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；

**【实验原理】**

**1.防火墙的实现技术**

<1>包过滤技术

  包过滤是防火墙的最基本过滤技术，它对内外网之间传输的数据包按照某些特征

事先设置一系列的安全规则进行过滤或筛选。包过滤防火墙检查每一条规则直至发现数据包中的信息与某些规则能符合，则允许或拒绝这个数据包穿过防火墙进行传输。如果没有一条规则能符合，则防火墙使用默认规则，一般情况下，要求丢包。

这些规则根据数据包中的信息进行设置，包括：

●IP源地址；

●IP目标地址；

●协议类型（TCP包、UDP包和ICMP包）；

●TCP或UDP包的目的端口、源端口；

●ICMP消息类型；

●TCP选项；

●TCP包的序列号、IP校验和等；

●数据包流向：in或out；

●数据包流经的网络接口；

●数据包协议类型：TCP、UDP、ICMP、IGMP等；

●其他协议选项：ICMP ECHO、ICMP ECHO REPLY等；

●数据包流向：in或out。

  因为包过滤只需对每个数据包与相应的安全规则进行比较，实现较为简单，速度快、费用低，并且对用户透明，因而得到了广泛的应用。这种技术实现效率高，但配置复杂，易引起很多问题，对更高层协议信息无理解能力，而且不能彻底防止地址欺骗。包过滤技术防火墙原理如图7-1所示。   
  


             图7-1 包过滤防火墙原理示意图

<2>地址翻译NAT技术

    NAT即网络地址翻译技术，它能够将单位内网使用的内部IP地址翻译成合法的公网IP，使内网使用内部IP的计算机无须变动，又能够与外网连接。

    对于局域网的主机使用10.0.0.0、172.16.0.0、192.168.0.0三个内部IP网段时，当内网主机要与外部网络进行通信，就要在网关处，由NAT将内部IP地址翻译为公网IP地址，从而在外部公网上正常使用。当外部公网响应的数据包返回给NAT后，NAT再将其翻译为内部的IP地址，发给内网的主机，从而实现内网主机与外网的正常通信，解决了IPv4地址不足的问题。同时，由于外网主机只能看到数据包来自NAT翻译后的公网IP，而看不到内网主机的内部IP，所以NAT可保护及隐藏内网计算机。

    NAT有三种类型：静态NAT、动态地址NAT、网络地址端口转换NAPT。静态NAT是将内部网络中的每个主机永久的映射成外部网络中的某个合法的地址。而动态地址NAT则是在外部网络中定义了一系列的合法地址，采用动态分配的方法映射到内部网络。NAPT则是把内部地址映射到外部网络的一个IP地址的不同端口上。

<3>应用级网关

    应用级网关即代理服务器，代理服务器通常运行在两个网络之间，它为内部网的客户提供HTTP、FTP等某些特定的因特网服务。代理服务器相对于内部网的客户来说是一台服务器，对于外部网的服务器来说，它又相当于客户机。当代理服务器接收到内部网的客户对某些因特网站点的访问请求后，首先会检查该请求是否符合事先制定的安全规则，如果允许，代理服务器会将此请求发送给因特网站点，从因特网站点反馈回的响应信息再由代理服务器转发给内部网的客户。代理服务器会将内部网的客户和因特网隔离。

    对于内外网转发的数据包，代理服务器在应用层对这些数据进行安全过滤，而包过滤技术与NAT技术主要在网络层和传输层进行过滤。由于代理服务器在应用层对不同的应用服务进行过滤，所以可以对常用的高层协议做更细的控制。

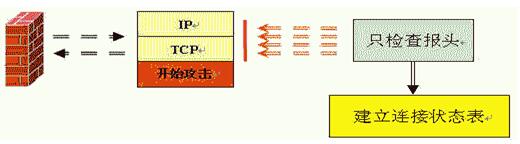
    由于安全级网关不允许用户直接访问网络，因而使效率降低，而且安全级网关需要对每一个特定的因特网服务安装相应的代理服务软件，内部网的客户要安装此软件的客户端软件，此外，并非所有的因特网应用服务都可以使用代理服务器。应用级网关技术防火墙原理如图7-2所示。  


                图7-2 应用级网关防火墙原理示意图

<4>状态检测技术

    状态检测防火墙不仅仅像包过滤防火墙仅考查数据包的IP地址等几个孤立的信息，而是增加了对数据包连接状态变化的额外考虑。它在防火墙的核心部分建立数据的连接状态表，将在内外网间传输的数据包以会话角度进行检测，利用状态表跟踪每一个会话状态。

    例如，某个内网主机访问外网的连接请求，防火墙会在连接状态表中加以标注，当此连接请求的外网响应数据包返回时，防火墙会将数据包的各层信息和连接状态表中记录的从内网到外网每天信息相匹配，如果从外网进入内网的这个数据包和连接状态表中的某个记录在各层状态信息一一对应，防火墙则判断此数据包是外网正常返回的响应数据包，会允许这个数据包通过防火墙进入内网。按照这个原则，防火墙将允许从外部响应此请求的数据包以及随后两台主机间传输的数据包通过，直到连接中断，而对由外部发起的企图连接内部主机的数据包全部丢弃，因此状态检测防火墙提供了完整的对传输层的控制能力。

    状态检测防火墙对每一个会话的记录、分析工作可能会造成网络连接的迟滞，当存在大量安全规则时尤为明显，采用硬件实现方式可有效改善这方面的缺陷。状态检测防火墙原理如图7-3所示。  
  
  
                  图7-3 状态检测防火墙示意图

**2.防火墙的网络部署**

  防火墙一般部署在内外网的网络边界，对进出内网的数据包进行规则匹配和过滤。硬件防火墙至少有两个网络接口，分别连接内外网。此外，硬件防火墙一般都支持网络接口的扩展，可以支持对其他网络的安全防护。

  第三个网络接口所连接的网络称为DMZ区域。DMZ可以理解为一个不同于外网或内网的特殊网络区域，一般放置一些不含机密信息的公用服务器，比如Web等。这样来自外网的访问者可以访问DMZ中的服务，但不可能接触到存放在内网中的机密或未公开信息等，即使DMZ中服务器受到攻击或破坏，也不会对内网中的机密信息造成影响。防火墙的网络部署如图7-4所示。  
  


             图7-4 防火墙的网络部署

当规划一个拥有DMZ的网络时，可以确定以下6条基本访问控制策略：

(1)内网可以访问外网

(2)内网可以访问DMZ

(3)外网不能访问内网

(4)外网可以访问DMZ

(5)DMZ不能访问内网

(6)DMZ不能访问外网

  当然，在部署防火墙时也可以根据各机构网络的具体情况而灵活部署，主要目的在于使用防火墙的规则限制和过滤手段，对防火墙各网络接口所连接的网络进行隔离和限制，保证各网络之间数据传输的安全。

**3.防火墙的分类**

防火墙分为网络层防火墙和应用层防火墙，这两种类型的防火墙可重叠。

  网络层防火墙可视为一种IP封包过滤器，运作在底层的TCP/IP协议栈上，我们可以以枚举的方式，只允许符合特定规则的封包通过，其余的一概禁止穿越防火墙，这些规则通常可以经由管理员定义或修改，不过某些防火墙设备只能套用内置的规则。我们也能以另一种较宽松的角度来制定防火墙规则，只要封包不符合任何一项“否定规则”就予以放行。较新的防火墙能利用封包的多样属性来进行过滤，例如：源IP地址、源端口号、目的IP地址、目的端口号、服务类型、通信协议、TTL值、来源的网络或网段等属性，网络层防火墙的典型代表是天融信防火墙。

  应用层防火墙是在TCP/IP堆栈的“应用层”上运作，应用层防火墙可以拦截进出某应用程序的所有封包，并且封锁其他的封包。理论上，这一类防火墙可以完全阻止外部的数据流进到受保护的机器里。天网防火墙是应用层防火墙的代表。

硬件防火墙介绍

网络卫士防火墙有以下三种工作模式：路由模式、透明模式以及混合模式。在透明模式下，防火墙的所有接口均作为交换接口工作。路由模式下，防火墙类似于一台路由器转发数据包，将接收到的数据包的目标MAC地址替换为相应接口的MAC地址，然后转发。该模式适用于防火墙的每个区域都不在同一个网段的情况，某些区域工作在透明模式下，其余区域工作在路由模式下。

**4.防火墙不能防范的安全威胁**

(1)不能防范内网之间的恶意攻击;

(2)不能防范绕过防火墙在非法内外联通道上进行的攻击;

(3)不能防范病毒和内部驱动的木马;

(4)不能防范针对防火墙开放端口的攻击;

**【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。



                 图7-5 瑞星个人防火墙的界面

                   图7-6 瑞星个人防火墙设置界面

**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：



                 图7-7 程序联网控制示图

**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：

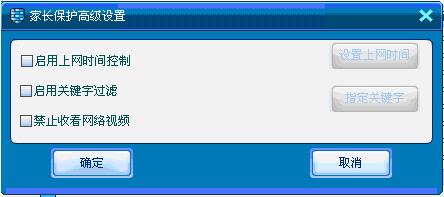


               图7-8 家长保护高级设置示图

 2.2 网络攻击拦截：

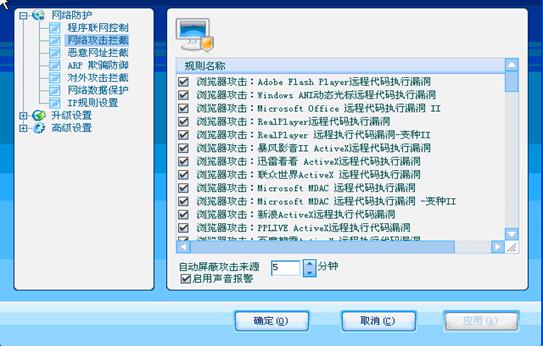


                图7-9  网络攻击拦截设置示图

【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：



                 图7-10 恶意网址拦截设置示图

【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：

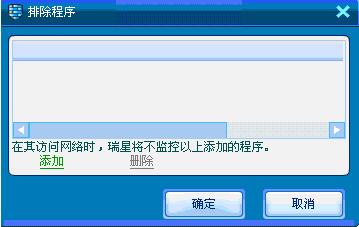


          图7-11 排除程序设置示图

代理服务器设置：点击【设置】，进入如图7-12：



         图7-12  代理服务器设置示图

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。

1. 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：



               图7-13 ARP欺骗防御示图

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。



          图7-14 ARP 静态规则设置示图

 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：



          图7-15 ARP 静态规则增加示图

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：

            图7-16  对外攻击拦截情况示图

 2.6 网络数据保护设置：点击后如图7-17所示：



                图7-17网络数据保护设置示图

 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



                  图7-18 IP规则设置示图

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http://192.168.82.245:8082/virexp/userfiles/image/CNSL/n7n19.jpg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：



  图7-19 可信区设置示图

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：



                 图7-20 黑名单设置示图

**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：



        图7-21 增加黑名单示图

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：

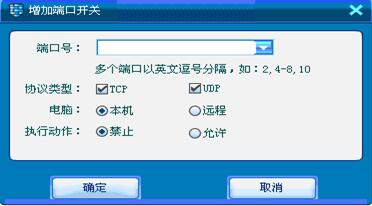


          图7-22增加端口开关示图

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：



                    图7-23高级设置示图

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：



              图7-24 软件安全设置示图

**“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：

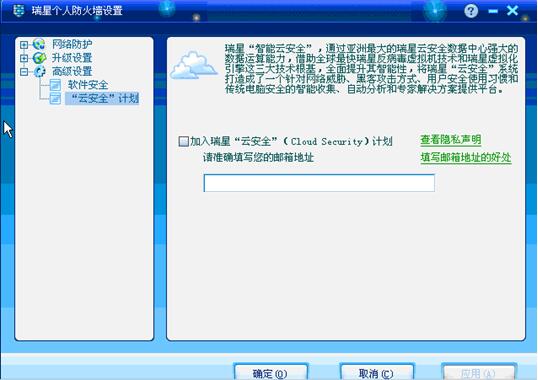


                   图7-25“云安全”计划示图

【实验报告】

  (1)运行瑞星防火墙设置向导，根据向导进行基本设置；

  (2)使用IP规则配置，可对主机中每一个发送和传送的数据包进行控制；ping局域网内的机器，观察能否收到reply；

  (3)修改IP规则配置，将“允许自己用ping命令探测其他机器”改为禁止并保存；

  (4)再次ping局域网内同一台机器，观察reply。