**卡巴斯基防火墙软件的设置技巧**

对“应用程序”的设置：

　　对于应用程序，我们知道他们都是以“.exe”为后缀名的，也就是可执行文件，所有程序的运行，包括病毒，都要以可执行文件来执行任务。“反黑客”里的“应用程序”项就是用来监控应用程序的联网状态的，由用户自己选择“允许”或“阻止”来控制是否联网。我们可以通过此设置来监控所有要联网的应用程序，并且“允许”、“阻止”。

　　一般你将“反黑客”设置成“学习(训练)模式”时，任何未设定规则而要联网的应用程序都会弹出窗口询问用户。我们也可以自主的进行设置。

　　进入“卡巴KIS主界面——设置——反黑客——点击第一个‘设置’ ”，便进入设置窗口，然后选择“应用程序规则”。如果你想添加规则，选择“添加”，编辑规则选择“编辑”，删除规则选择“删除”，同时还可以“导入”和“导出”数据库(没用过)。

　　当你想添加时，选择“添加后”，会有一个“浏览”和“应用程序”选项，“应用程序”选项里都是已经在运行的应用程序，“浏览”需要自己寻找想添加规则的应用程序。选择好之后，进入编辑界面，再点击“添加”，出现编辑窗口。规则名称最好填应用程序的名称。“远程IP地址”的意思是“是否允许程序访问此远程IP地址”，比如QQ发出后，它要连接QQ服务器的IP;“远程端口”的意思是“是否允许程序通过某IP(非自己)的某端口进行访问”，比如QQ发出后，它要连接QQ服务器的IP的某端口;“本地端口”的意思是“是否允许程序通过自己的IP的某端口访问”;“时间范围”的意思是“允许或阻止此程序在这段时间进行网络访问”。附加操作大家都知道是什么意思，就不介绍了。设完了吗?没有!!你还需要在“规则描述”里进行设置，选择“允许或阻止”，“出入网”，“TCP连接或UDP数据包”，“端口、IP和时间”等设置。

　　设置完之后，你可以随时在“模版”里进行规则的“允许或阻止”等设定，不需要重新进入修改。

　　对“包过滤规则”的设置：

　　“包过滤”是什么?就是通过防火墙的设置，监测包的特征来“放行或阻止”的，“允许、阻止或限制”每个IP的数据包的传送和连接数，阻挡攻击，禁止访问某些站点等。这不就是“防火墙”的最基本的特性了么?对!有了“包过滤”，就勉强算是“防火墙”了。

　　在设置上，和应用程序实际上差不多，只不过多了一个“本地IP地址”而已。现在，我要介绍一下怎么设置“IP地址”。和“应用程序规则”一样，进入“远程或本地IP地址”后都有很多选择，“电脑IP地址(也就是单独设置某一地址)”、“IP地址范围”和“子网地址”。“子网地址”应用的不多，本人也不是很懂，就不介绍了。“本地IP地址”的设置，输入自己局域网内的IP就行了(不包括自己)，“IP地址范围”也是输入局域网内允许的范围;这是属于局域网内部的连接。“远程IP地址”应用不多，我就不介绍了。

　　对于包过滤，用卡巴自带的规则一般就够了，不需要添加新的规则。

　　对“区域”的设置：

　　“区域”里都是已存在和连接的网络，在这里可以添加新的网络连接的信任机制。默认的一般都有一个“Internet”，设置为“Internet”。局域网的话就会有另一个连接，最好设置为“本地网络”。隐秘模式便会隐蔽你的IP地址，保护安全。

　　“Internet”，“本地网络”和“可信”的区别在于：

　　Internet：阻止文件和打印机共享，阻止错误报告，应用应用程序规则和包过滤规则;(应用在公用网络)

　　本地网络：允许文件和打印机共享，允许错误报告，应用应用程序规则和包过滤规则;(应用在有网关的网络，局域网)

　　可信：允许文件和打印机共享，允许错误报告，不应用应用程序规则和包过滤规则。(允许任何连接)

　　一般自己不用设置，在连接了新网络之后便会自动提示你，让你进行选择(默认是Internet)。

　　“附加”里基本不用设置，用推荐项最好。

　　侵入探测系统：

　　这个为默认开启，也是肯定要开启的，根据其他人的观点，在“设置”里可以把“阻止攻击电脑”那个时间限制的勾去掉，并不会影响入侵的探测和阻止。时间限制只是用来封锁你的网络，使攻击者(黑客)不能连接你的电脑，没有太大的用处。默认的60分钟太长，意味着你在受到攻击后一个小时都不能上网。不放心的话，可以设为2分钟。

总之，卡巴的“反黑客”个人用户(不总是受到攻击)也就够用了，黑客一般不会无聊到攻击个人电脑的地步。如果不放心的话，把“反黑客”关掉，安装一个你信得过的防火墙。

想知道更多的消息，请关注拓飞数据恢复。