出现“瑞星个人防火墙设置”界面，此时可以设置应用程序访问网络的权限。

在此界面单击“添加规则”按钮，在“增加应用程序规则”对话框（如图7-6所示）中选择需要设置的程序的名称。接下来可以设置网络连接的类型和相应类型的连接可以访问的端口，以不符合设置条件时的处理方式。其中，“通过TCP协议发送消息”是指可以通过TC协议连接外网，“提供TCP协议服务”是指打开TCP监听端口提供对外服务，允许外网计算机连接此端口。

 单击“确定”后，“应用程序访问网络权限设置”界面中会出现刚刚设置的应用程序的规则条目。在“应用程序访问网络权限设置”界面中添加了对应用程序处理的规则后，也可按此规则后面的“选项”或“删除”按钮，对此规则进行修改。在“应用程序访问网络权限设置”界面中添加的应用程序，防火墙允许其和外网的连接，未添加的应用程序，则不允许。





 2. 网络防护

【防护级别】设置防护级别以便保护电脑的安全；

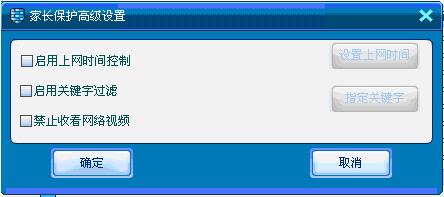
【规则匹配顺序】默认访问规则优先。

  2.1 程序联网控制：

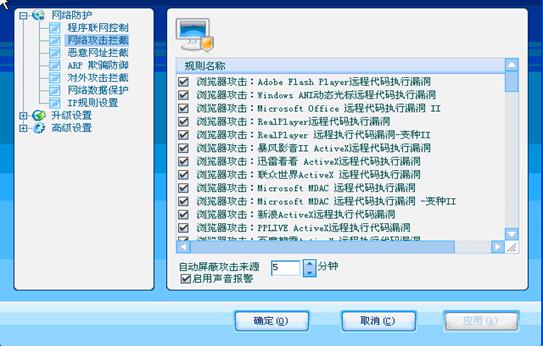


基本设置

  启用家长保护：勾选此项，防火墙将启用家长保护功能。如要关闭家长保护功能，取消勾选即可。复选框的选择，不需保存可立即生效。 只有在启用家长保护后，所有网站访问规则才能够生效。启用后，可进行设置，如图7-8所示：



 2.2 网络攻击拦截：



【自动屏蔽攻击来源】：时间自行设置；

【启用声音报警】：勾选此项，防火墙将启用此功能

 2.3 恶意网址拦截：



【已保护的程序】项显示当前受保护的程序列表；

添加：单击【添加】后，从本地上导入需保护的程序，单击确定；

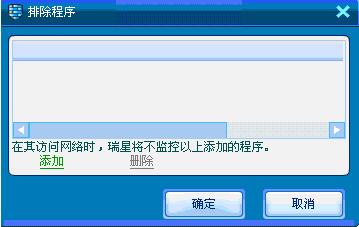
删除：选定要删除的程序，单击【删除】按钮，按【确定】删除。

搜索支持的浏览器:

相关设置：

网站黑白名单的设置同IP规则设置，见后。

排除程序，其【添加】和【删除】操作同上，如图7-11：



   代理服务器设置：点击【设置】，进入如图7-12：



勾选【启用钓鱼网页扫描功能】、【启用搜索引擎搜索结果风险分析】，进行相应设置。

ARP 欺骗防御

ARP欺骗是通过发送虚假的ARP包给局域网内的其他计算机或网关，通过冒充别人的身份来欺骗局域网中的其他的计算机，使得其他的计算机无法正常通信，或者监听被欺骗者的通信内容。瑞星个人防火墙2008版针对这个问题增加了ARP欺骗防御功能，用户通过设置ARP规则保护计算机的正常通讯，设置界面如图7-13所示：



防御方式：

【定时检查本机ARP缓存】：定时检查防火墙内的ARP缓存表和系统的ARP缓存表，将二者进行比较。默认每一分钟检查一次，用户也可以自己设置时间间隔；

【拒绝IP地址冲突攻击】：勾选此选项后，当防火墙侦测到局域网中的计算机的IP地址冲突时，会自动阻止所受的攻击并将所受攻击事件记录到日志中；

【禁止本机对外发送虚假ARP数据包】：勾选此项后，；

【发现可疑或欺骗ARP包时如何提示我】：用户可以选择【气泡通知】、【托盘动画】和【声音报警】三种方式，用户可以同时勾选这三个选项。

相关设置：

ARP 静态规则：

ARP静态规则里存储用户信任的计算机IP-MAC地址对应表（如图），如果有其他的计算机冒充该表内的计算机将被防火墙阻止，并报警提示用户，设置示图如图7-14。



 用户可以通过添加ARP静态规则来维护一个局域网内的各个计算机的IP地址和MAC地址对应表。这样就能发现某个MAC地址会冒用某个IP。具体操作如下：

单击页面中的【增加】按钮，进入【ARP静态规则】页面，如图7-15：



输入计算机名称，输入想要确定的计算机IP地址，单击【自动获取】得到该计算机的MAC地址，最后单击【确定】完成。

2.5 对外攻击拦截，点击后，出现检测到的情况如图7-16所示：

 2.6 网络数据保护设置：点击后如图7-17所示：



 1. 端口隐身：

启用端口隐身：启用该功能，勾选此项，防火墙将启用端口隐身。如要关闭该功能，取消勾选即可

【发现端口扫描时如何提示我】：用户可以选择【气泡通知】、【托盘动画】和【声音报警】三种方式，用户可以同时勾选这三个选项。

 2. MSN聊天加密：可勾选【启用MSN聊天加密】，启用加密功能。

设置完后，点击【应用】后【确定即可】。

2.7 IP规则设置



此处设置IP层的过滤规则。

需要注意的是，规则越多性能越低；不需要增加与应用相关的规则，系统在应用需要时打开端口；也不需要增加防范性规则，系统已经内置并且自动升级。

显示内容

列表中显示当前使用的IP规则，具体列出规则名称、状态、协议、对方端口、本地端口、是否报警等，规则按过滤顺序排序，打勾的项表示生效

相关操作

增加规则：

单击【增加】按钮 或 在右键菜单中选择【增加】，打开【添加IP规则】窗口

输入规则名称，并选择规则匹配成功后执行的动作

选择“规则应用于”和“如何处理触发本规则的IP包”选项，单击【下一步】按钮；设置通信的本地电脑地址与远程电脑地址，设置好后，单击【下一步】按钮；

之后进行协议、对方端口和本地端口的设置， 单击【下一步】按钮，选择匹配成功后的报警方式，分别为：

托盘动画：防火墙托盘图标变为IMG_274并且闪烁

气泡通知：通过气泡窗口通知用户，气泡窗口会自动消失

弹出窗口：通过弹出窗口通知用户

记录日志：是否记录日志

完成IP规则的添加设置。

编辑规则 ：

选中待修改的规则，规则加亮显示，在右键菜单中选择【编辑】，打开【IP规则设置】窗口

修改对应项目，基本内容与『增加』相同。单击【完成】完成修改，或单击【取消】放弃此次修改

您也可以双击对应项目打开【IP规则设置】窗口

删除规则：

选中待删除的规则，规则加亮显示，单击【删除】按钮 或 在右键菜单中选择【删除】

确认删除，选择规则时可配合【Ctrl】键与【Shift】键进行多选。

 导入规则：

单击【导入】按钮，在弹出的文件选择窗口中选中规则文件(\*.fwr)，再单击【打开】

如果列表中已有规则，导入时会询问是否删除现有规则，您可以选择【是】、【否】或【取消】

导出规则 ：

单击【导出】按钮，在弹出的保存窗口中填写文件名，再单击【保存】

如果您选择的文件已存在，导出时会询问是否覆盖

（2）可信区：点击“IP规则设置”中的可信区“设置”，如图7-19所示：



通过可信区的设置，可以把局域网和互联网区分对待。

在此处，您可以进行可信区列表和可信区服务的设置。 在可信区内指定局域网计算机的IP，默认对方计算机不在此区域。

如果您的计算机是直接连到互连网的(例如拨号上网)，就不要把IP加入可信区。

显示内容

列表中显示当前可信区中项目的名称、本地地址、对方地址

相关操作

增加可信区

单击【增加】按钮 或在右键菜单中选择【增加】，打开【可信区设置】窗口

输入名称、本地地址、对方地址，单击【确定】即可

【本地地址】为“指定地址”时，可以单击【浏览】在列表中选择一个本地地址。

编辑规则

选中待修改的规则，规则加亮显示，在右键菜单中选择【编辑】，打开【可信区设置】窗口

修改对应项目，单击【确定】完成修改，或单击【取消】放弃此次修改

您也可以双击对应项目打开【可信区设置】窗口

删除规则

选中待删除的规则，规则加亮显示，单击【删除】按钮 或 在右键菜单中选择【删除】

确认删除，您也可以选中项目按【Delete】键来删除规则。

选择可信区服务

选中相应规则，在下方勾选服务名称选项：【允许Ping入/出（回显应答）】、【允许Ping入/出（请求回显）】、【LAN下放行对方敏感端口】、【LAN下放行敏感端口】

（1）黑名单

此处为禁止与本机通讯的计算机列表，例如：攻击本机的计算机可加入此区域 ，如图7-20：



显示内容

列表中显示当前黑名单中计算机的名称、地址、来源、生效时间

打勾的项表示生效

相关操作

1.增加规则

单击【增加】按钮 或 在右键菜单中选择【增加】，打开【增加黑名单】窗口，如图7-21所示：



输入名称、地址类型、地址/地址范围，单击【保存】即可

选中待修改的规则，规则加亮显示，在右键菜单中选择【编辑】，打开【编辑黑名单】窗口

修改对应项目，单击【确定】完成修改，或单击【取消】放弃此次修改

您也可以双击对应项目打开【编辑黑名单】窗口

3.删除规则

选中待删除的规则，规则加亮显示，单击【删除】按钮 或 在右键菜单中选择【删除】

您也可以选中项目按【Delete】键来删除规则。

选择规则时可配合【Ctrl】键与【Shift】键进行多选。  
（2）白名单

此处为完全信任的计算机列表，列表中的计算机对本机有完全访问权限。例如：VPN服务器可加入此区域。

显示、操作同黑名单。

（3）端口开关

在此处您可以允许或禁止端口中的通讯，可简单开关本机与远程的端口。

显示内容

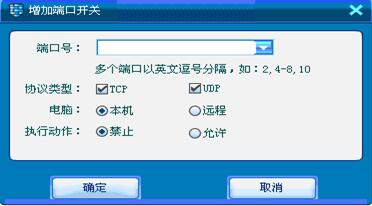
列表中显示当前端口规则中每一项的端口、动作、协议、计算机

打勾的项表示生效

相关操作

增加规则

单击【增加】按钮或在右键菜单中选择【增加】，打开【增加端口开关】窗口，如图7-22：



输入端口列表、协议类型、计算机、执行动作，单击【确定】即可

输入端口号时，多个端口以英文逗号分隔，如：2,4-8,10

编辑规则

选中待修改的规则，规则加亮显示，在右键菜单中选择【编辑】，打开【编辑端口开关】窗口

修改对应项目，单击【确定】完成修改，或单击【取消】放弃此次修改

您也可以双击对应项目打开【编辑端口开关】窗口

删除规则

选中待删除的规则，规则加亮显示，单击【删除】按钮 或 在右键菜单中选择【删除】

确认删除

您也可以选中项目按【Delete】键来删除规则。

高级设置

进入方法

打开防火墙主程序

在右上方依次选择【设置】

在左侧树形菜单中单击【选项】下的【高级设置】，如图7-23所示：



设置项目：

显示信息：可以通过勾选“显示网页信息”和“显示登录图标”来设置。

日志：可设置“日志保留时间”，勾选“记录规则修改日志”和“记录系统动作日志”

软件安全

瑞星密码：“启用瑞星密码保护”若勾选此项，用以保护软件设置不被他人修改，可设置“使用验证码”和“使用密码”两种方式。

系统启动时账户模式：“管理员账户”和“普通账户”两个选项。如图7-24所示：



“云安全”计划

通过勾选“加入瑞星‘云安全’计划”选项和填写邮箱地址选项设置，如图7-25所示：

