卓冠防火墙管理员使用手册

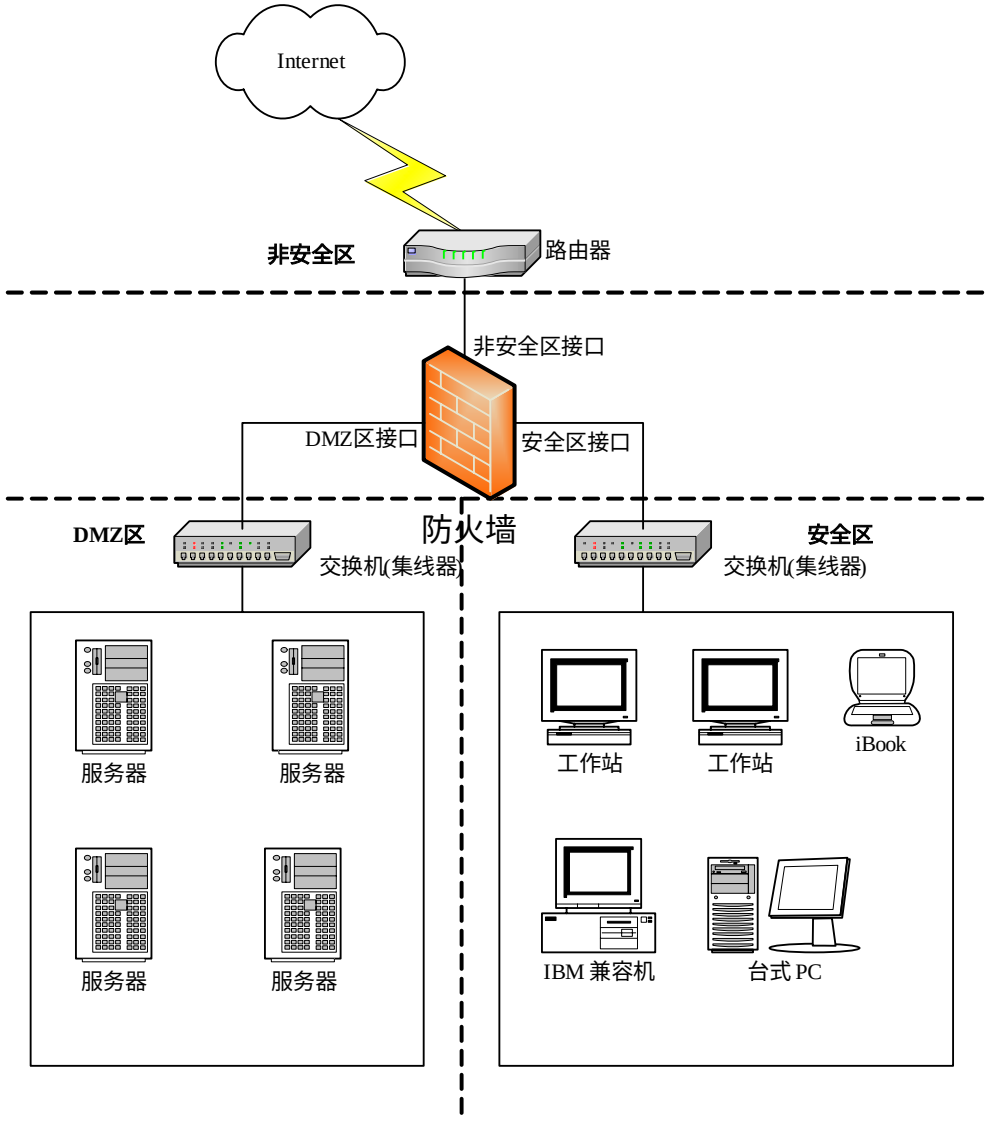
NAXGATE 3.0

2005.12

卓冠防火墙管理员使用手册

一、 产品基本组成

卓冠防火墙由以下部分组成：防火墙机器、用户手册、管理软件安装光盘组成。卓冠防火墙定位于能为用户提供高级别安全防护的状态包过滤防火墙，其安全性能达到国家颁发的包过滤防火墙技术要求(GB/T 18019-1999)。通过合理配置、使用卓冠防火墙，可以在企业内网与因特网（或其他非信任网络）之间架设一道安全屏障，它既能保证内网用户顺利访问因特网，又能保护内网的计算机不被外部黑客非法访问或破坏。



二、 防火墙术语

1. 卓冠防火墙（NaXGate 3.0）

如无特殊说明，本报告中“ 卓冠防火墙 ”特指“ NaXGate 防火墙 ”。

2. 主机（host）

存在于网络中的任何一台计算机，它能够运行基本的网络协议，在本报告中，主机也指提供某种服务的服务器，主机可能是可信的，也可能是不可信的、在防火墙外、但与防火墙相互作用的计算机，它不具有影响防火墙安全策略执行的特权。

1 内部网（internal）

存在于防火墙后面，受防火墙保护的网络，一般指企业内部私有局域网

2 外部网（external）

被防火墙认为不安全的网络，一般指连接的 Internet 网络

5 非军事化区（DMZ）

亦称中立区（Demilitarized Zone），提供对外服务的区域，它与内部网络从物理上面是分离的，避免了入侵者使用 Ethernet sniffer 偷窃内部网络秘密的危险。管理员可以定义安全策略来阻止外部到内部网络的连接请求，但允许外部连接到公共服务器上，这些公共服务器的集合称为非军事化区（DMZ）或中立区，停火区。

6 防火墙管理员（authorized administrator）

授权管理防火墙的人员，也称为防火墙系统管理员。管理员可以配置防火墙的安全规则，以控制流经防火墙的信息。允许防火墙管理员远程配置防火墙，其安全性由防火墙系统提供。

7 授权管理主机（administrator host）

网络中的一台授权主机，防火墙管理员通过该主机配置防火墙。管理主机可以属于内部网络，也可以属于 DMZ 区网络，还可以属于外部网络。管理主机中安装有瑞星防火墙远程管理程序。

8 包过滤（Packet Filtering）

对进入防火墙和从防火墙出去的 IP 包进行分析，并根据一定的规则在网络层控制这些 IP 包的行为，行为包括：允许/拒绝。

9 代理服务（Proxy Service）

代理是只允许单个主机或一小部分主机提供 Internet 访问服务，而不允许所有的主机都提供此服务，具有直接访问 Internet 能力的主机作为不能直接访问 Internet 的主机的代理，使得它们也能够具有访问 Internet 能力。

10 用户（user）

在防火墙外，但与防火墙相互作用的人，他不具有影响防火墙安全策略执行的特权。

11 授权组管理员（authorized group administrator）

这里指用户的组管理员，他只具有管理本组用户的职能。

12 可信主机（trusted host）

任何具有旁路或绕过防火墙安全策略权限的授权计算机。

三、 产品的缺省配置和安全策略

卓冠防火墙的网口出厂配置如下表所示：

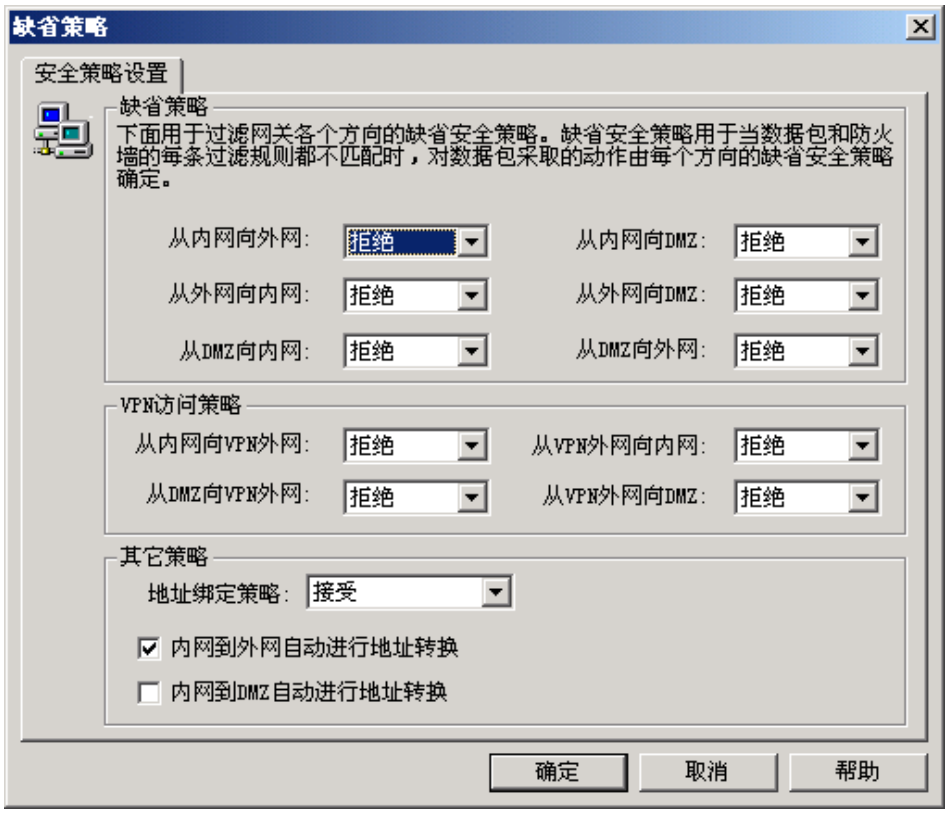
端口类型	IP 地址	子网掩码
内网口	192.168.10.1	255.255.255.0
外网口	192.168.20.1	255.255.255.0
DMZ 口	192.168.30.1	255.255.255.0

配置管理员的用户名出厂设置为“Admin”（区分大小写），出厂密码为”111111”。

日志管理员的用户名出厂设置为“Audit”（区分大小写），出厂密码为”111111”。

串口配置的出厂密码为”111111”。

卓冠防火墙所有的策略规则的出厂配置为空,缺省的安全策略为拒绝。



四、 功能列表

- 精心设计的协议状态检测引擎。
- 支持网络监控、入侵检测互动响应。
- 正向地址转换和反向地址映射。
- 流量统计和控制功能。
- 基于时间段的访问控制策略。
- 基于用户的一次性口令客户端强身份验证。
- 可简单的检测一些碎片攻击、并提供了实时报警功能。
- IP 地址和 MAC 地址绑定,并支持 IP 和 MAC 地址的扫描绑定。
- 可直接基于 MAC 地址进行数据包过滤。
- 完善的防火墙日志及状态监控。
- 支持路由模式和透明网桥模式。
- 强大的日志、报警、邮件、SNMP Trap 等响应方式。
- 灵活方便的第三方互动响应协议，方便第三方产品的集成。
- 全新的防火墙配置管理方式，支持面向对象的集中配置管理。
- 文件过滤策略，可对通过 HTTP 和 FTP 下载的文件进行文件扩展名的过滤。
- 流量统计和控制功能，有效控制源地址主机上行、下行带宽。

- 支持黑白名单过滤功能,可在线升级系统黑名单库。
- 支持多网段静态路由。

五、 产品规格

符合IEEE802.3Ethernet以及IEEE802.3u Fast Ethernet标准。
支持TCP/IP、ICMP、NAT、静态路由等协议。
端口支持自动协商功能，自动调整传输方式和传输速度。
提供状态指示灯。
工作环境：温度：0-40℃
高度：0-4000m
相对湿度：10-90%, 不结露

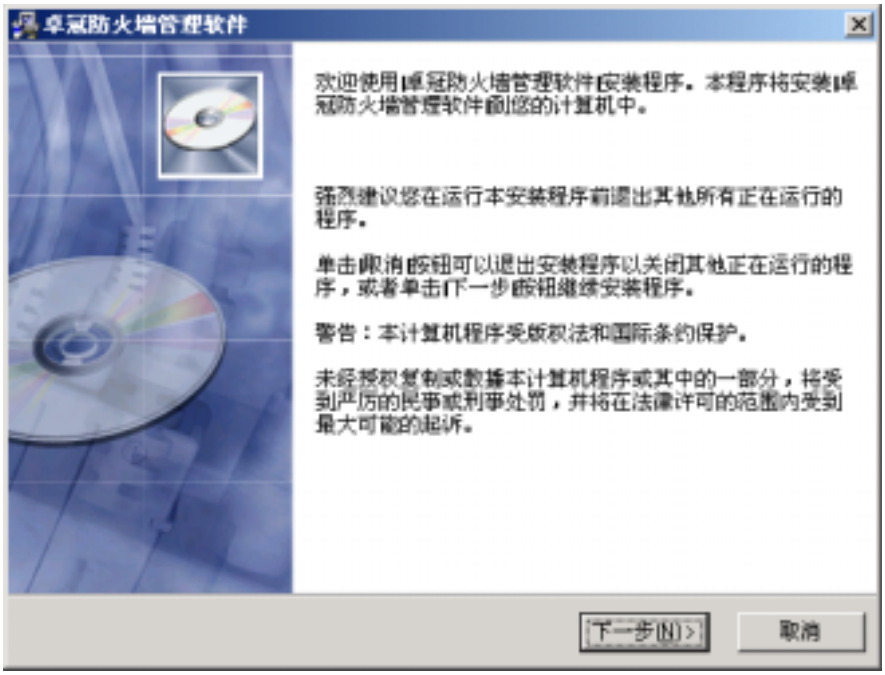
六、 客户端安装与卸载

6.1 软件运行环境与系统需求

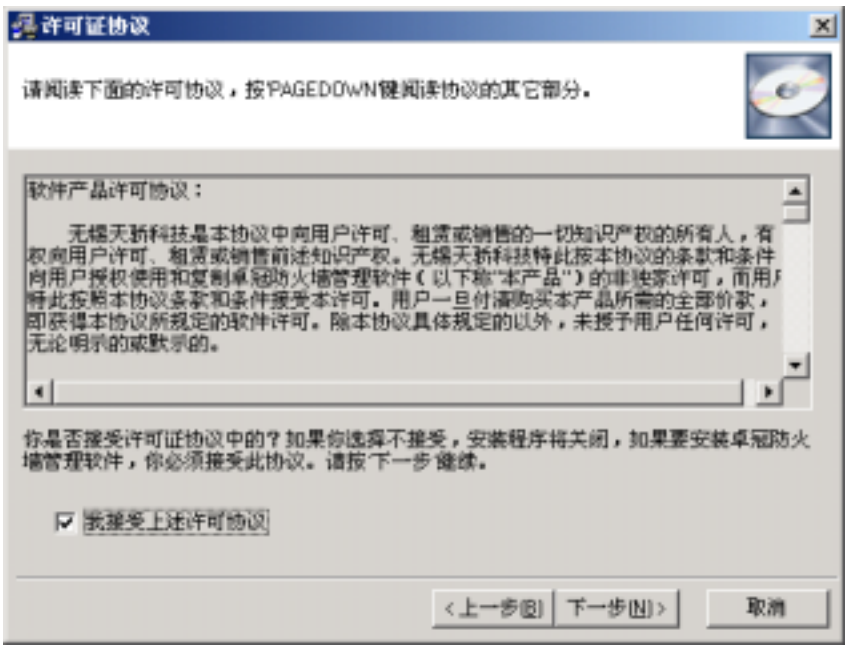
卓冠防火墙客户端管理系统运行于 Windows NT 4.0(SP6) 和 Windows 2000 平台上。256M 内存（推荐 512M 内存）,PII 600 CPU,100M 硬盘空间。至少 800x600 的显示分辨率。

6.2 安装软件

- **第一步**：启动计算机并进入 Windows（95/98/Me/NT/2000/XP/2003）系统；
- **第二步**：从光盘安装：将卓冠防火墙客户端管理系统安装光盘放入光驱，浏览光盘，运行【光盘卓冠防火墙客户端】目录下的 setup.exe 程序（或浏览 HTTP：//www.naxgate.com 下载最新卓冠防火墙客户端管理系统安装文件 setup.exe），然后在弹出的安装界面中选择【下一步】。



- **第三步**：阅读【最终用户许可协议】，选择【我接受】，按【下一步】继续；

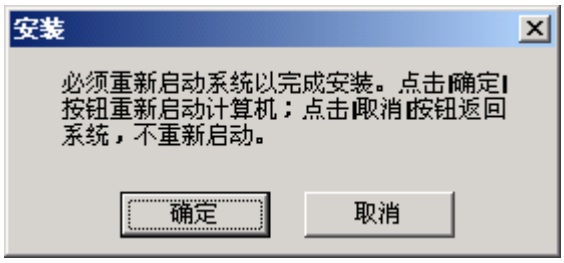


- **第四步**：在【安装信息】窗口中显示了安装路径名称的信息，如果您需要更改安装路径，请点击浏览按钮，选择相应的路径，点击【下一步】继续安装；

- **第五步**：在【选择程序组】窗口中输入您个性化的程序组名称或使用缺省的名称，确认后，按【下一步】开始复制文件；

- **第六步：**在文件复制过程中，程序会询问用户是否在桌面上建立快捷方式。文件复制完成后，最后选择【完成】结束安装。

- **第七步：**安装结束后，需要重启电脑，才能正常使用本软件。点击确定后，电脑重启。



6.3 卸载软件

卸载卓冠防火墙管理软件有二种方法：

- 方法一：在 Windows 画面中，选择【开始】/【程序】/【卓冠防火墙】/【卸载卓冠防火墙管理软件】，随即开始卸载。
- 方法二：在 Windows 画面中，选择【开始】/【设置】/【控制面板】/【添加/删除程序】/【卓冠防火墙管理软件】/【更改/删除】，随即开始卸载卓冠防火墙管理软件。稍后会显示【卓冠防火墙管理软件】窗口，有三个选项，分别是：Automatic（自动）、Custom（定制）、Repair（修复）、请选择 automatic【完成】结束卸载；如果卸载中发生异常，则还会显示【详细情况】按钮，单击【详细情况】按钮可查看有关发生异常的信息。

七、 产品的安装过程，启动和设置

- 给防火墙加电,启动防火墙内部的安全操作系统和加载相应的功能模块,；
- 然后进行串口配置，对防火墙的各网口地址和路由进行配置；
- 然后通过配置管理界面对防火墙的对象和规则进行配置；
- 再通过日志和状态监控界面查看和分析防火墙的日志信息。

下面分别进行说明。

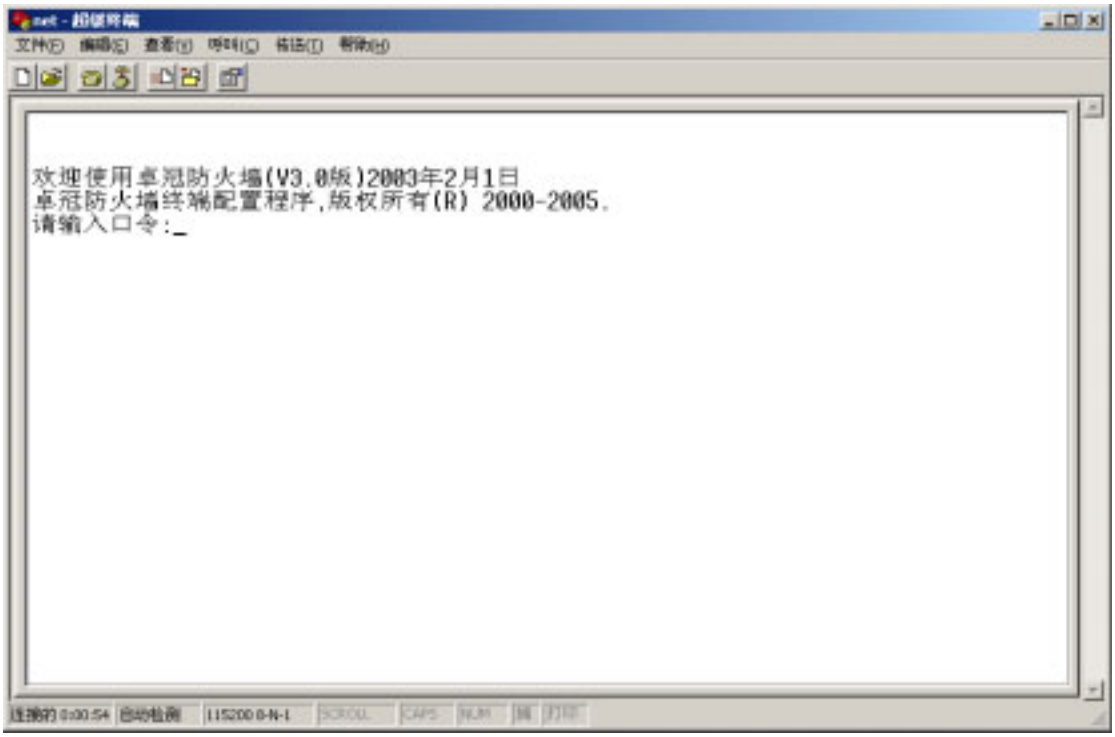
7.1 防火墙启动

给防火墙接上电源，打开防火墙的电源开关。对防火墙进行加电引导。大约 20 秒后，防火墙启动完毕，可以对其进行串口配置了。

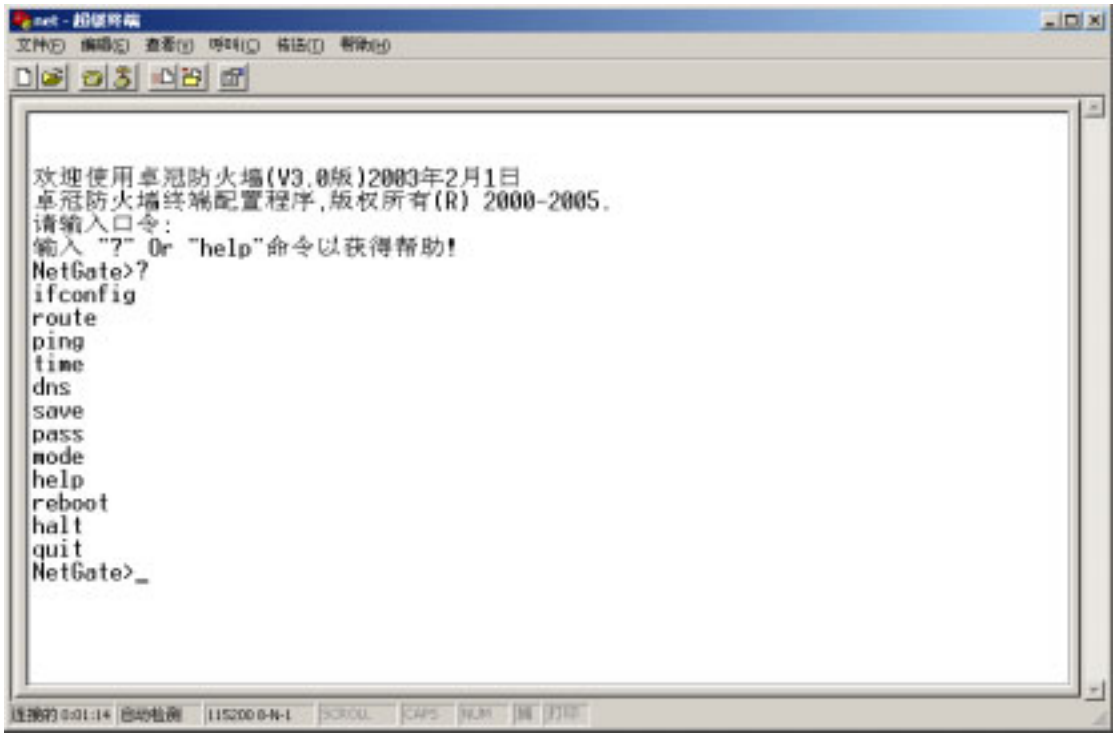
7.2 串口配置

串口配置约定：内网口的接口名称为eth0，外网口的接口名称为eth1，DMZ口的接口名称为eth2。每个接口可以配置1个或1个以上的地址。如果要在一个接口上配置多个地址，可以通过对接口的别名进行地址配置的方式来实现。如内网口的接口别名地址为
eth0:0，eth0:1，eth0:2，eth0:3等。

串口配置为管理主机通过 RS232 与防火墙的 CONSOLE 接口通过串口线缆相连接进行的；管理主机上运行任何终端仿真软件，如 WINDOWS 的 HyperTerminal 等，终端软件要求支持主要的终端类型，如 VT100，ANSI 等； 终端软件的通信参数为：DTE，115200-N-8-1。如下为一终端管理界面：



输入口令,直接进行防火墙网口地址配置,路由配置和 DNS 配置。



步骤：

① 选择一台有仿真终端程序的机器（例如 HyperTerminal 或 Xterm，前者普通的 95/98/NT/2000 下就有），用随机带的串口线将它的串口和防火墙的 console 口连接，串口参数为：波特率 115200，数据位=8，无奇偶校验，1 位停止位。

② 连接上以后，终端上将出现登录提示（在有的时候可能要先敲几下回车键才出现提示）。

输入回车，输入口令 111111 这是命令行超级用户的缺省口令，以后可以修改这个口令。

③ 将内网网线插上防火墙内网网卡接口、外网网线插上防火墙外网网卡接口，DMZ 区网线插上防火墙 DMZ 网卡接口。

④ 设置防火墙的 IP 地址。首先输入 ifconfig，则显示出防火墙当前的 IP 地址配置，根据实际环境给防火墙配置合适的 IP 地址。

规定：eth0　内网网卡
　　eth1　外网网卡
　　eth2　DMZ 网卡

例：ifconfig eth0 192.168.10.1　　255.255.255.0
例：ifconfig eth1 192.168.20.1　　255.255.255.0
例：ifconfig eth2 192.168.30.1　　255.255.255.0

⑤ 设置防火墙的路由模式/网桥模式

mode [Bridge/Route]
例：mode bridge
例：mode route

⑥ 配置（增加、删除）防火墙上的缺省路由

route add/del default ip

例：route add default 192.168.20.254

例：route del default 192.168.20.254

⑦ 配置（增加、删除）防火墙上的路由表

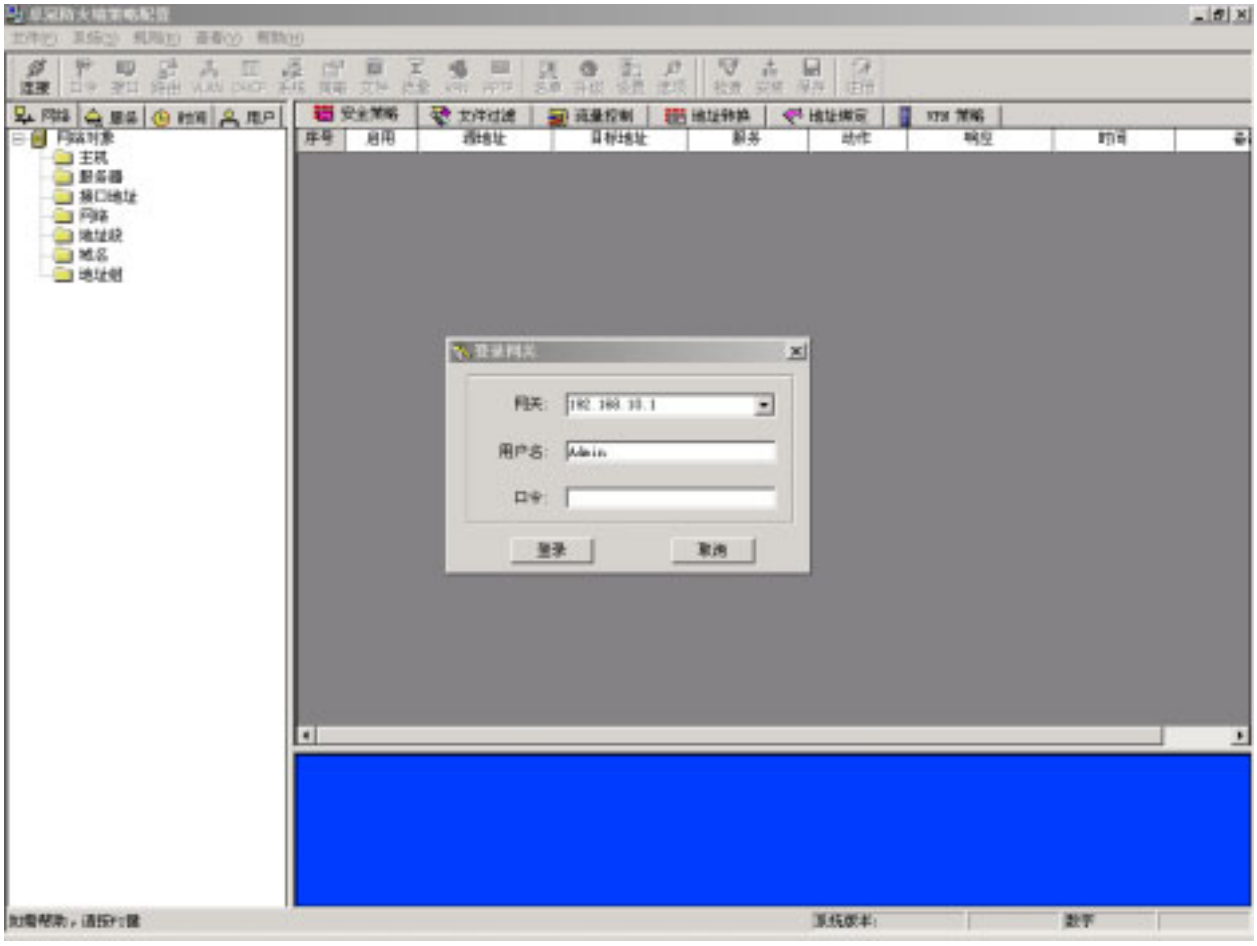
route add/del ip mask gateway

例：route add 192.168.1.0 255.255.255.0 192.168.0.254

例：route del 192.168.1.0 255.255.255.0 192.168.0.254

⑧ 经过以上的配置后，已经可以使用 GUI 管理器对防火墙进行配置了。但是以上的配置现在只是在内存中，并没有保存到配置文件中，此时如果马上关机然后开机，则以上的配置就会丢失。可以在命令行中输入 save，将配置保存到配置文件中。

当防火墙的地址和路由信息配置完成后，就可以采用图形管理界面进行防火墙的策略配置了。双击桌面“ 卓冠防火墙策略管理 ”快捷方式，出现如下界面，在网关处填写上面定义的 eth0 防火墙内网地址，（产品出厂缺省防火墙内网地址是：192.168.10.1） ，用户名 Admin,缺省口令是“ 111111 ”,点击“ 登陆 ”按钮，即进入策略管理界面。



7.3 对象、规则和属性配置

7.3.1 对象管理

卓冠防火墙采用面向对象的策略配置管理思路。卓冠防火墙的管理是基于对象的，所有的规则都是由对象和属性组成的。因此在进行规则配置之前，必须先定义出适当的对象。例如，为了限制某台机器的访问，必须先定义一个包括这台机器的对象。对象和物理的机器不是一一对应的，可能有某个对象包含多台物理机器，

而某台物理机器可能同时属于多个对象，还有一些对象不包括任何的物理机器，只是逻辑上的概念。对象的定义主要是为配置防火墙服务的。目前卓冠防火墙主要有五类对象：网络对象、服务对象、时间对象、用户对象和文件扩展名对象。下面对每一类对象管理进行详细说明。

地址对象:

名字	意义
主机	表示网络内某台电脑的主机名,可以用 IP 地址和 MAC 地址表示。
服务器	表示内网或 DMZ 区域内的 WWW,FTP 或邮件服务主机
接口地址	表示防火墙网卡地址,接口地址主要是进行地址转换时用的。
子网	表示网络内某子网定义。例:192.168.1.0/24
地址段	表示一段连续的 IP 地址。例:192.168.1.100-192.168.1.150
域名	Internet 域名。
地址组	定义主机、服务器、接口地址、子网、地址段、域名的组合

服务对象：

名字	意义
TCP 服务端口定义	定义 TCP 服务端口。
UDP 服务端口定义	定义 UDP 服务端口
ICMP 服务端口定义	定义 ICMP 服务端口
Other 服务定义	定义其它的一些 IP 协议
服务组对象	定义 TCP 服务、UDP 服务、ICMP 服务、Other 服务任意组合

时间对象：

名字	意义
时间对象	定义时间属性，时间调度

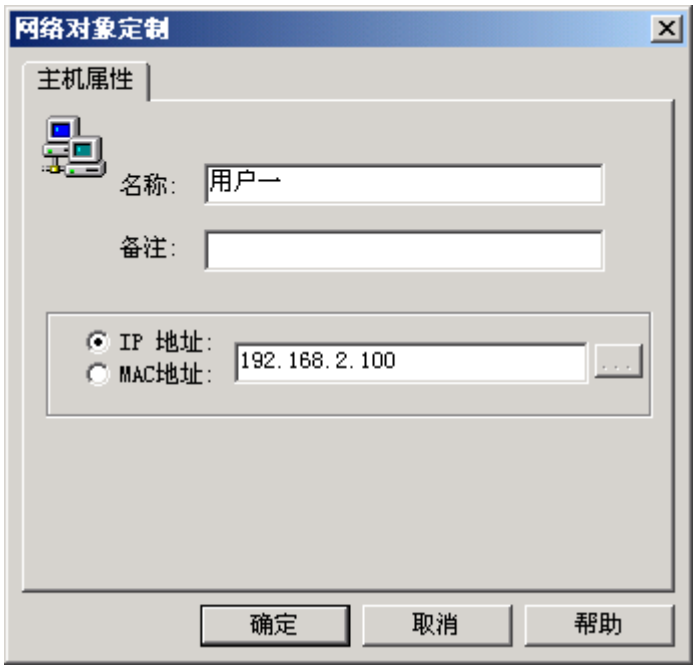
用户对象

名字	意义
互动用户	定义和其它第三方产品的的互动用户
普通用户	系统在实现基于用户的强身份验证和一次性口令客户端验证时,用户可自定义普通用户。
用户组	定义普通用户组

文件扩展名对象

名字	意义
文件扩展名类别	定义过滤文件类别及相应的扩展名格式

定义内网的主机名及其 IP 地址对象



定义内部服务器 ip 地址对象。

对防止 DDOS 攻击的相关参数做了定义：TCP Syn Flood 阀值、UDP Dos 阀值、ICMP Dos 阀值,目前这些项是灰的，在以后的版本中将实现。

定义虚拟 IP 地址转换对象

一般用定义外网网卡地址对象，作为策略的源或目的,用于地址转换

定义子网对象

子网表示一段连续的 IP 地址。可以作为策略的源或目的，

定义段对象

地址段表示一段连续的 IP 地址。可以作为策略的源或目的，

如果要表示某个区域上的所有机器，则可以用以下方式说明：某个区域（如 Intranet）上的子网 0.0.0.0-255.255.255.255。

定义 internet 域名对象

定义主机、服务器、虚拟 IP 地址、子网、网络地址段、地址域名。任意组合对象组

定义 TCP 通信协议对象，如果企业源端口固定，则需要定义源端口

定义 UDP 通信协议对象，如果企业源端口固定，则需要定义源端口

定义 ICMP 通信协议对象

类型代码		
0	ICMP_ECHOREPLY	Echo Reply
3	ICMP_DEST_UNREACH	Destination Unreachable
4	ICMP_SOURCE_QUENCH	Source Quench
5	ICMP_REDIRECT	Redirect (change route)
8	ICMP_ECHO	Echo Request
11	ICMP_TIME_EXCEEDED	Time Exceeded
12	ICMP_PARAMETERPROB	Parameter Problem
13	ICMP_TIMESTAMP	Timestamp Request
14	ICMP_TIMESTAMPREPLY	Timestamp Reply
15	ICMP_INFO_REQUEST	Information Request
16	ICMP_INFO_REPLY	Information Reply
17	ICMP_ADDRESS	Address Mask Request
18	ICMP_ADDRESSREPLY	Address Mask Reply
18	NR_ICMP_TYPES	

Codes for UNREACH. 类型 3 代码定义

类型代码	类型名称	
0	ICMP_NET_UNREACH	Network Unreachable
1	ICMP_HOST_UNREACH	Host Unreachable
2	ICMP_PROT_UNREACH	Protocol Unreachable
3	ICMP_PORT_UNREACH	Port Unreachable
4	ICMP_FRAG_NEEDED	Fragmentation Needed/DF set
5	ICMP_SR_FAILED	Source Route failed

6	ICMP_NET_UNKNOWN	
7	ICMP_HOST_UNKNOWN	
8	ICMP_HOST_ISOLATED	
9	ICMP_NET_ANO	
10	ICMP_HOST_ANO	
11	ICMP_NET_UNR_TOS	
12	ICMP_HOST_UNR_TOS	
13	ICMP_PKT_FILTERED	Packet filtered
14	ICMP_PREC_VIOLATION	Precedence violation
15	ICMP_PREC_CUTOFF	Precedence cut off
15	NR_ICMP_UNREACH	instead of hardcoding immediate value

Codes for REDIRECT. 类型 5 代码定义

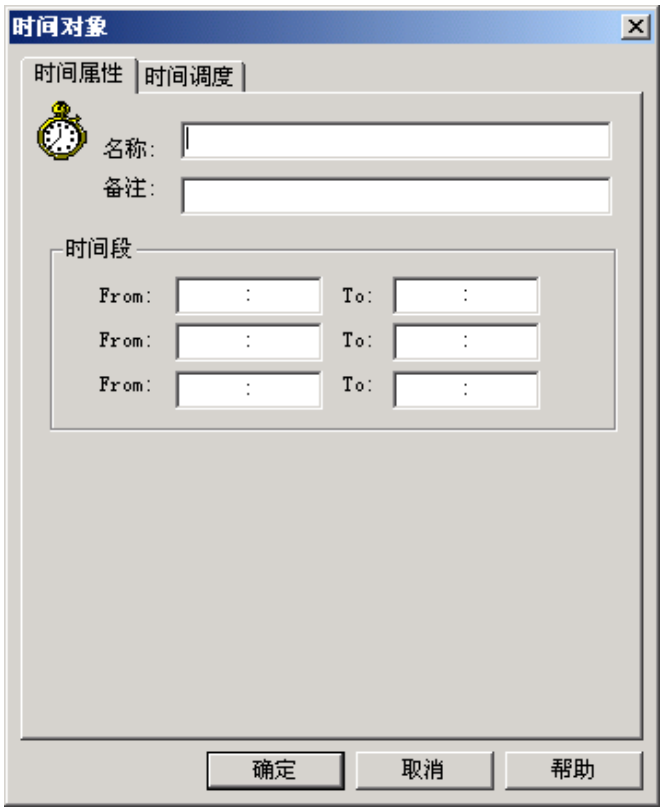
0	ICMP_REDIR_NET	Redirect Net
1	ICMP_REDIR_HOST	Redirect Host
2	ICMP_REDIR_NETTOS	Redirect Net for TOS
3	ICMP_REDIR_HOSTTOS	Redirect Host for TOS

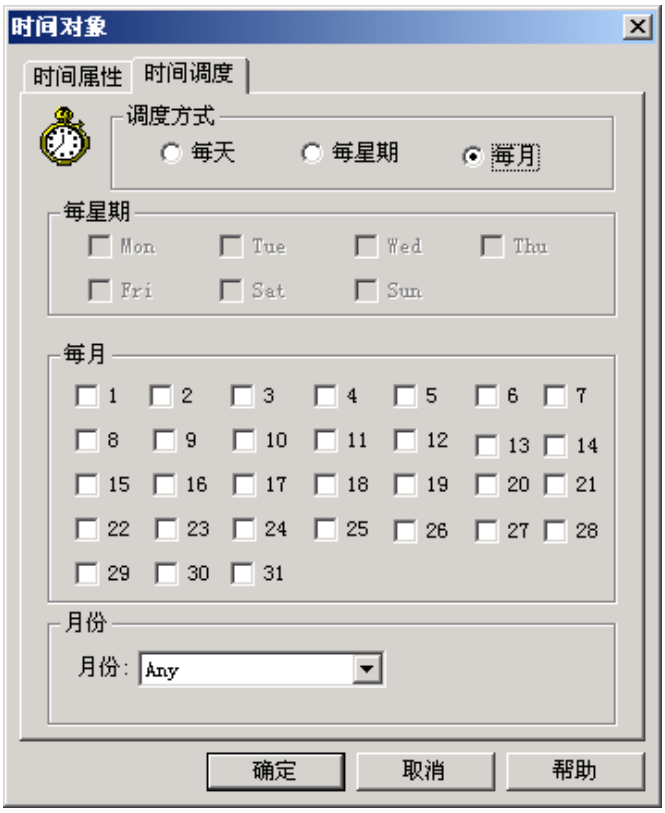
Codes for TIME_EXCEEDED. 类型 11 代码定义

0	ICMP_EXC_TTL	TTL count exceeded
1	ICMP_EXC_FRAGTIME	Fragment Reass time exceeded

定义协议组对象

定义时间对象

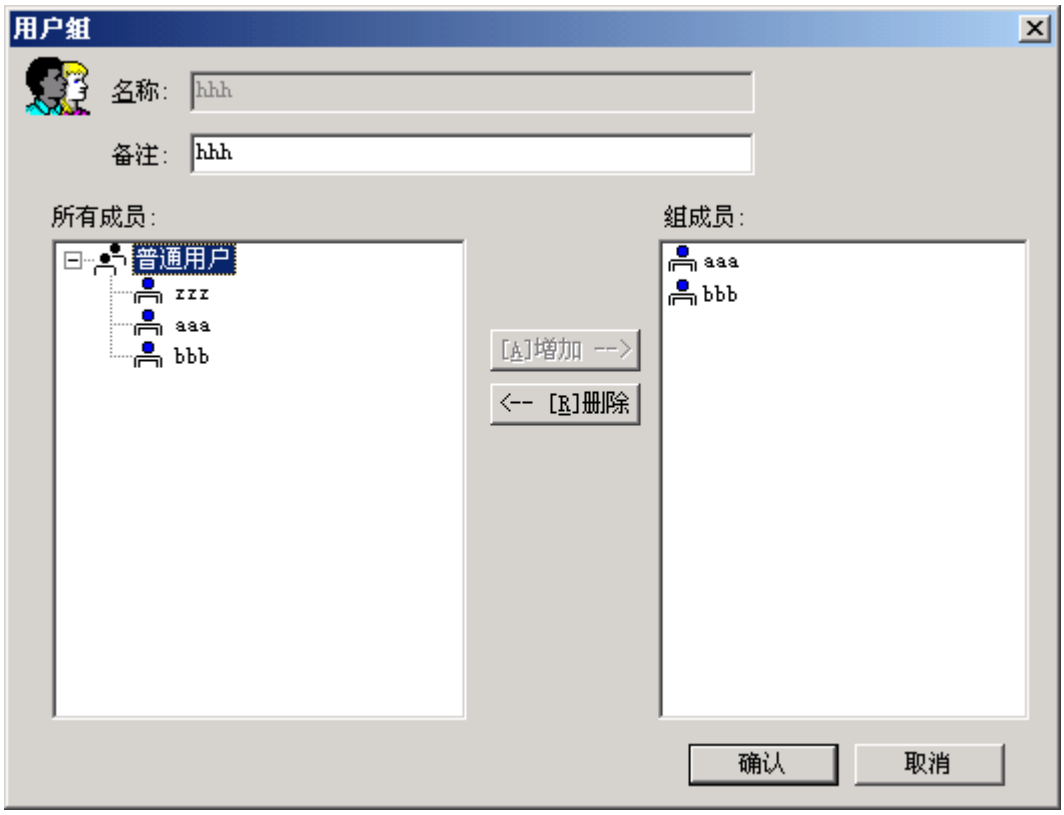




定义与卓冠防火墙其它安全产品交互的互动用户对象

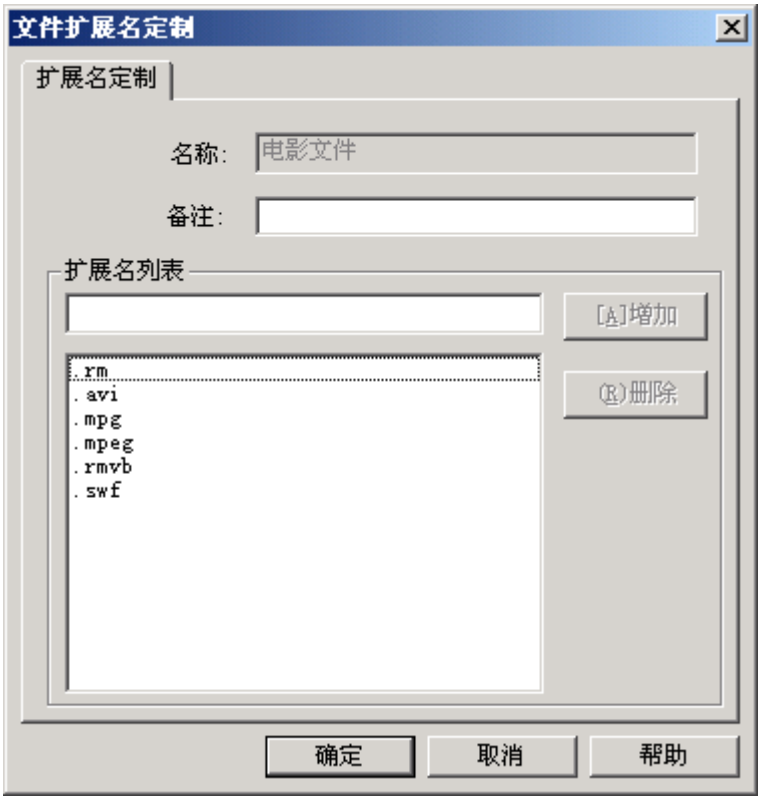
定义与卓冠防火墙用户认证的普通用户对象

定义与卓冠防火墙用户认证的普通用户组对象



定义文件类型对象

定义与文件类型相对应的文件扩展名



7.3.2 策略配置

首先策略设置分为五大部分：安全策略、文件过滤、流量控制、地址转换、地址绑定。

7.3.2.1 策略配置界面。

安全策略项目包括：序号、启用、源地址、目标地址、服务、动作、响应、时间、备注。

序号：策略号越小，策略优先级越高。

启用： 打勾后则本条策略是启用。

源地址、目标地址：可以是在左边网络内定义的主机、服务器、接口地址、网络、地址段、域名、地址组任一对象。

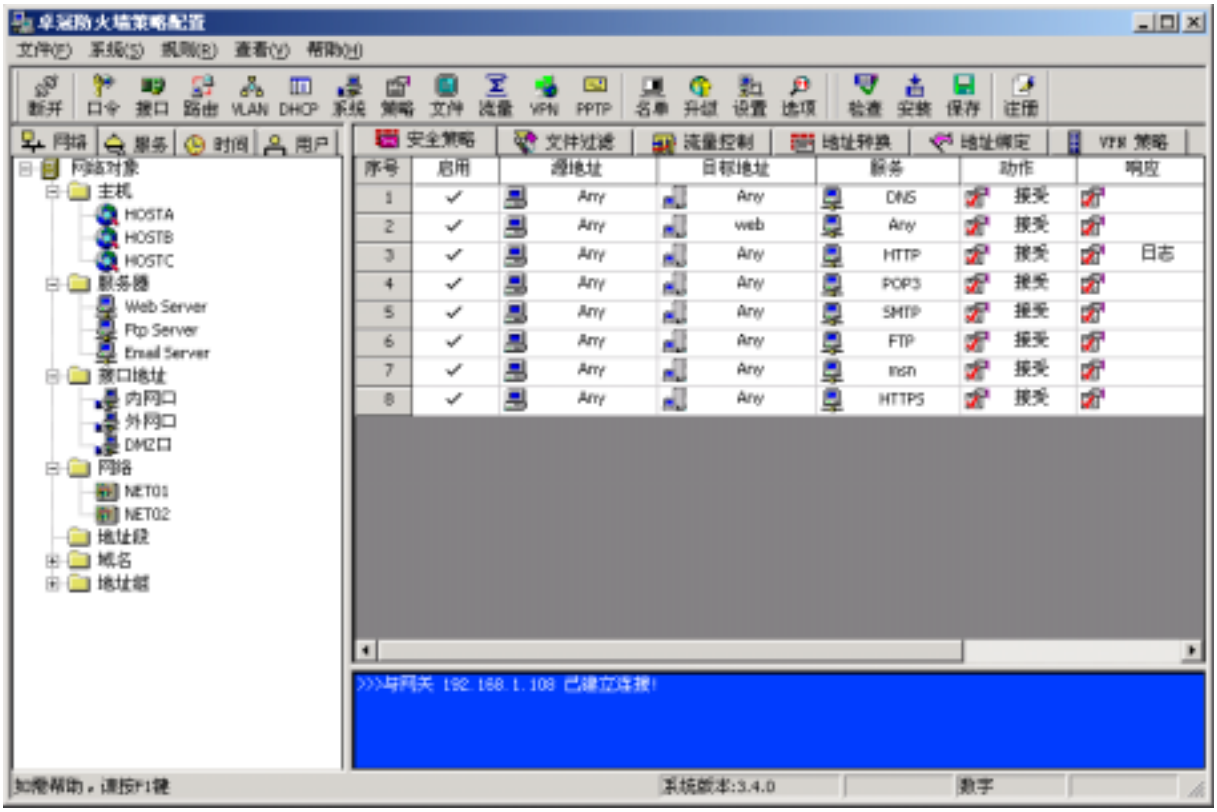
服务：可以是在左边服务内定义的 TCP、UDP、ICMP、其它服务、服务组任一对象

动作：可以是接受、拒绝、丢弃三种操作。

响应：日志、报警、邮件、SNMP、SYSLOG

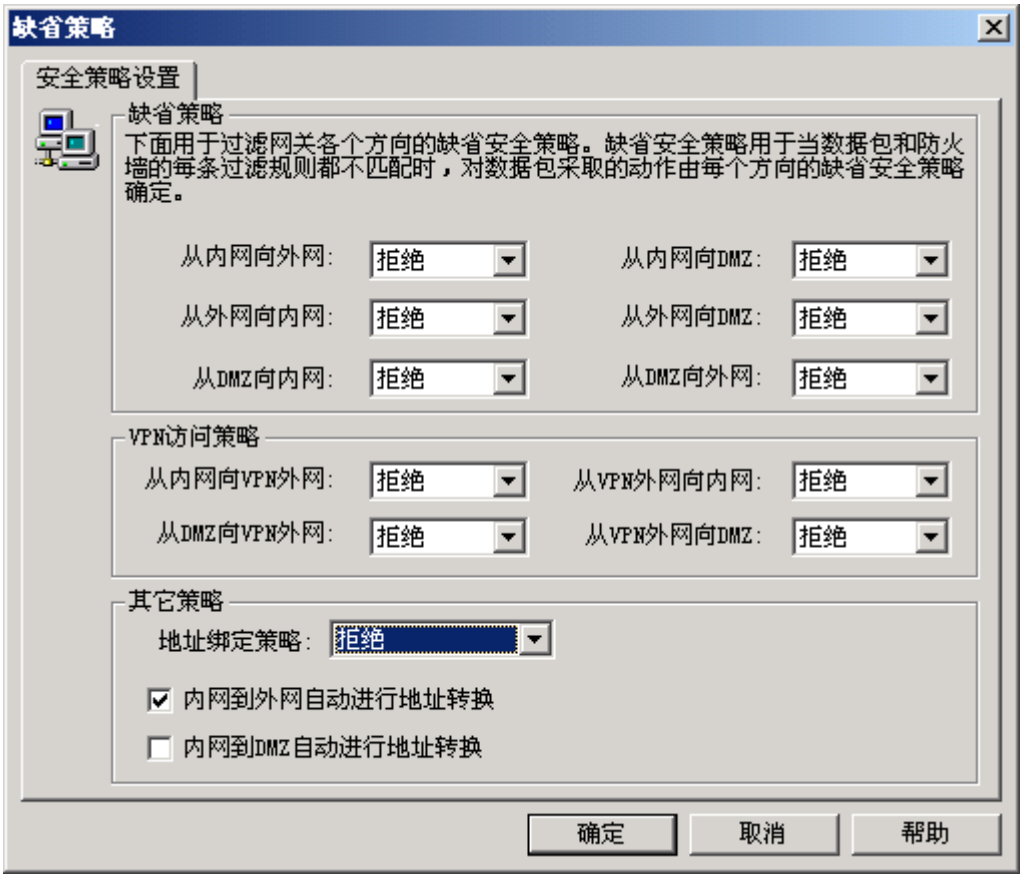
时间：本条策略作用时间（时间对象可以自定义）

备注：本条策略的说明



策略可以通过占击功能栏或菜单栏，右键快捷菜单来增加、删除、插入、清空、剪切、复制策略，也可定义相应的源主机、目的主机对象。

防火墙规则检查的顺序是从上到下.当数据包和所有规则不匹配时，缺省安全策略起作用。



7.3.2.2 文件过滤配置界面

文件过滤项目包括：序号、启用、源地址、文件扩展名、动作、响应、备注。

序号：策略号越小，策略优先级越高。

启用：打勾后则本条策略是启用。

源地址：可以是在左边网络内定义的 host、server、NAT IP、Network、Range、Domain、Group 任一对象。

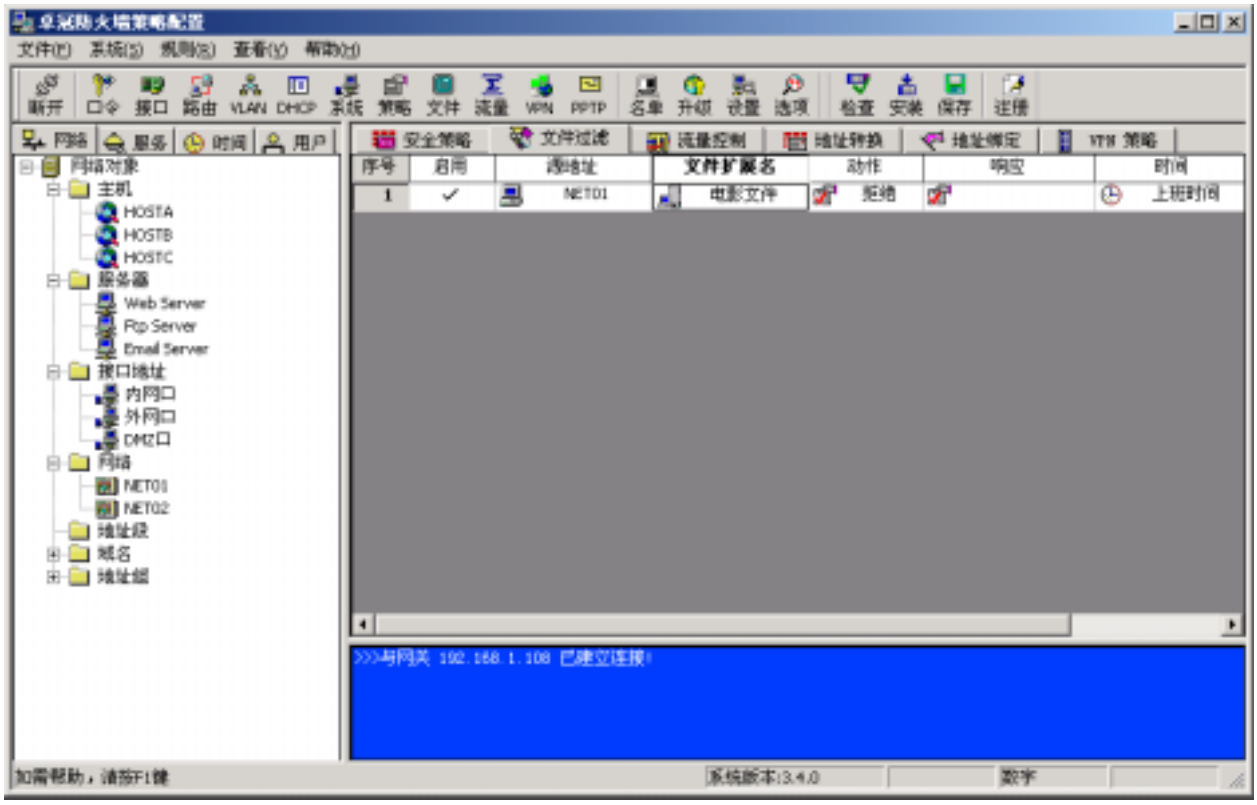
文件扩展名：被限制使用的文件类型（可自定义其包括那些文件扩展名文件）

动作：可以是接受、拒绝、丢弃三种操作。

响应：日志、报警、邮件、SNMP、SYSLOG

备注：本条策略的说明

策略可以通过占击功能栏或菜单栏，右键快捷菜单来增加、删除、插入、清空、剪切、复制策略，也可定义相应的源主机、目的主机对象



7.3.2.3 流量控制界面

流量控制项目包括：序号、启用、源地址、目标地址、服务、上行、下行，备注。

序号：策略号越小，策略优先级越高。

启用：打勾后则本条策略是启用。

源地址、目标地址：可以是在左边网络内定义的 host、server、NAT IP、Network、Range、Domain、Group 任一对象。

服务：可以是在左边服务内定义的 TCP、UDP、ICMP、OTHER、GROUP 任一对象

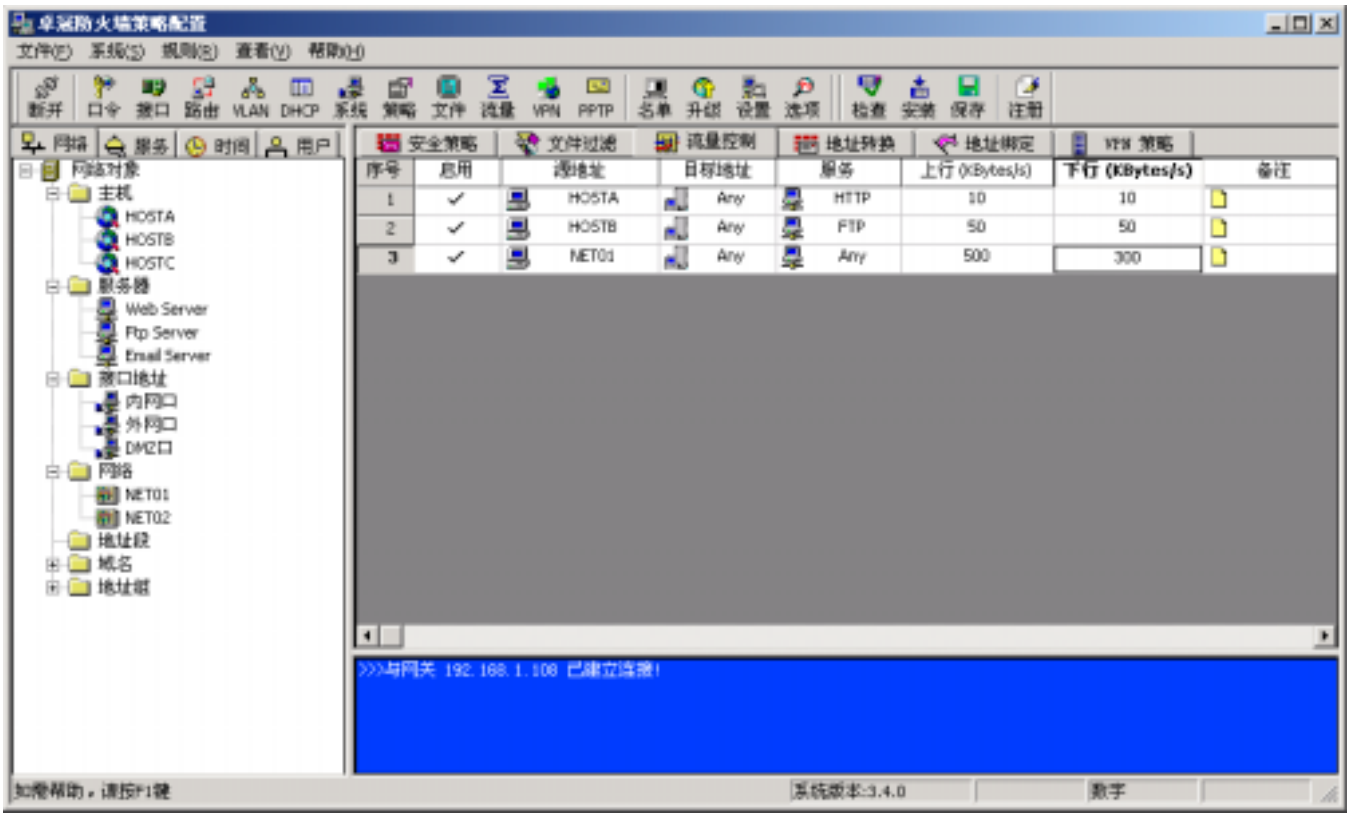
上行：源地址主机上行最高流量，以 kbytes 为单位。

下行：源地址主机下行最高流量，以 kbytes 为单位。

备注：本条策略的说明

策略可以通过占击功能栏或菜单栏，右键快捷菜单来增加、删除、插入、清空、剪切、复制策略，也可定义相应的源主机、目的主机对象

本防火墙出厂时不做任何设置



7.3.2.4 地址转换

地址转换项目包括：序号、启用、转换前、转换后、备注。

转换前包括源地址、目标地址、服务

转换后包括源地址、目标地址、服务

序号：策略号越小，策略优先级越高。

启用：占击右键快捷选规则有效，相应栏即打勾，表示本策略起作用

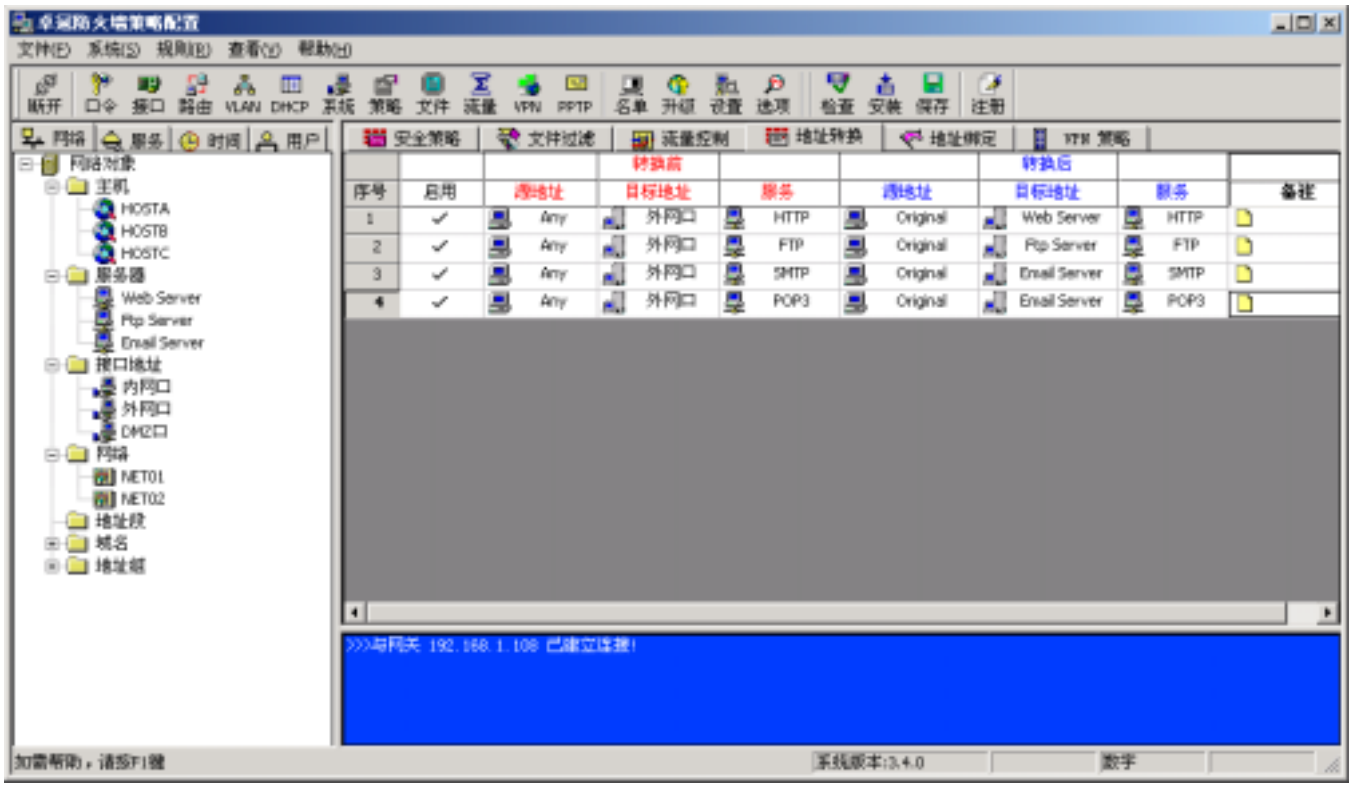
源地址、目标地址：可以是在左边网络内定义的 host、server、NAT IP、Network、Range、Domain、Group 任一对象。

服务：可以是在左边服务内定义的 TCP、UDP、ICMP、OTHER、GROUP 任一对象

备注：本条策略的说明

策略可以通过占击功能栏或菜单栏，右键快捷菜单来增加、删除、插入、清空、剪切、复制策略，也可定义相应的源主机、目的主机对象

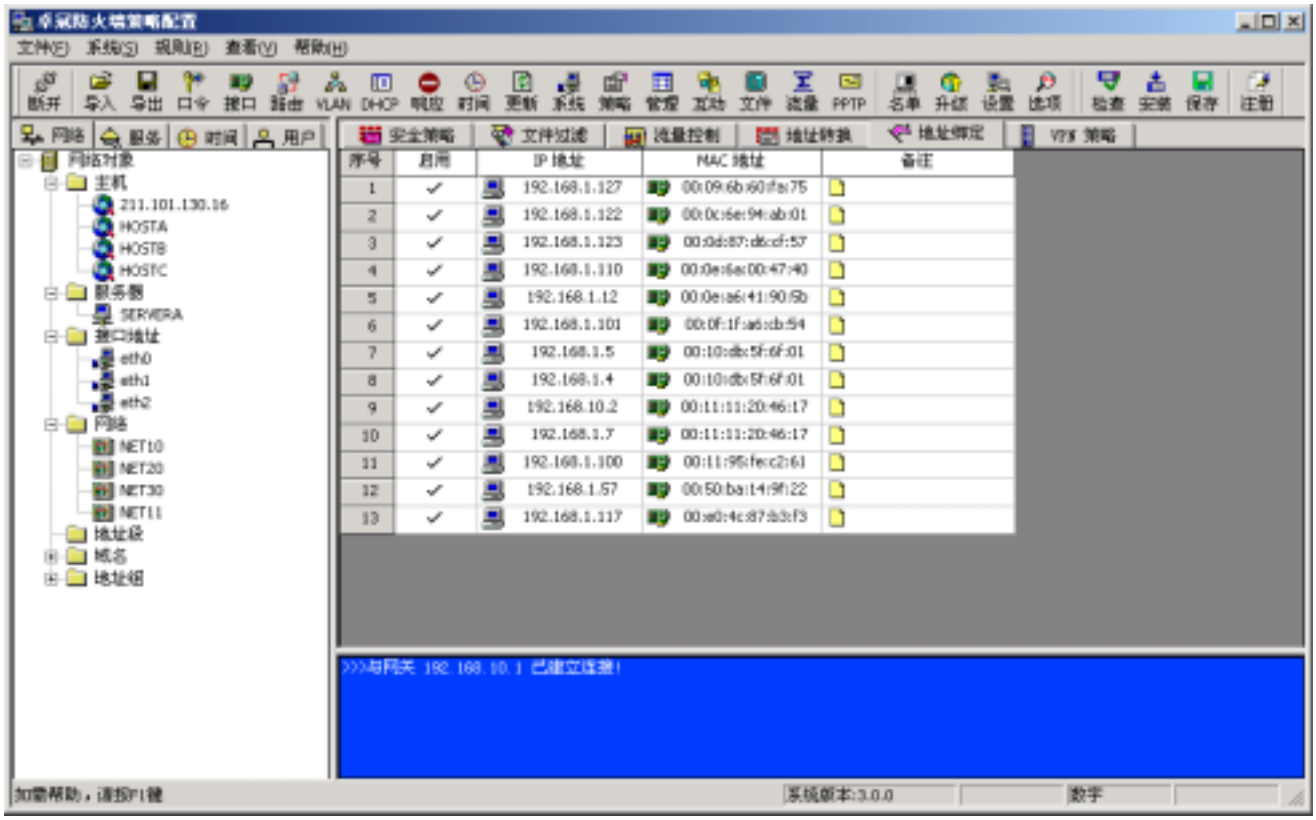
卓冠防火墙出厂时，该策略未做设置，需根据客户的网络拓朴结构，做相应的设置



7.3.2.5 IP 地址与 MAC 地址绑定

以防客户端改动 IP 地址后，使策略不起作用。

本规则只对单网段网络环境起作用，在多网段网络环境只对与卓冠防火墙内网网卡同一网段的电脑起作用 MAC 地址的获得。



7.3.2.6 防火墙对防火墙 VPN 及 PPTP 服务设置

- **网关对网关的 VPN**

例：实现两台防火墙通过网关对网关的 VPN，共享密钥模式（密钥为 vpn），实现各自内网网段之间的互访

卓冠防火墙 A（墙下的内部网段是 192.168.0.0）

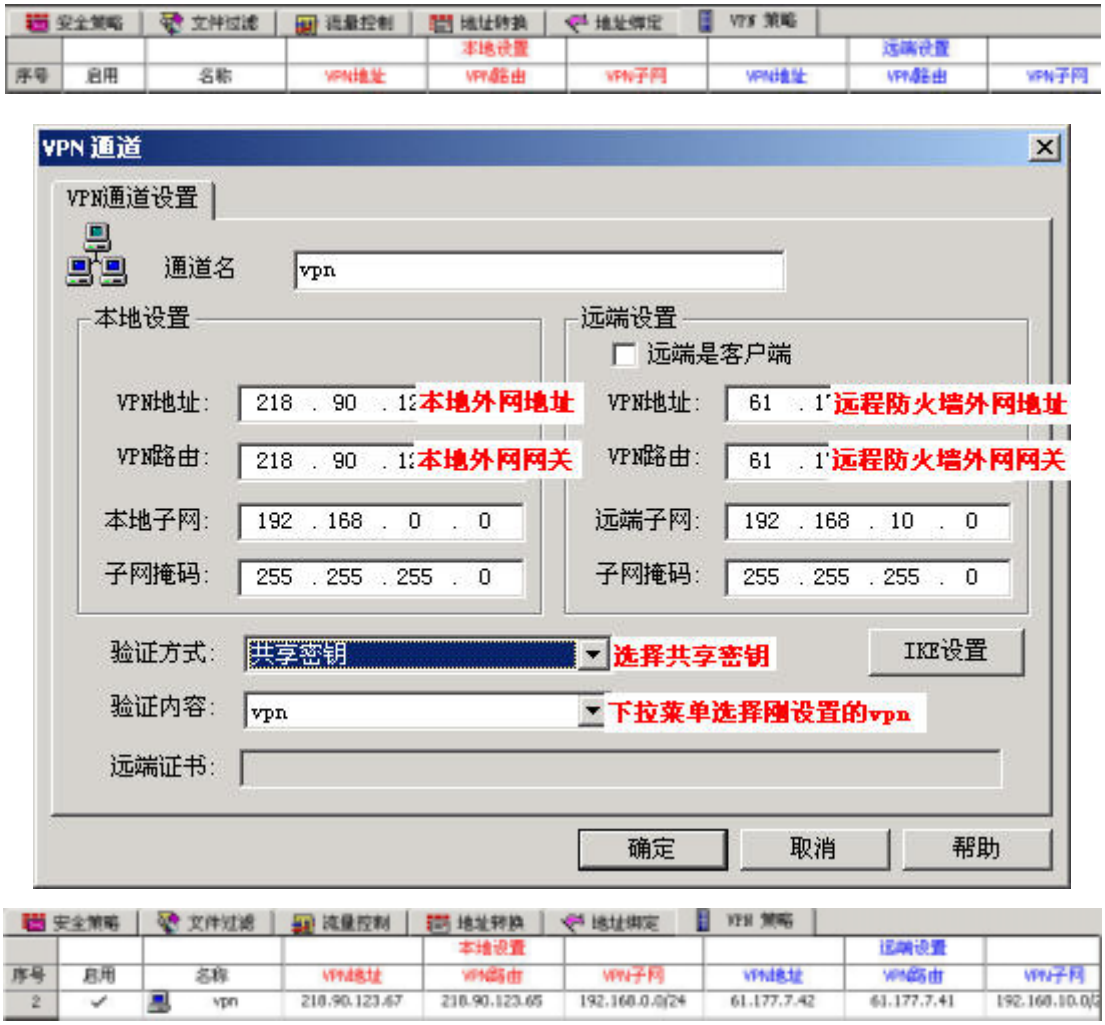
卓冠防火墙 B（墙下的内部网段是 192.168.10.0）

卓冠防火墙 A 的设置：

进入防火墙 A 策略管理，点击菜单栏里的“ vpn ”

设置”vpn 共享密钥”名称和密码均设置为”vpn”

在“ vpn 策略 ”里增加一条规则



通道名可任意取

本地设置：VPN 地址指本地防火墙 IP 地址

VPN 路由指本地防火墙缺省网关地址

本地子网指本地 VPN 共享网段

子网掩码指本地 VPN 共享网段的掩码

远程设置：VPN 地址指远端防火墙 IP 地址

VPN 路由指远端防火墙缺省网关地址

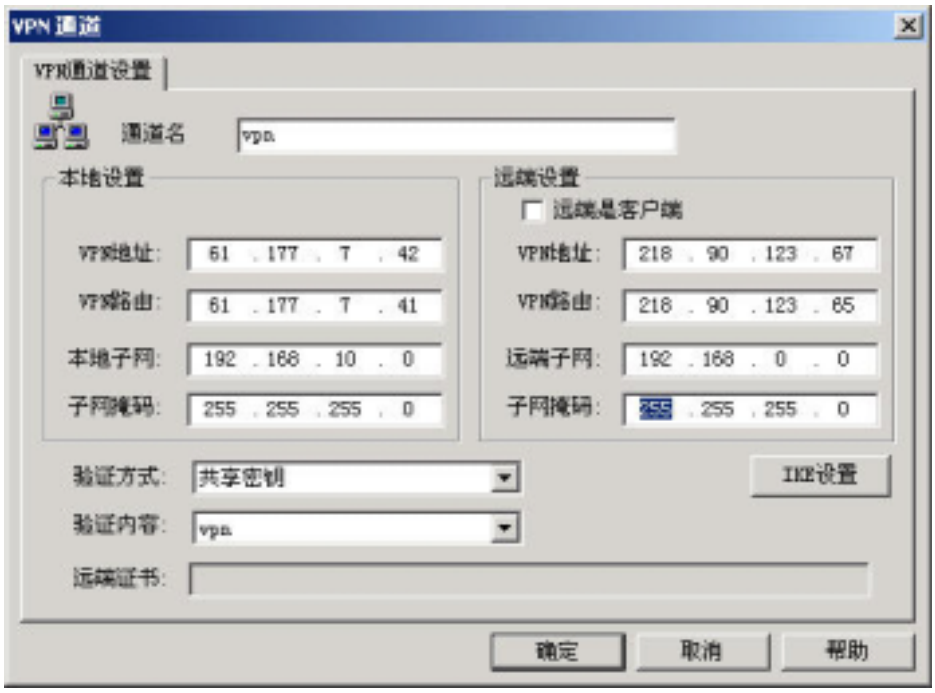
远端子网指远端 VPN 共享网段

子网掩码指远端 VPN 共享网段的掩码

预共享密钥：VPN 共享密钥

卓冠防火墙 B 的设置：

对于远端的防火墙则与本地防设置正好相反，本地设置参数是远端防火墙的远程设置参数；远端设置参数是远端防火墙的本地设置参数

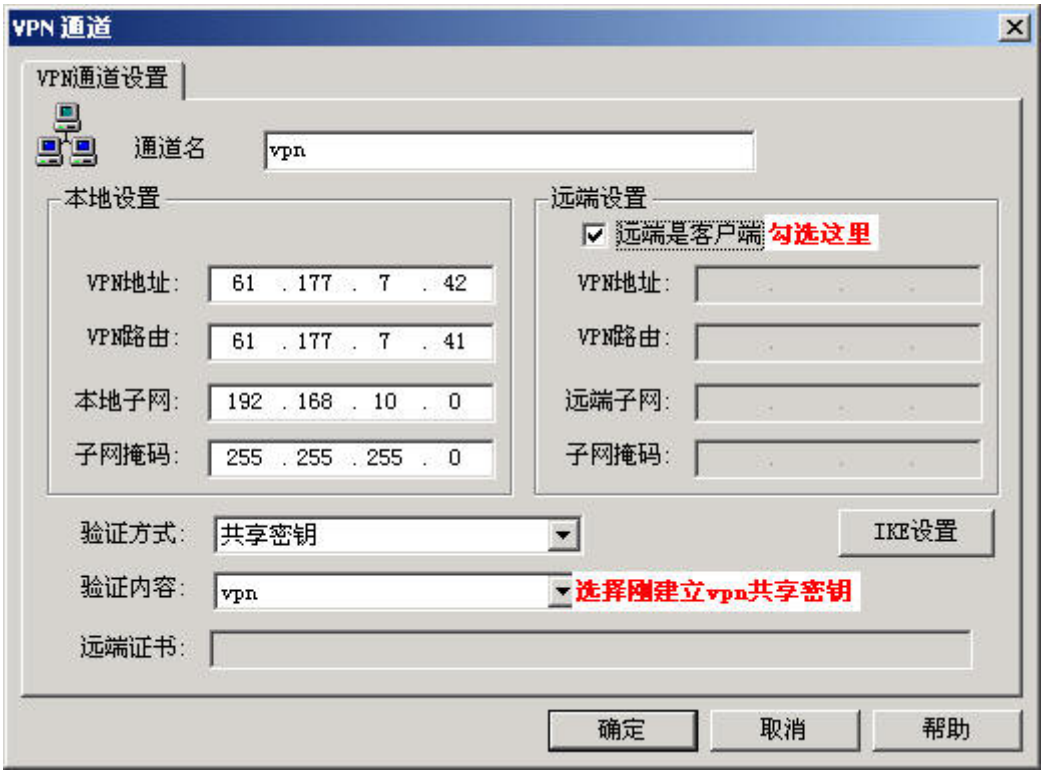


- **Ipsec vpn 客户端拨入防火墙的配置：**

  首先，进入防火墙策略管理，点击菜单栏里的“ vpn ”

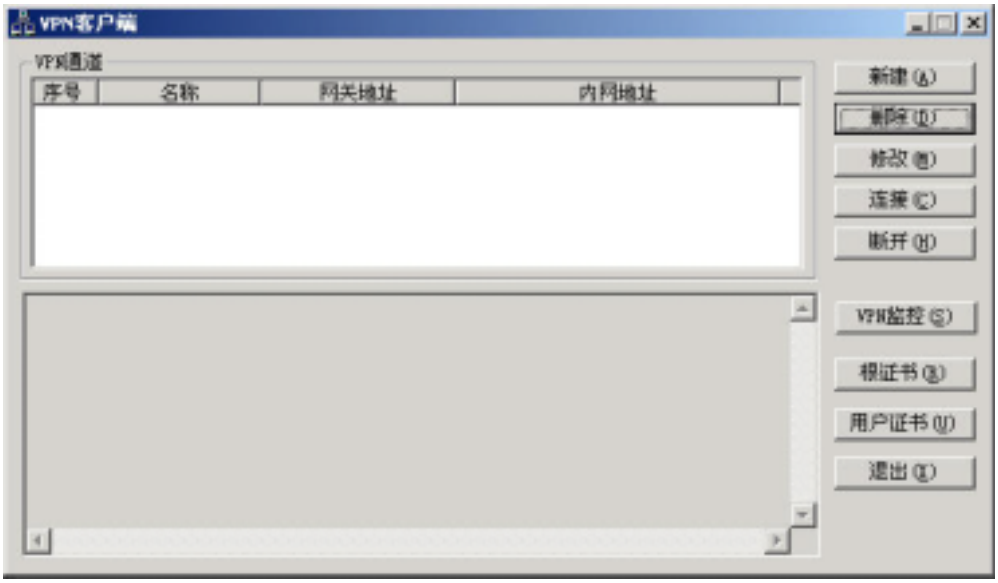
设置”vpn 共享密钥”名称和密码均设置为”vpn”,

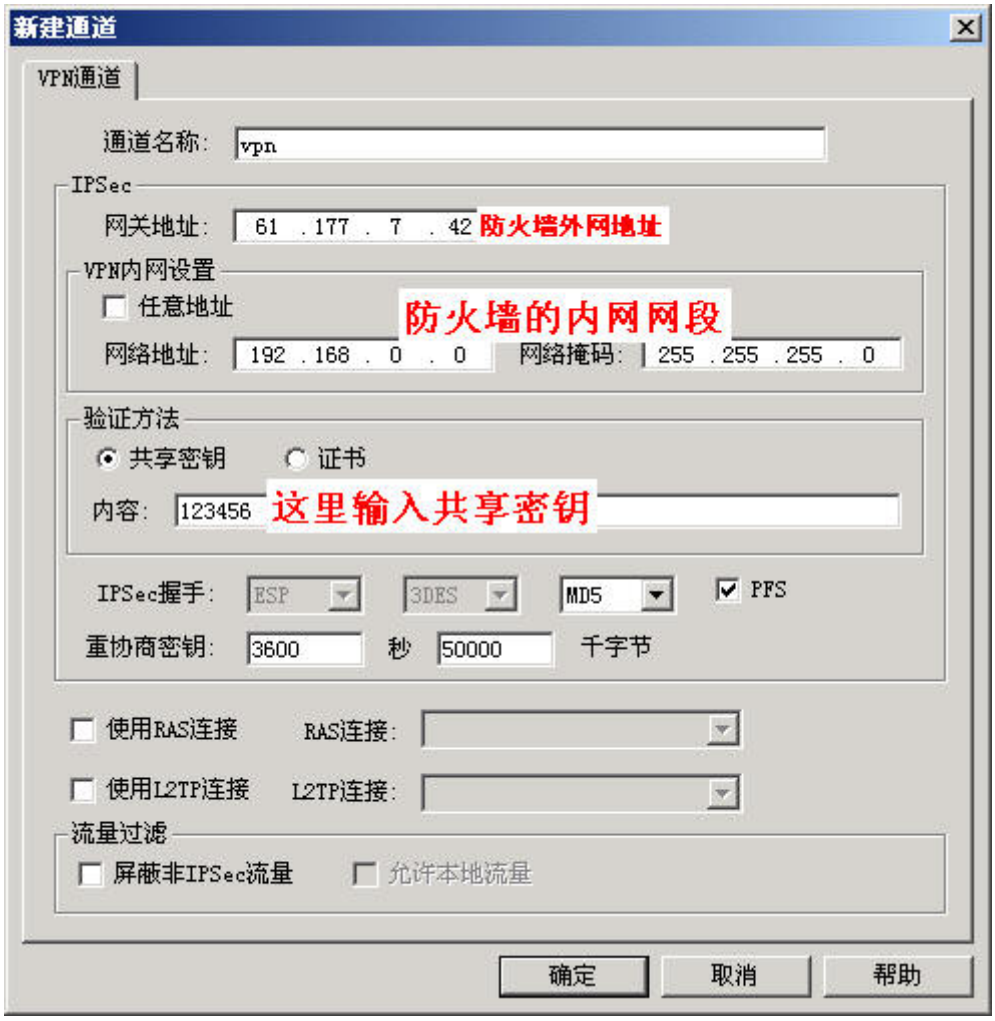
在“ vpn 策略 ”里增加一条规则

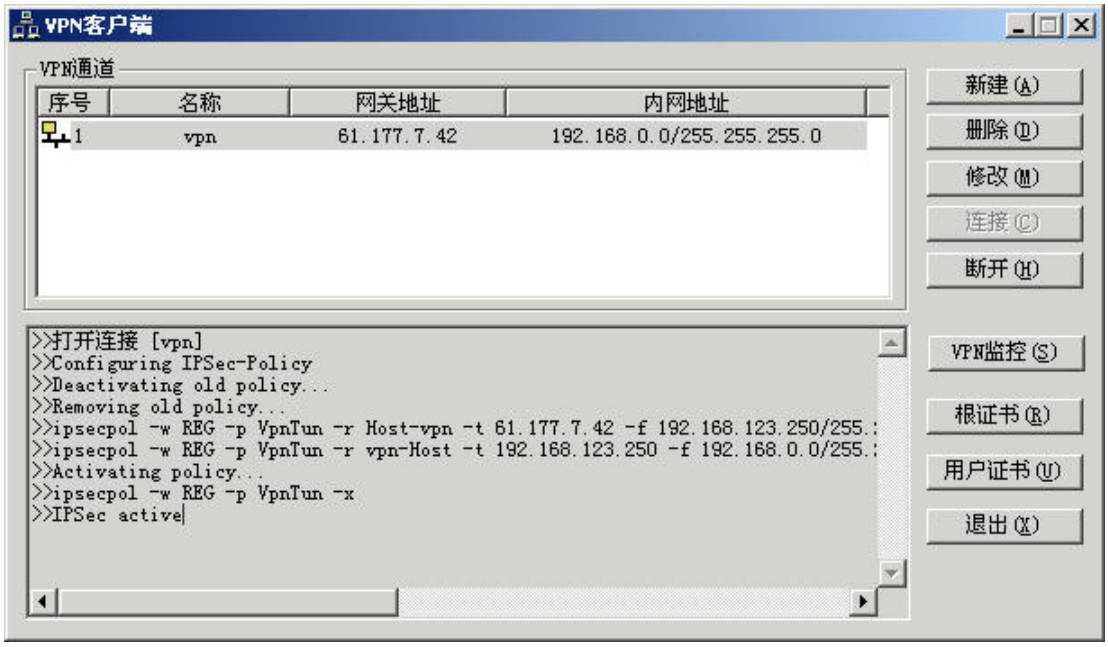


接下来安装配置客户端：

安装完客户端后,点击桌面快捷方式,运行 VPN 客户端，
新建一个 vpn 通道，如图

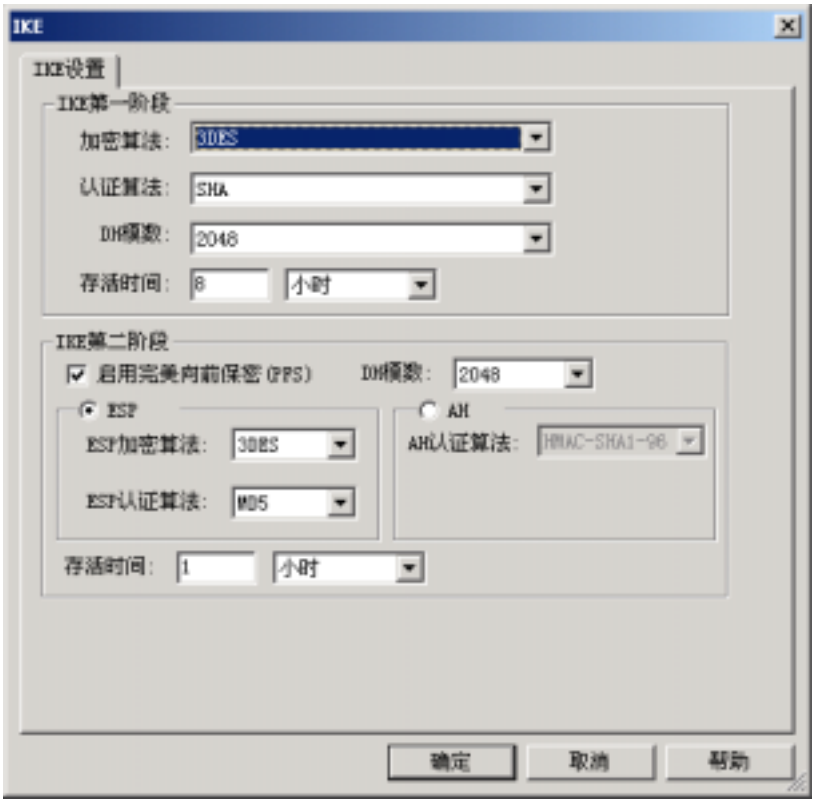






点击连接按钮，即可实现 VPN 拨入了！

注意:IKE 设置如下图，本地防火墙设置参数和远端防火墙设置参数要相同。



- 防火墙 pptp 服务

  操作步骤如下：

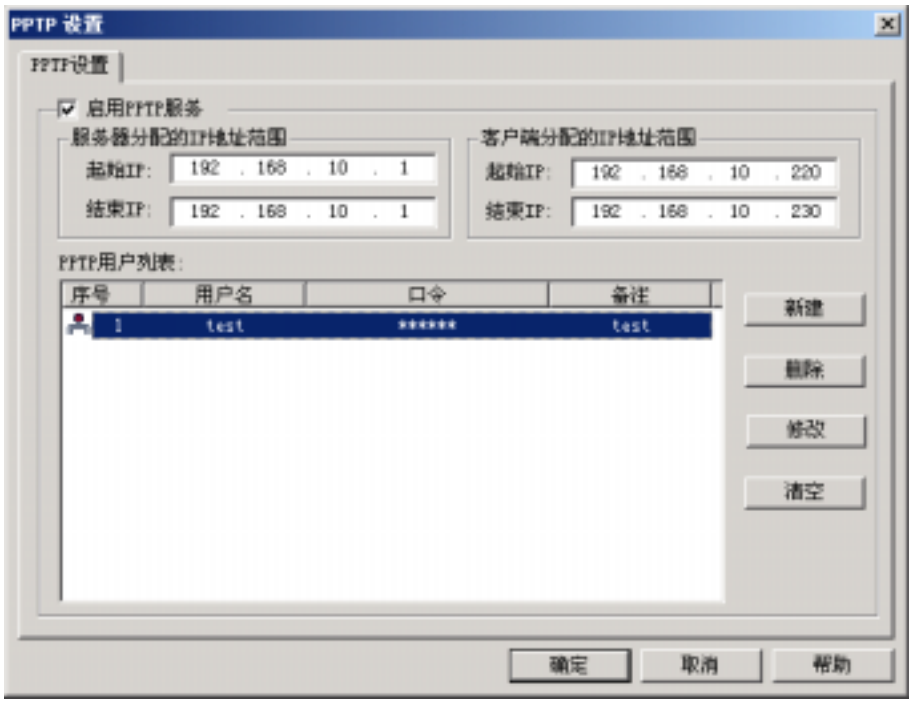
  点击策略管理主界面,PPTP 按钮 

,设置如下 PPTP 策略:

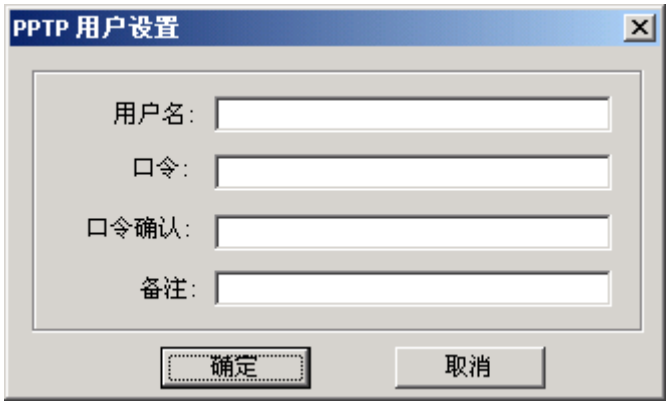
  在启动 PPTP 服务框打勾启动 PPTP 服务。

  服务器分配地的 IP 地址范围指防火墙内网地址。

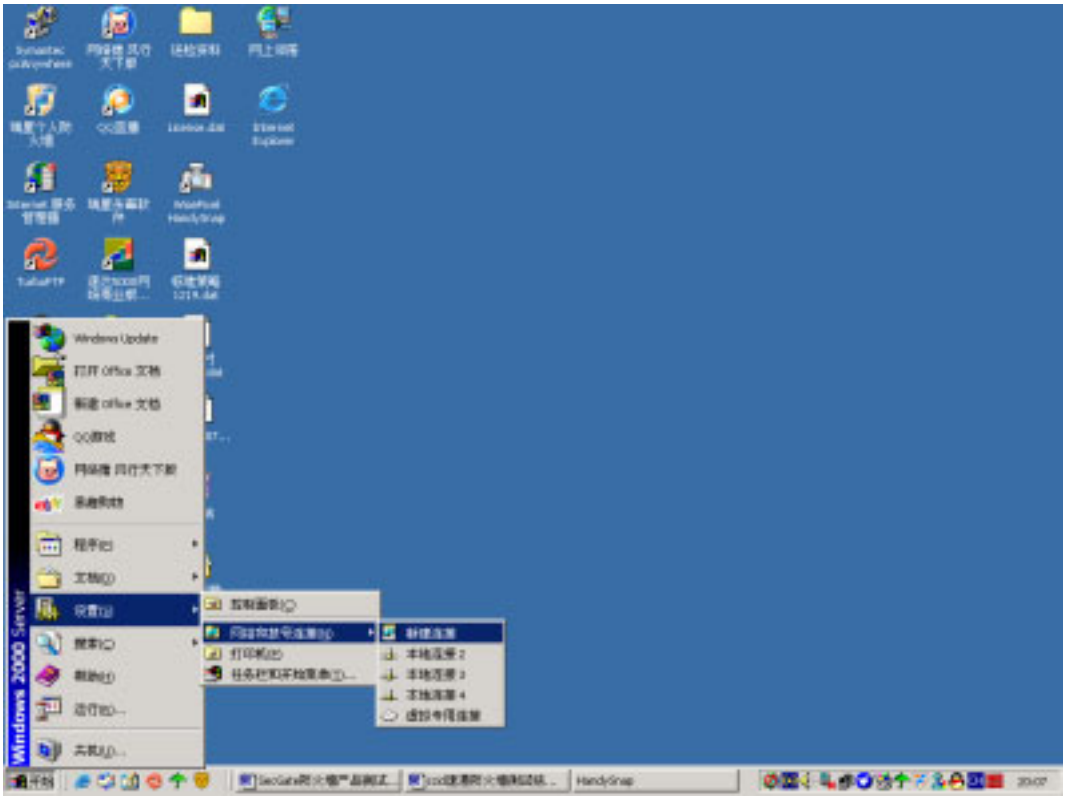
客户端分配的 IP 地址范围指 PPTP 客户端拨入后得到的 IP 地址范围。



在 PPTP 用户列表中可新建拨入用户的用户名及其口令。

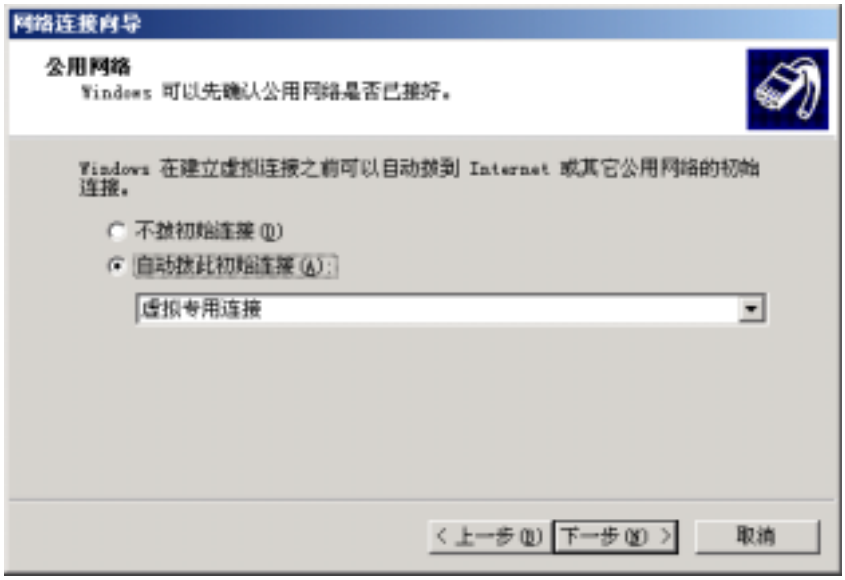


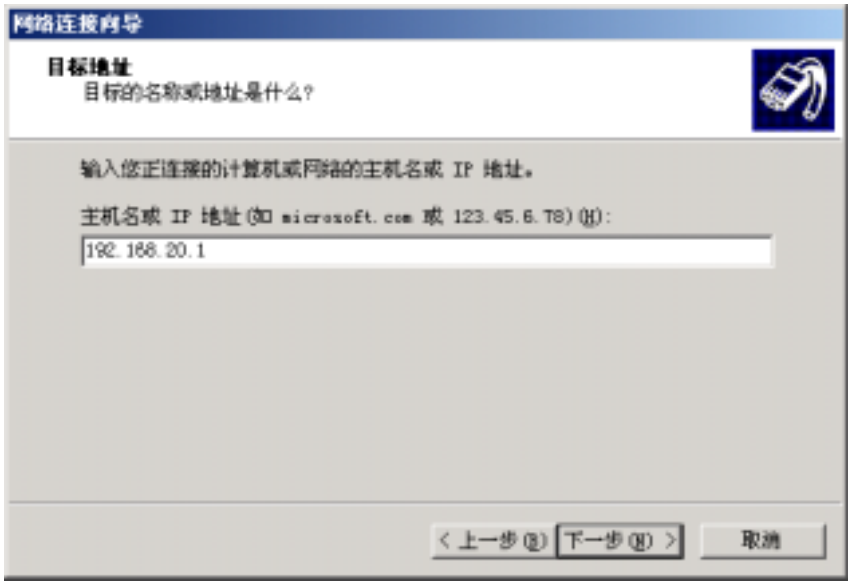
客户端设置（以 windows 2000 为例）：首先从开始---->设置---->网络拨号连接---->新建连接----->下一步---->选择通过 Internet 连接到专用网络---->选择自动拨此初始连接---->下一步---->完成。即创建一个 PPTP 的 VPN 连接

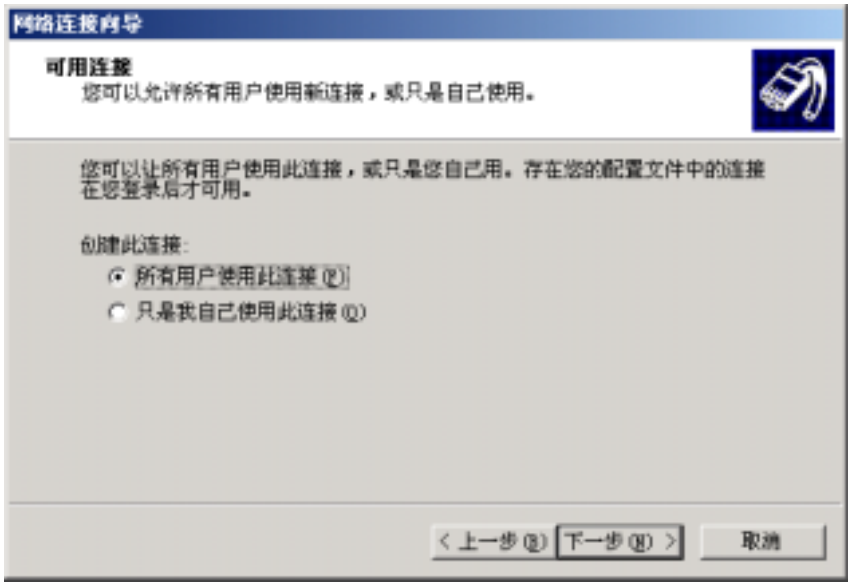

Windows 2000 Server

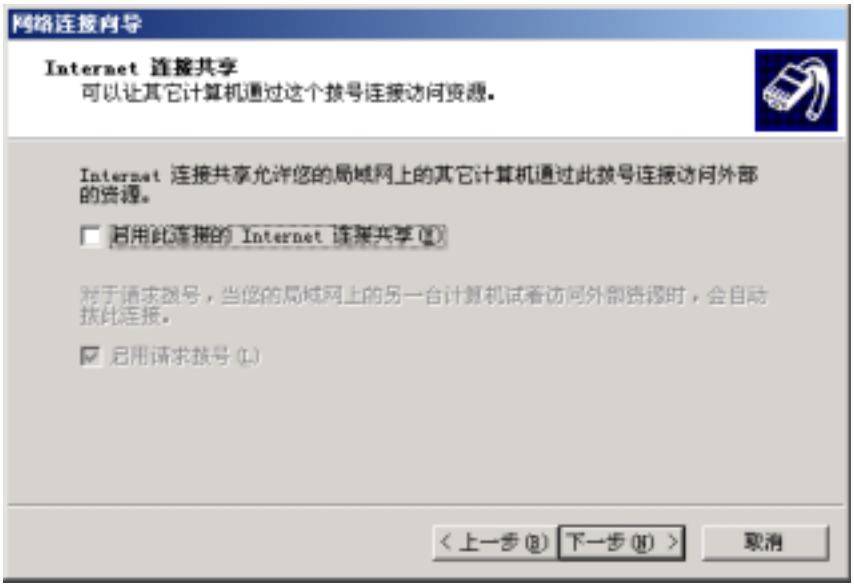

网络连接向导
欢迎使用“网络连接向导”
用这个向导，您可以创建一个连到其它计算机和网络，启用应用程序的连接，如 电子邮件、Web 浏览、文件共享和打印。
要继续，请单击“下一步”。
< 上一步(B)
下一步(N) >
取消

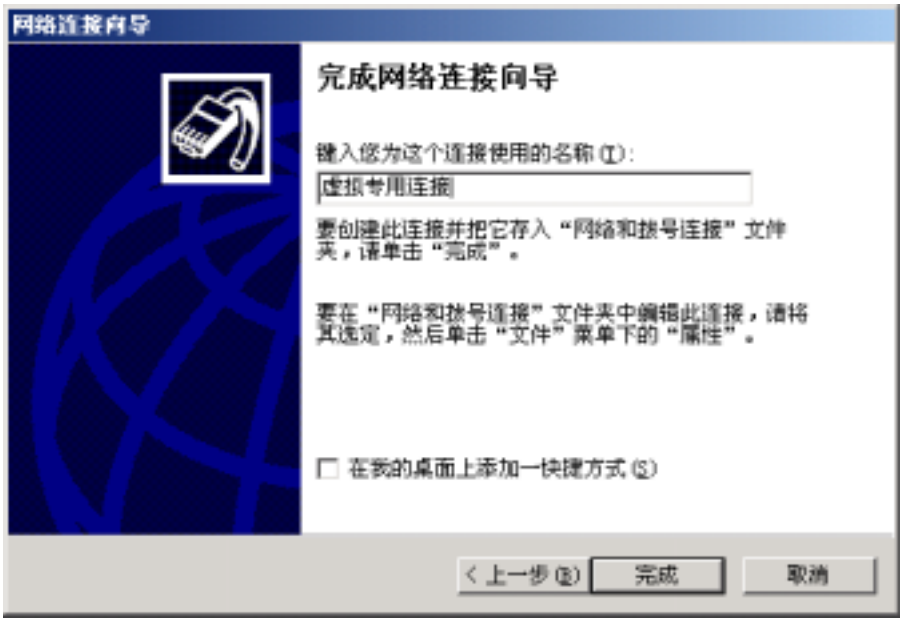

网络连接向导
网络连接类型
根据网络配置和联网需要，您可以选择要创建的网络连接类型。
拨号到专用网络(P)
用我的电话线(调制解调器或 ISDN)连接。
拨号到 Internet(D)
用我的电话线(调制解调器或 ISDN)连接到 Internet。
通过 Internet 连接到专用网络(V)
通过 Internet 创建虚拟专用网络(VPN)连接，即"隧道"。
接受传入的连接(A)
让其它计算机使用电话线，Internet 或用电缆直接连接到我的计算机。
直接连接到另一台计算机(C)
使用我的串行、并行或红外端口连接。
< 上一步(B)
下一步(N) >
取消


网络连接向导
公用网络
Windows 可以先确认公用网络是否已接好。
Windows 在建立虚拟连接之前可以自动拨到 Internet 或其它公用网络的初始连接。
不拨初始连接(D)
自动拨此初始连接(A):
虚拟专用连接
< 上一步(B)
下一步(N) >
取消


网络连接向导
目标地址
目标的名称或地址是什么?
输入您正连接的计算机或网络的主机名或 IP 地址。
主机名或 IP 地址(如 microsoft.com 或 123.45.6.78)(H):
192.168.20.1
< 上一步(B)
下一步(N) >
取消


网络连接向导
可用连接
您可以允许所有用户使用新连接，或只是自己使用。
您可以让所有用户使用此连接，或只是您自己用。存在您的配置文件中的连接在您登录后才可用。
创建此连接:
所有用户使用此连接(A)
只是我自己使用此连接(O)
< 上一步(B)
下一步(N) >
取消

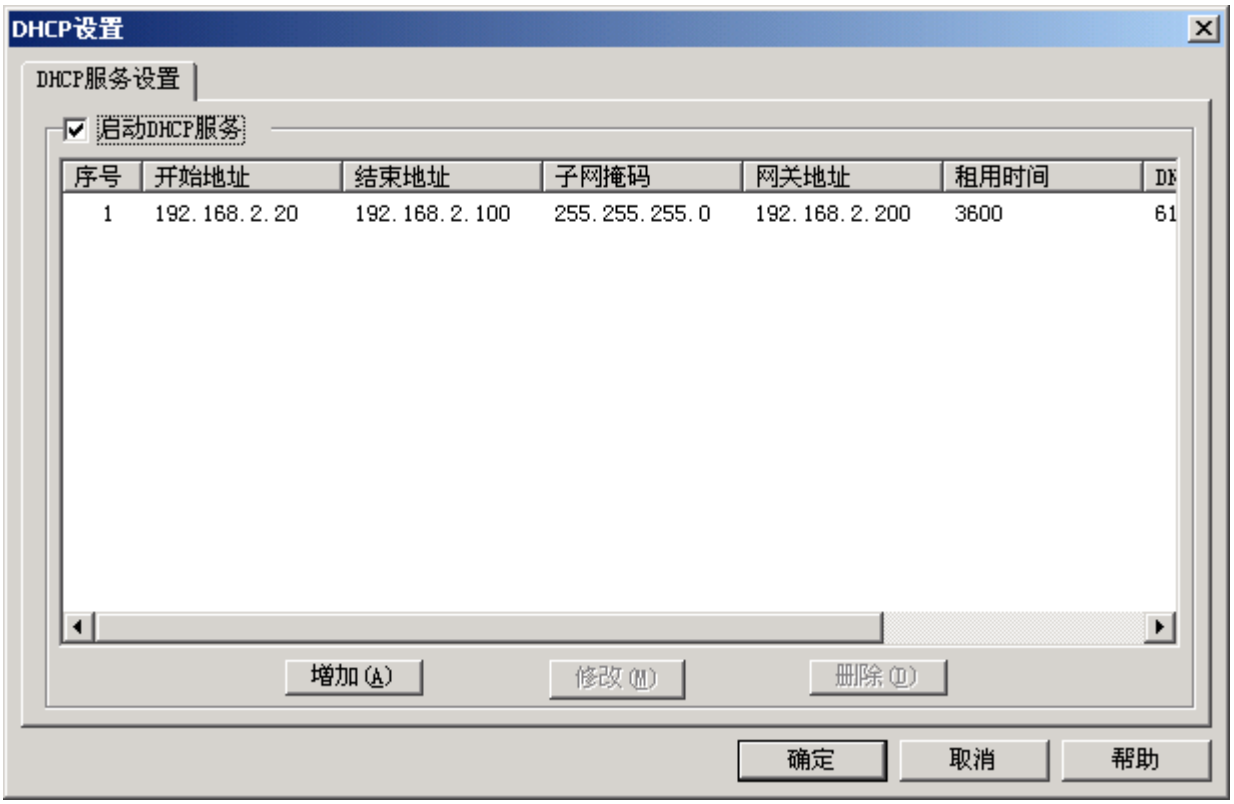

网络连接向导
Internet 连接共享
可以让其它计算机通过这个拨号连接访问资源。
Internet 连接共享允许您的局域网上的其它计算机通过此拨号连接访问外部的资源。
启用此连接的 Internet 连接共享(E)
对于请求拨号，当您的局域网上的另一台计算机试着访问外部资源时，会自动拨此连接。
启用请求拨号(D)
< 上一步(B)
下一步(N) >
取消


网络连接向导
完成网络连接向导
键入您为这个连接使用的名称(T):
虚拟专用连接
要创建此连接并把它存入“网络和拨号连接”文件夹，请单击“完成”。
要在“网络和拨号连接”文件夹中编辑此连接，请将其选定，然后单击“文件”菜单下的“属性”。
在我的桌面上添加一快捷方式(S)
< 上一步(B)
完成
取消

7.3.2.7 DHCP 服务设置

点击策略管理主界面,DHCP 按钮 

,设置如下 DHCP 策略:



7.3.2.8 黑名单库网络更新功能

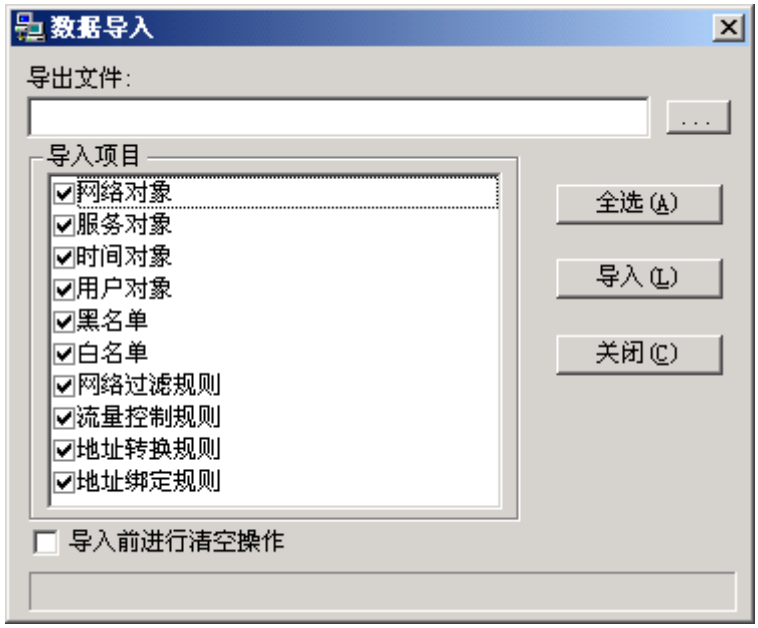
此功能是本软件的一大特色，由于有害网站库的记录数高达数百万条，用户添加几乎不可能，故有害网站

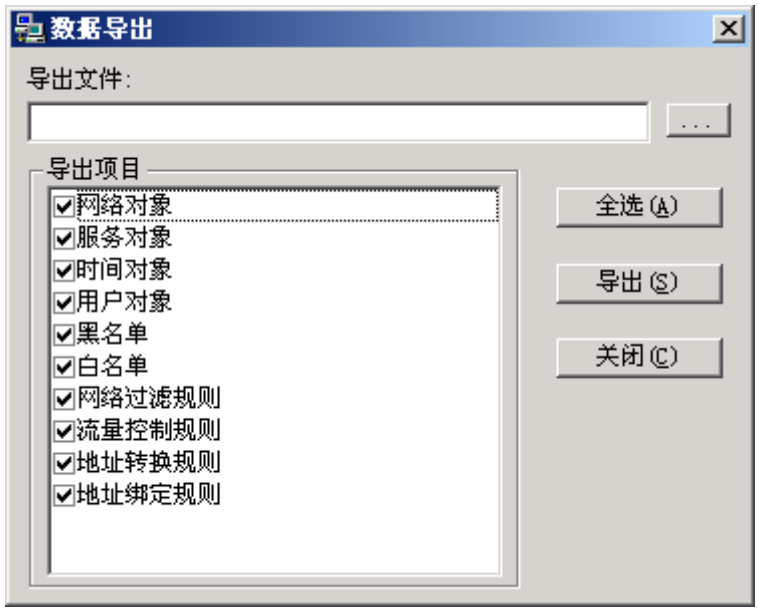
库由本公司统一收集，用户在成功完成用户注册后，点击主界面上的“ 升级 ”按钮进行智能升级，本软件会自动进行黑名单库的升级。同时我们对有害网站库做了统一的分类，用户可以设置使相应分类下的有害网站在客户端不能访问。

- 网络黑名单：凡在黑名单定义的网站，如果打勾生效，并安装了策略，则客户端均不允许访问所定义的网站。本功能可定义黑名单组，如游戏网站、证券网站等。在组下面我们可以再定义网站项，个数不限。增加的网站系统会自动解析 ip 地址，同时可在组及项目前面打勾，使只有打勾的网站在安全策略里生效。
- 网络白名单：如果我们想访问在黑名单中定义的网站，那么则需要在白名单定义项目，如果打勾生效，并安装了策略，则客户端可访问白名单定义的网站，无论黑名单中是否定义了此网站。本功能可定义白名单组，如新闻网站、教育网站等。在组下面我们可以再定义网站项，个数不限。增加的网站，系统会自动解析ip地址，同时可在组及项目前面打勾，使只有打勾的网站在安全策略里生效。

7.3.2.9 策略数据导入、导出

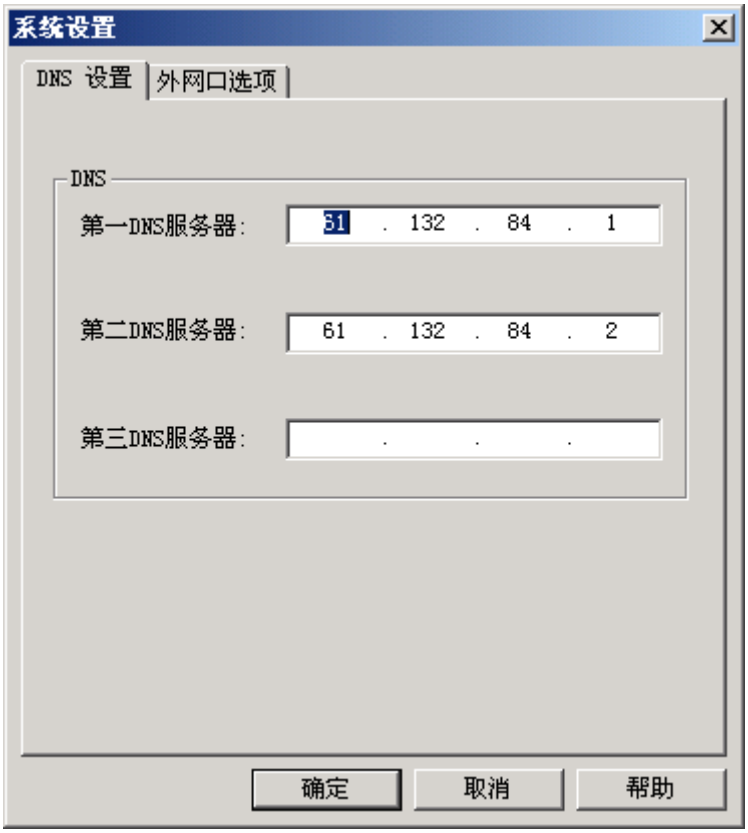
可将先前备份的或第三方定义的网络对象、服务对象、时间对象、黑名单、白名单、网络过滤规则、流量控制规则、地址转换规则、地址转换规则、地址绑定规则。方便用户初始化或恢复设置策略。





7.3.2.10 DNS 代理设置

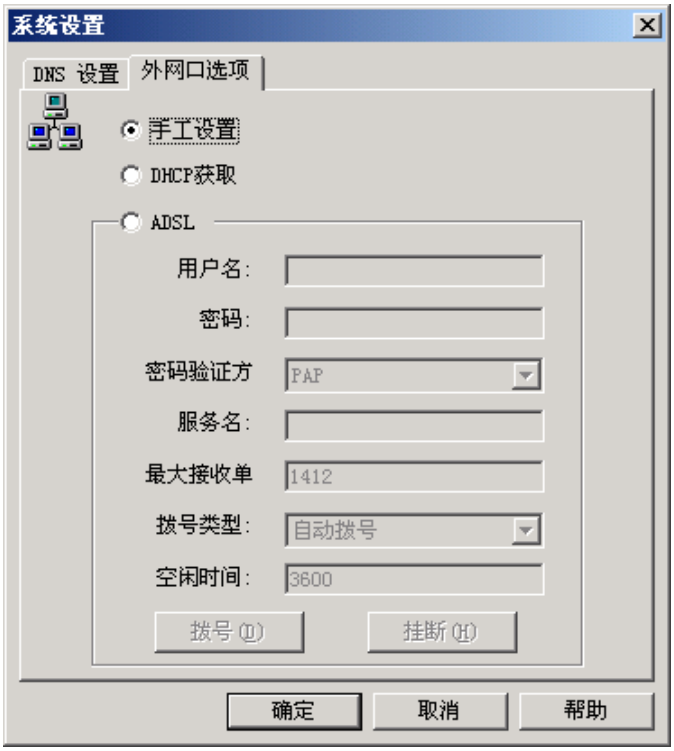
DNS 代理设置的含义：在安全区客户端的 TCP/IP 设置可填写防火墙内网地址做为 DNS 地址，而无需填写公网 DNS。由防火墙做 DNS 代理转发。



7.3.2.11 外网口其他获得地址方式

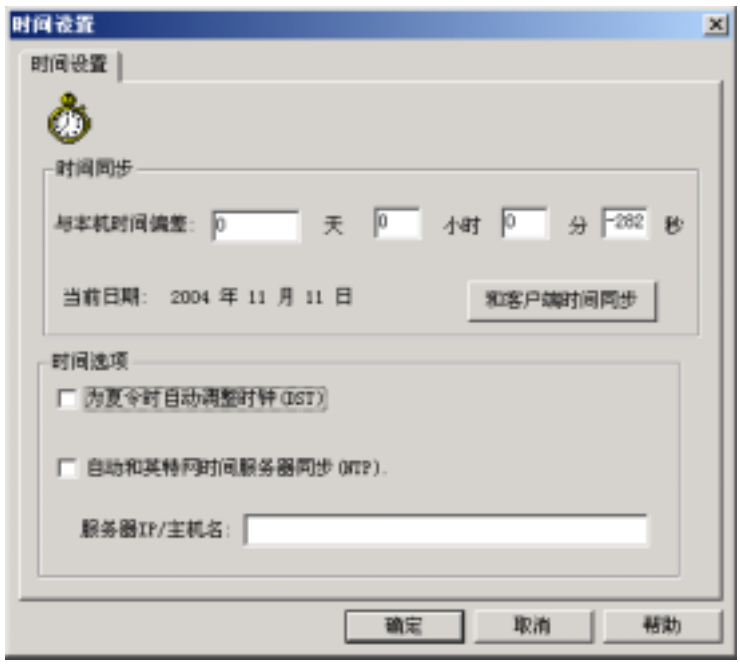
点击主界面,系统按钮 

,再点击外网口选项，如下图所示:可设置外网口 IP 地址动态分配获取，也可设置为 ADSL 的拨号接入并支持自动重拨功能。



7.3.2.12 对系统时间方面的调整

检查防火墙时间与当前客户端时间的偏差。如果时间偏差过大，超出许可证指定日期范围，防火墙会发生异常现象：PING 不通，策略不起作用。点击与客户端时间同步按钮，即可改变防火墙系统时间，也可与英特网上标准的时间服务进行自动同步，只需在时间服务器 IP/主机名填入相应的 IP 地址。



7.3.2.13 管理地址设定

指定防火墙监控端运行的 IP 地址，防止软件被不从不安全的地方进行配置。

7.4 日志和状态监控

卓冠防火墙需要一台单独的日志客户端，因为防火墙可以根据用户的需要生成大量的日志数据。防火墙可

以让用户选择如何记录日志。在访问策略中：定义访问策略时，设置完源地址、目标地址、服务、动作、时间后，可以定义匹配这条策略时做何种日志。

防火墙的审计信息可以自动实时传送到日志客户端，审计信息传输条件必须有审计服务器连接上防火墙的日志服务，当防火墙上无任何审计服务器连接时，防火墙将审计信息写入本地的内存缓冲中，防火墙本地缓冲为 50M；

在审计信息数量达到缓冲区的最大数值后，仍无日志客户端连接上防火墙，则防火墙将覆盖最早的审计信息；

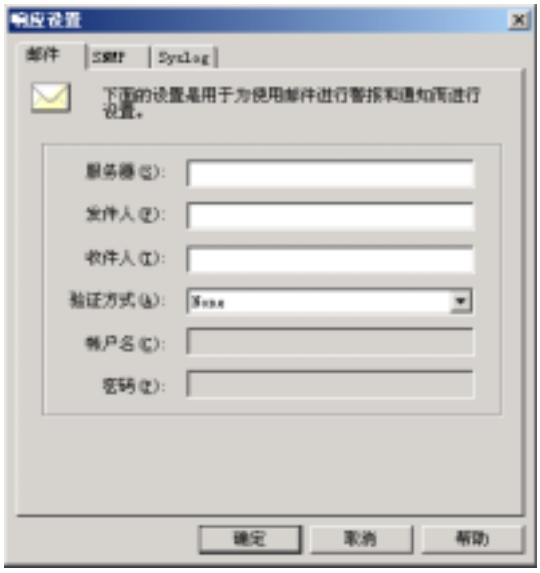
任何时候，一旦有日志客户端连接上防火墙，防火墙的审计信息存储模式立即由本地存储模式转换为网络传输模式，本地当前的审计信息也同时传到日志客户端上；

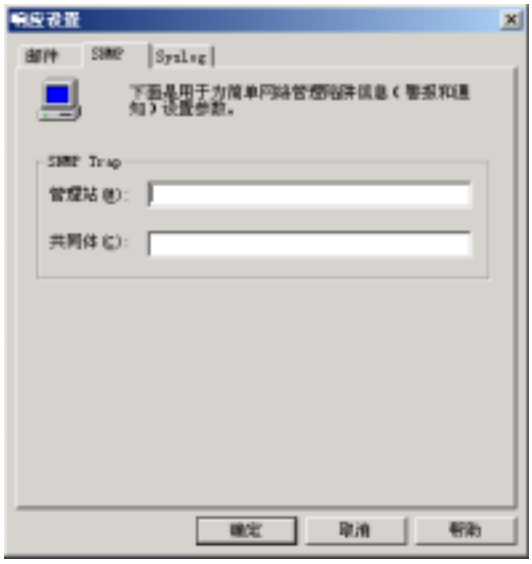
7.4.1 日志功能的使用

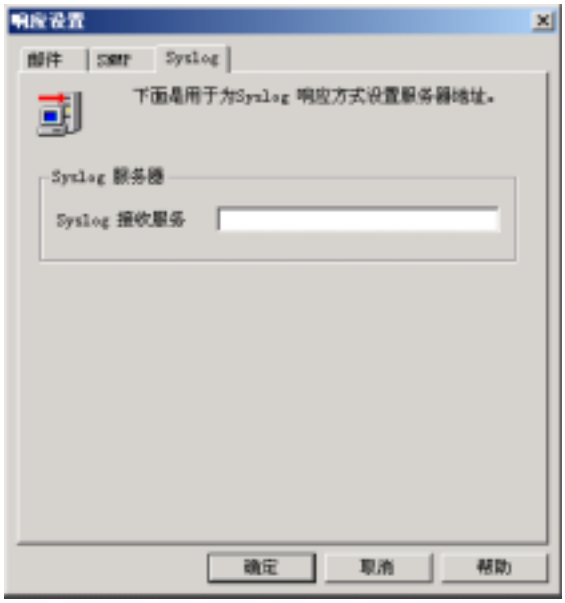
- 首先对需要做日志的行为,在策略主控制界面相应的策略行的响应项,双击,添加日志行为,如下图所示

- 响应类型分为日志、报警、邮件、SNMP、Syslog。响应类型设置：点击主界面 

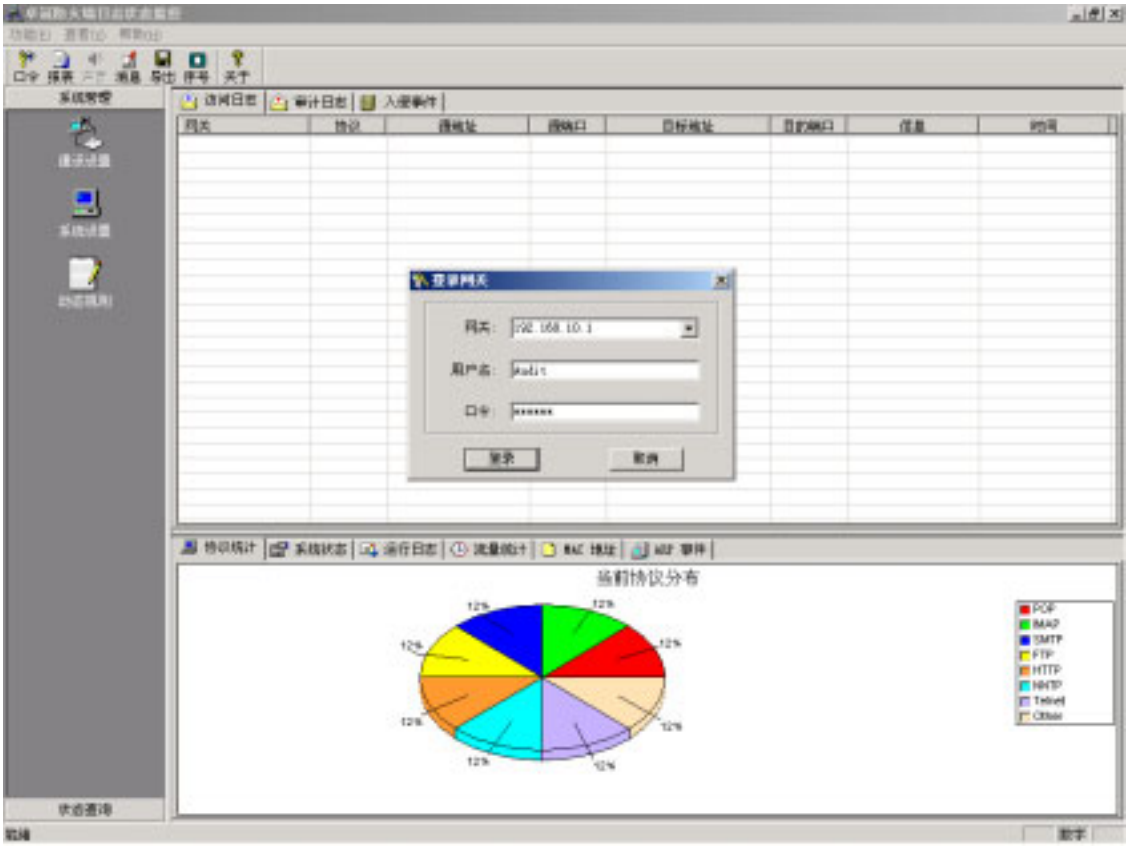
按钮，如下图：

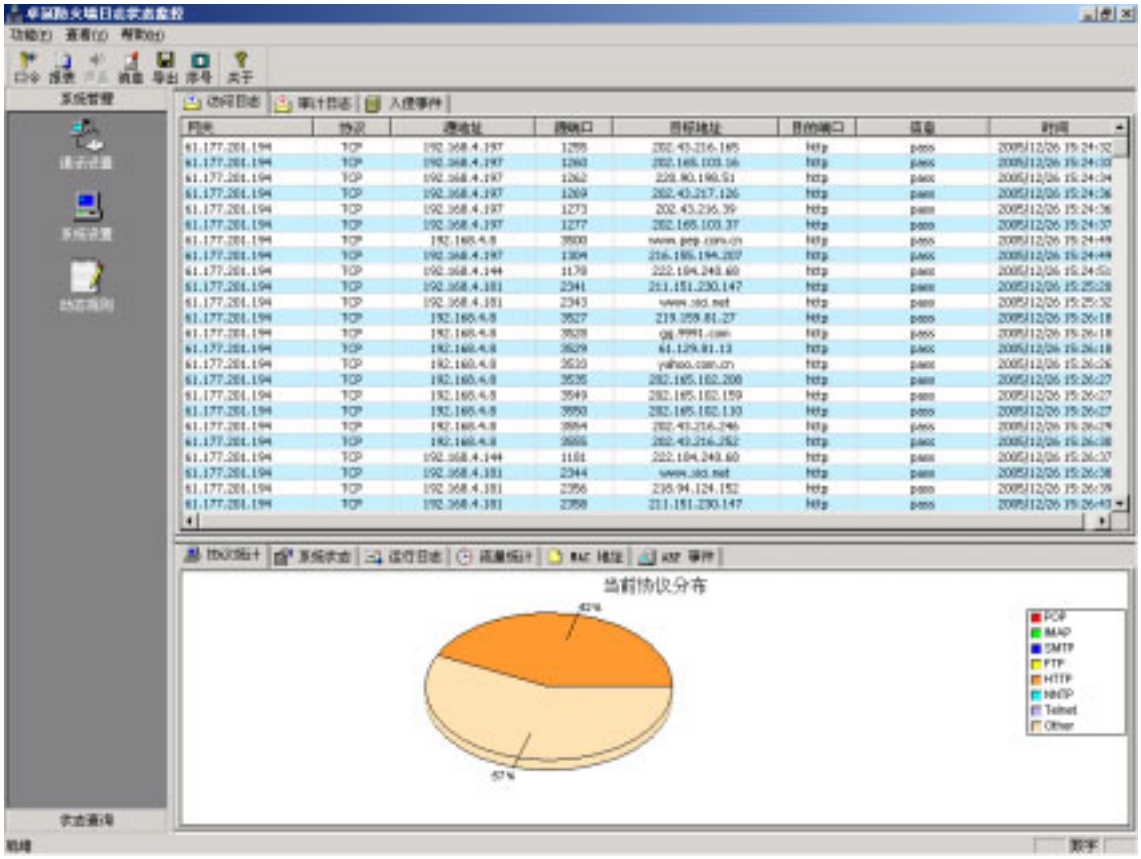






- 依次点击【保存】、【安装】按钮，规则正式生效。
- 打开桌面日志管理端程序,输入缺省用户名 Audit，缺省口令 111111

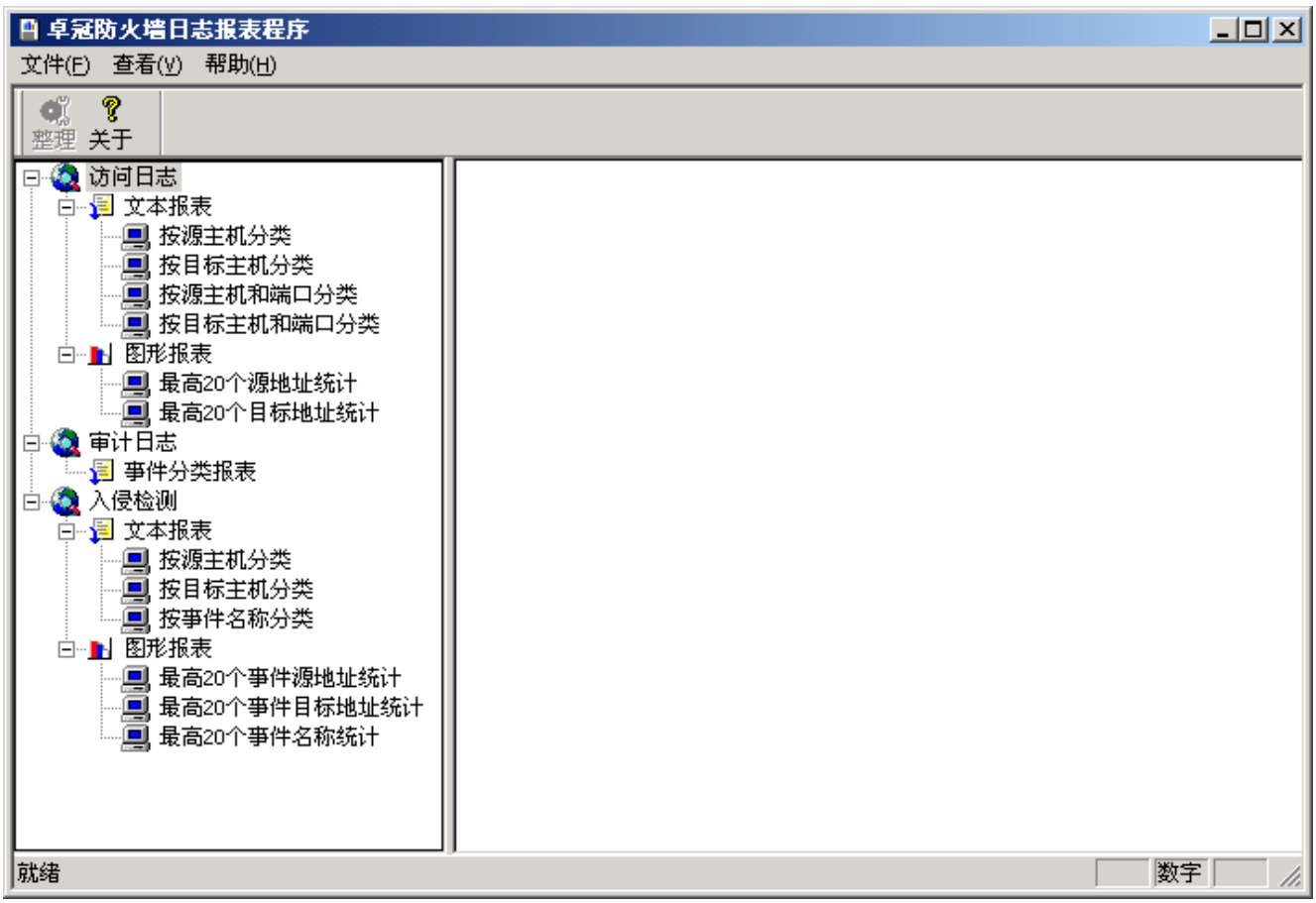




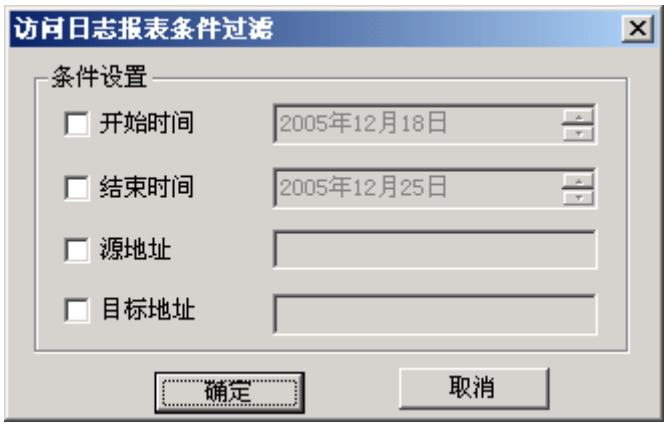
- 由上图可见，相应的 HTTP 日志行为已经记示到本地日志管理端

7.4.2 日志分析工具的使用

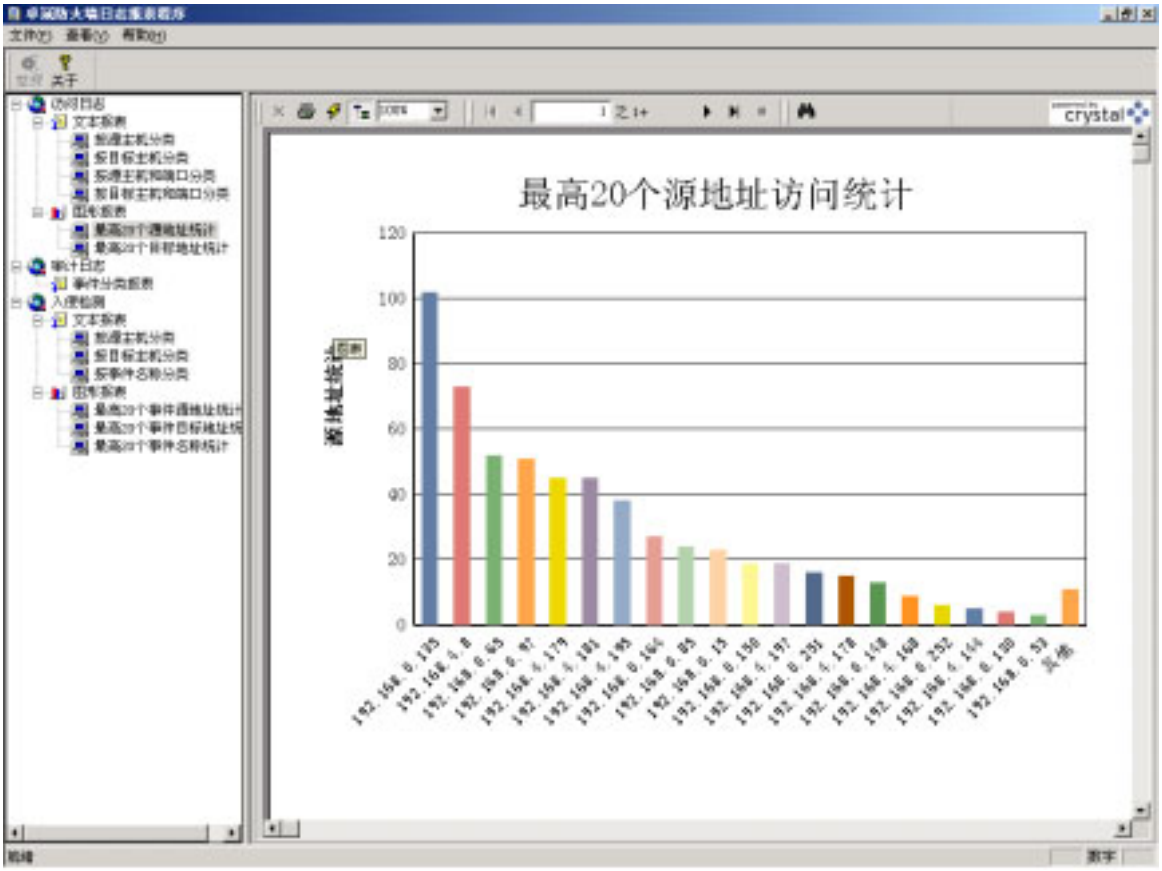
- 首选点日志控制端主界面 报表 按钮，显示如下图界面。

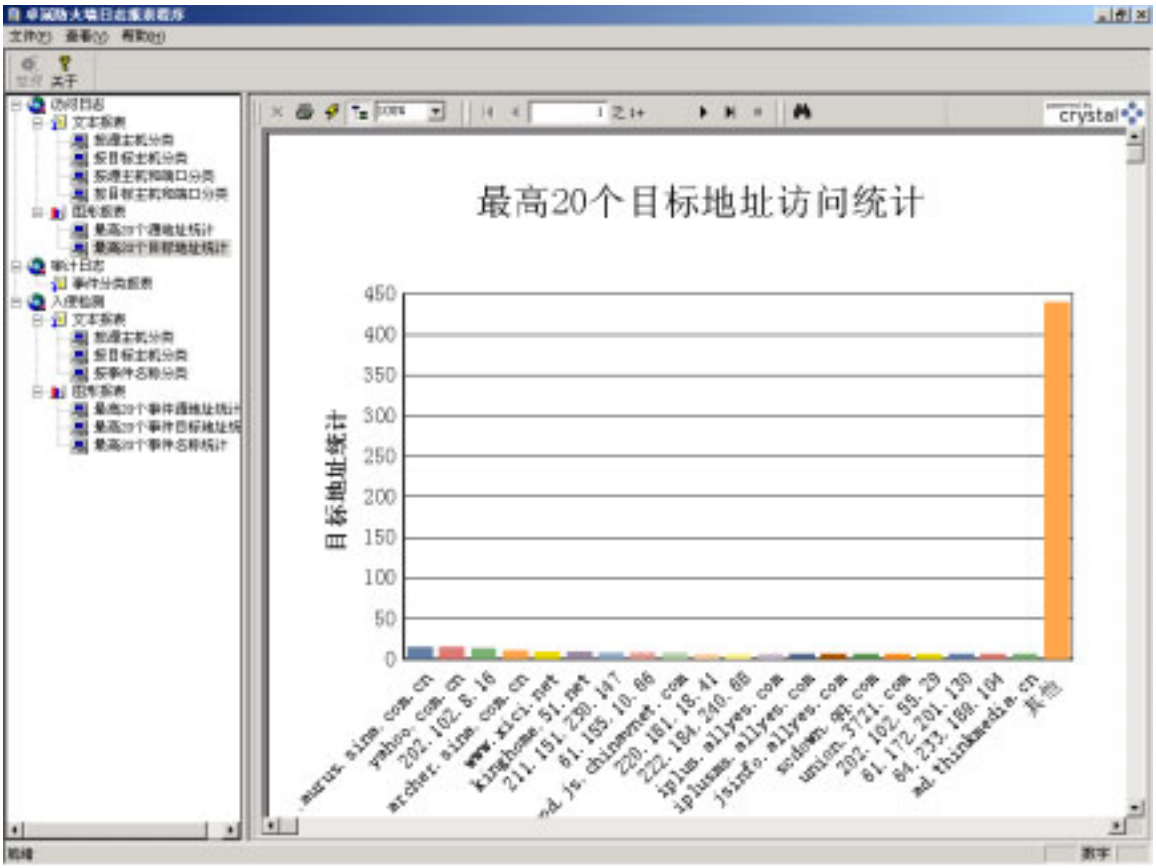


- 点击左边树型菜单栏相应的选项，显示如下条件选择框，输入条件，确认后即可获得相应的图表。




按源地址分类访问统计报表
192.168.0.130
192.168.0.131
192.168.0.135

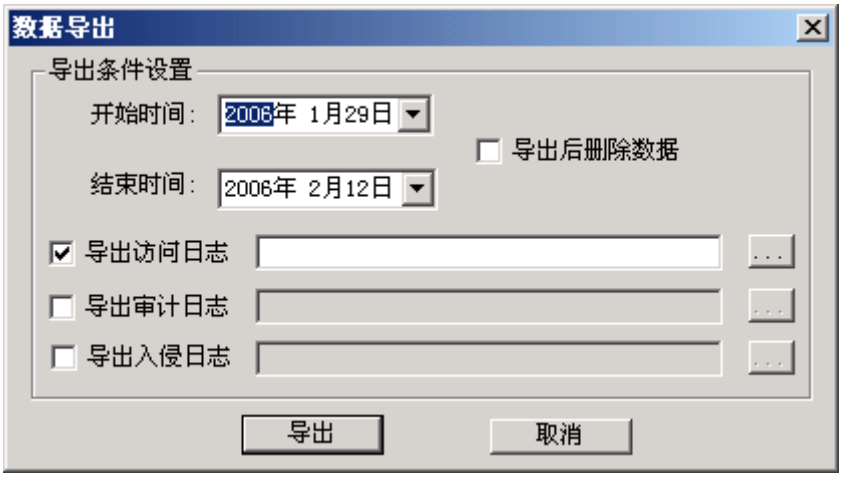

最高20个源地址访问统计
120
100
80
60
40
20
0



7.4.3 日志管理功能的使用

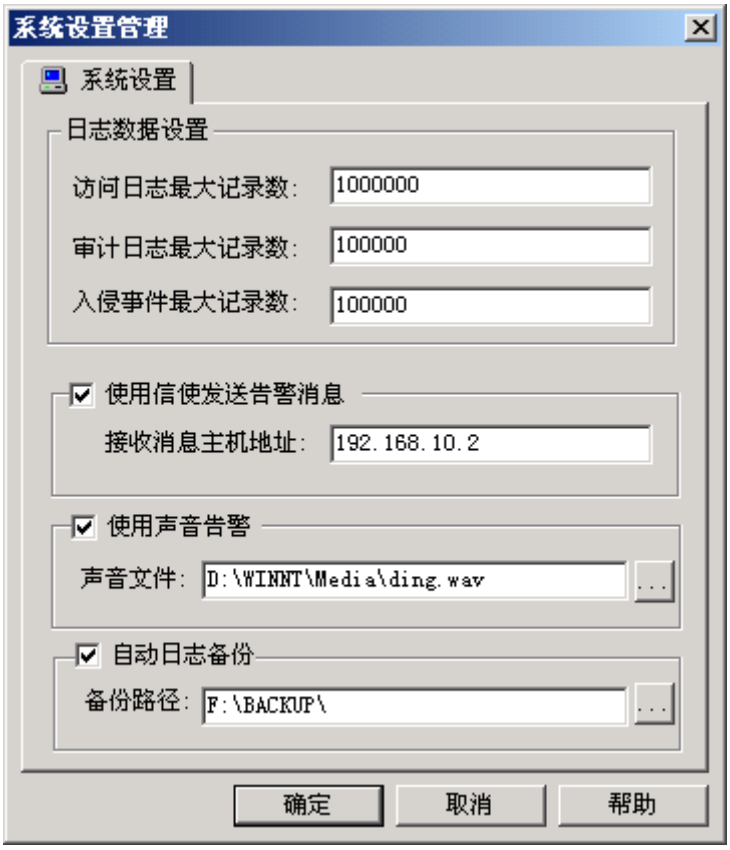
- 创建、存档、删除和清空日志审计记录，本防火墙提供两种日志存档删除的方式。

- 第一种：手工日志导出方式：点击  按钮，显示下图对话框，管理员可设置日志导出的文件名以及导出的时间范围，导出后可选择清空日志。



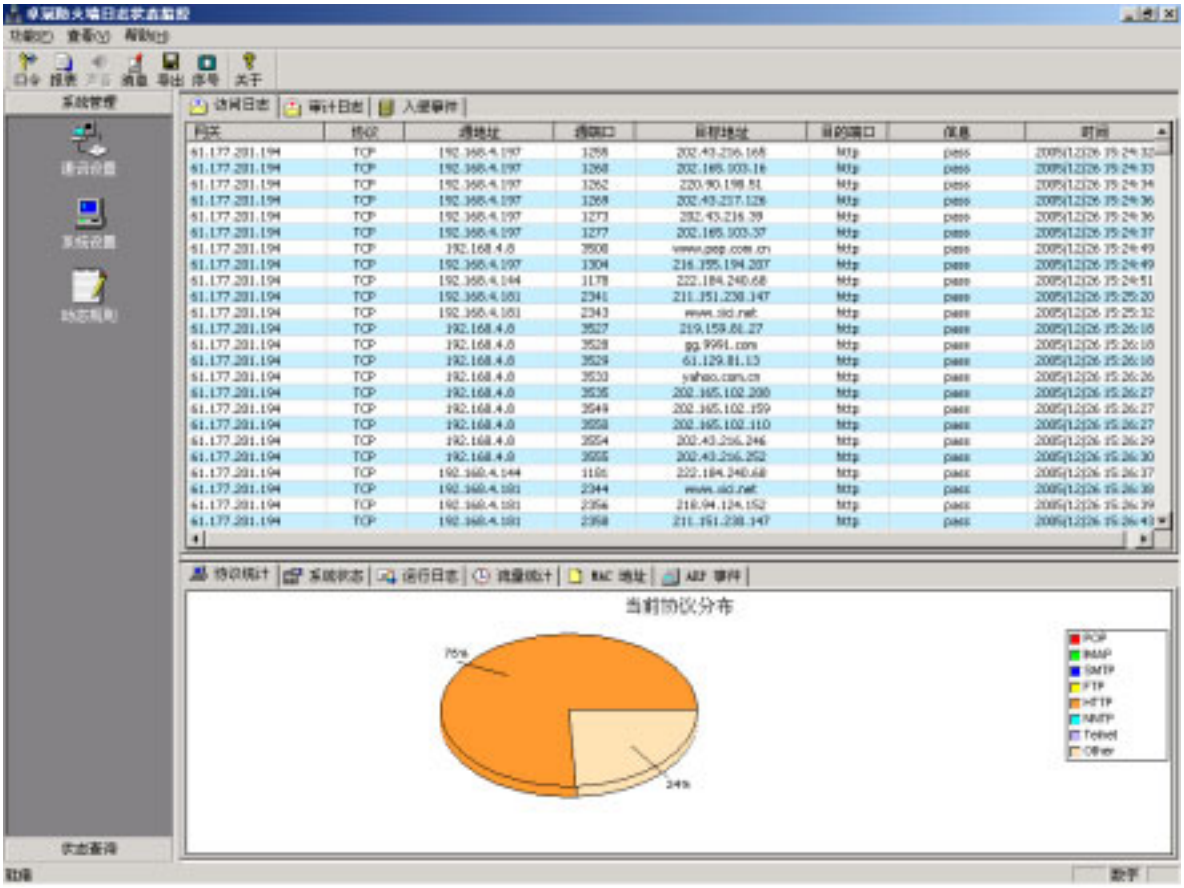
- 第二种：自动日志导出方式：点击  按钮，显示下图对话框，管理员可设置自动日志备份路径。自动备份触发条件由日志数据设置对话框设置。其含义是：当访问日志最大记录数达到 1000000 条时，

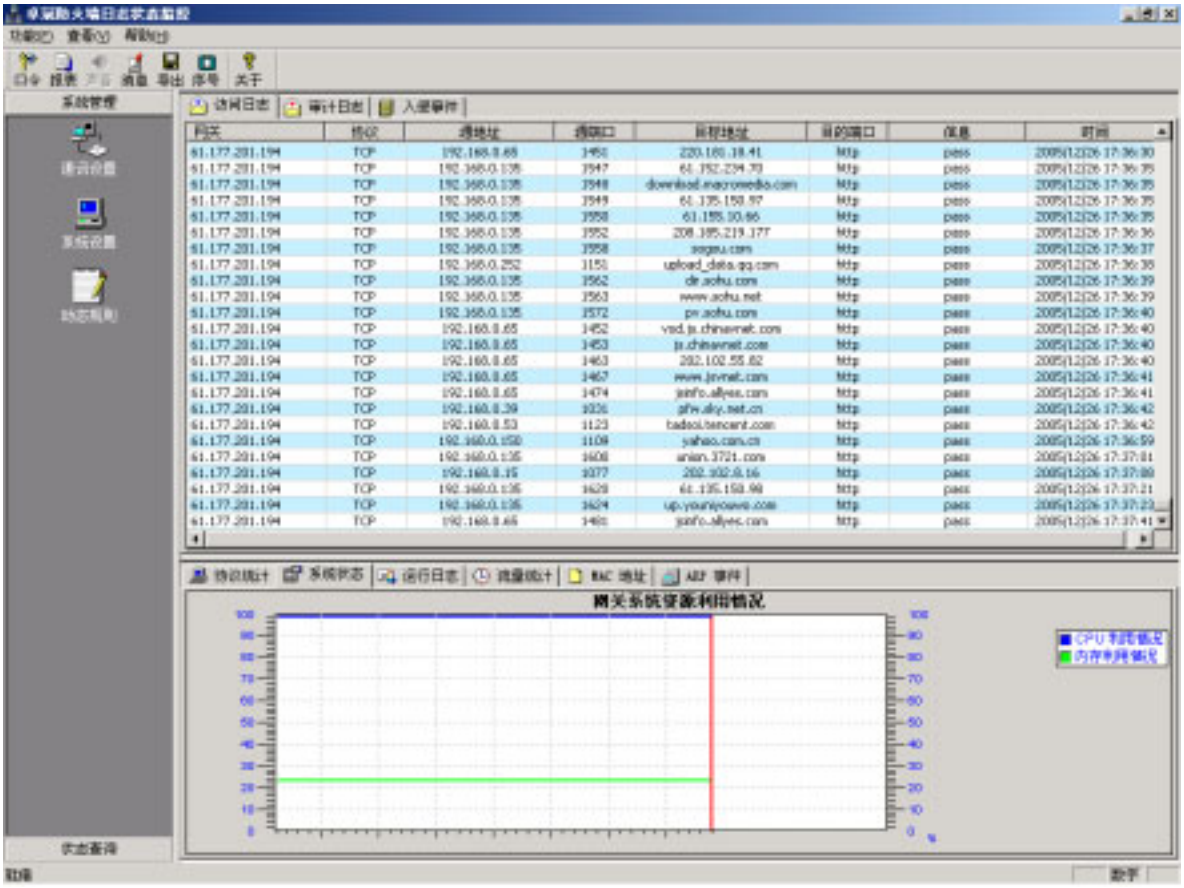
或审计日志最大记录数达到 100000 条时，或入侵事件最大记录数达到 100000 条时，本地日志 ACCESS 数据库将把其库中最前一天的记录以文本文件方式保存到自动日志备份路径下。同时清空 ACCESS 数据库中最前一天的记录。



7.4.4 防火墙的状态监控

- 点击日志状态监控主界面右下部【协议统计】按钮，则显示当前所有接收的日志的协议分布饼图。
- 点击日志状态监控主界面右下部【系统状态】按钮，则显示当前防火墙 CPU 及内存资源使用曲线图。
- 点击日志状态监控主界面右下部【运行日志】按钮，则显示当前日志接收端与防火墙连接建立的时间表。
- 点击日志状态监控主界面右下部【流量统计】按钮，则显示当前所有与防火墙连接的客户端的上行、下行包数、字节数以及其合计数。
- 点击日志状态监控主界面右下部【MAC 地址】按钮，则显示当前所有与防火墙连接的客户端的网卡的 MAC 地址（防火墙内网网广播地址范围内的客户端）。
- 点击日志状态监控主界面右下部【ARP 事件】按钮，则显示自日志状态监控运行开始，防火墙内网网广播地址范围内的客户端同一 IP 地址发生 MAC 变化的事件。


当前协议分布
75%
24%


网关系统资源利用情况