SysKeeper-2000 反向隔离装置(单 bit)用户手册

南京南瑞集团公司信息系统分公司

注意：

本手册中的内容是南瑞安全隔离装置（反向单 bit）用户手册。本材料的相关权利归南瑞集团公司信息系统分公司所有。用户手册的任何部分未经本公司许可，不得转印、影印或复印。

反向隔离装置（单bit）用户手册

Version1.0　2008-2-20

南瑞集团公司信息系统分公司

本资料将定期更新，如预获取最新相关信息，

请访问南瑞集团公司网站：http://www.nari-china.com

您的意见和建议请发送至：sp_support@nari-china.com

南瑞集团公司信息系统分公司

南京南瑞路 8 号，210003

电话（TEL）:025-83096601　025-83096605(市场部)

025-83096702　025-83096712(技术支持)

传真（FAX）:025-83096701

一、产品介绍

SysKeeper-2000 网络安全隔离装置(反向单 bit)的硬件系统基于 RISC 体系结构的嵌入式微处理器(Motorola PowerPC)，双 CPU 之间通过高速传输芯片进行物理连接，两个处理系统不同时连通；主板上分别集成两个以太网接口用来连接要隔离的两个网络，集成一个串口用来连接配置终端，使用户能够方便的配置和监控隔离装置；支持完备的安全事件告警机制，采用标准 Syslog 日志协议输出报警信息；双机接口支持隔离装置的双机热备和链路冗余备份，避免重要数据的丢失；硬件看门狗时刻监控系统状态，保证隔离装置稳定、可靠的运行。

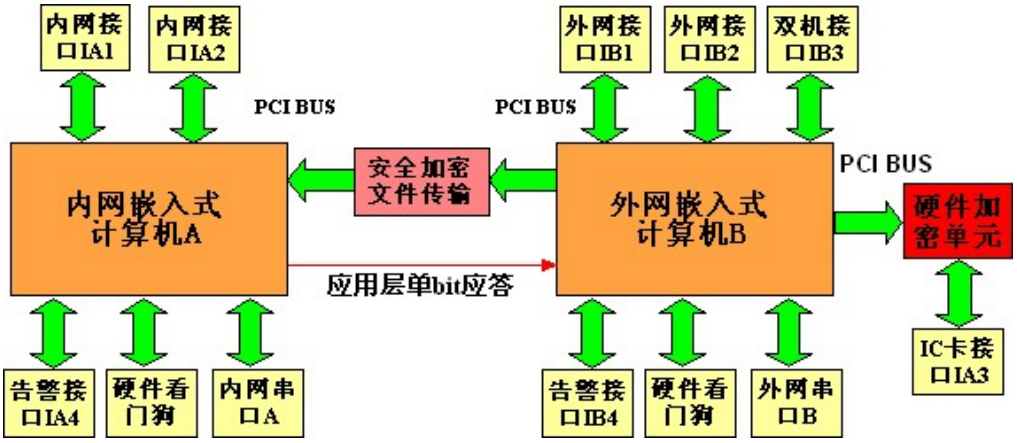

图 1 SysKeeper-2000 网络安全隔离装置(反向型)硬件结构框图

SysKeeper-2000 网络安全隔离装置(反向单 bit 型)的软件系统基于特别裁剪的嵌入式 Linux 内核，实现两个安全区之间的非网络方式的安全的数据交换；取消所有网络功能，采取无 IP 地址的透明监听方式，支持网络地址转换，报文综合过滤，割断穿透性的 TCP 连接；单向数据通信控制，单向连接控制；反向隔离装置采用带签名的 E 语言进行传输，只允许传输采取 E 语言格式书写的文件，装置中对传输的 E 语言文件进行检查，如此便能将病毒文件、非文本文件和非 E 语言文件阻隔，最大限度保障内网高安全区的安全，在更深层次上保证数据传输的机密型和完整性。

反向隔离装置的前面板图如图 2 所示。前面板有 8 个指示灯，分别是电源指示灯、内网灯、外网灯、告警灯、加密卡状态灯、数据加密灯、智能卡读写器状态灯、智能卡读写灯。内网灯亮表示有数据从内网传输到外网；外网灯亮表示有数据从外网传输到内网，如果内外网数据传输的流量太小，可能观察不到内外网灯的闪烁，此时可以根据后面板网卡指示灯的情况观察是否有数据接收和发送。告警灯亮并伴有声音告警表示隔离装置正受到网络恶意攻击。加密卡状态灯亮表示隔离装置内置有数据加密卡，数据加密灯闪烁表示加密卡正在加解密数据；智能卡读写器状态灯闪烁表示隔离装置内置有智能卡读写器，智能卡读写器状态灯亮表示智能卡读写器插槽中有智能 IC 卡，智能卡读写灯亮表示智能卡上的用户数据正在被读取。

图 2　SysKeeper-2000 网络安全隔离装置(反向型)前面板图

后面板图如图 3 所示。隔离装置设计有双电源，一个电源作为主电源供电，另一个作为辅电源备份，两个电源可以在线无缝切换。内网配置口用来监控内网侧的状态信息；外网配置口用来配置反向隔离装置，并监控内网侧的状态信息。内网网口用来连接内网；外网网口用来连接外网。内外网口的网卡指示灯绿灯亮表示网口与网络正确连接；黄灯亮表示网络速率是 100M，暗表示网络速率是 10M，闪烁表示有数据正在接收或发送。双机接口支持隔离装置的双机热备。告警接口支持使用专用协议输出报警信息。

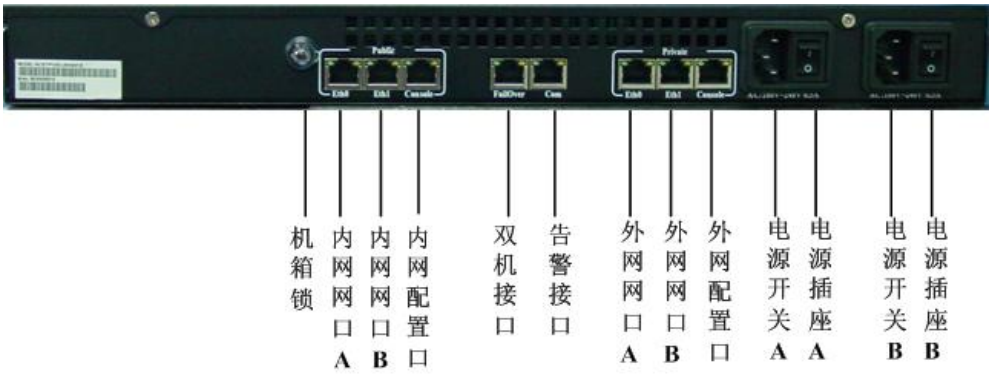

图 3 SysKeeper-2000 网络安全隔离装置(反向型)后面板图

二、产品分发与安装

SysKeeper-2000 网络安全隔离装置(反向型)完整的产品分发包包括硬件和软件两大部分。用户在使用本产品时，应先检查产品是否具有 NARI 标志，外观是否有损坏现象。如有以上现象，请勿使用并及时与本公司取得联系，处理相关事宜。为了产品稳定、可靠的运行，请勿私自打开隔离装置机箱。

隔离装置随机带有一张配置软件安装光盘和一根串口配置线，用于在安装 Windows2000/XP/2003/NT/9x 操作系统的计算机上配置隔离装置。

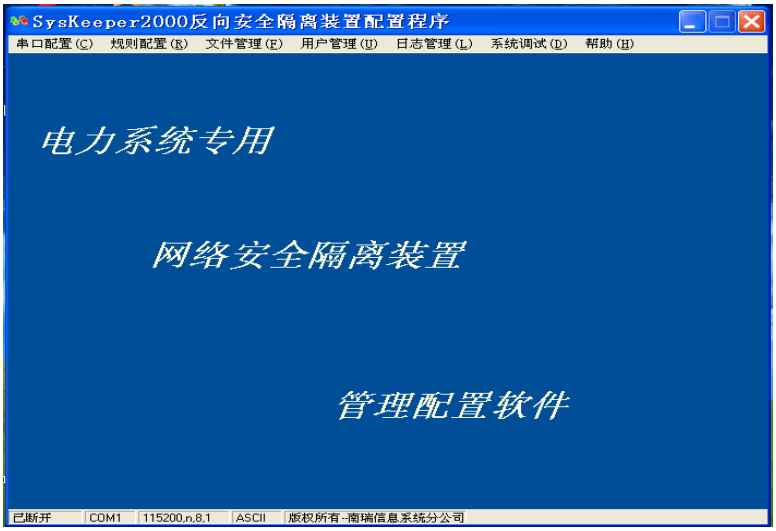

图 4　反向隔离装置配置软件主界面

SysKeeper-2000 网络安全隔离装置的安装和部署非常简单，隔离装置部署在网络的唯一出口处，通过内网接口和外网接口，分别与内网和外网相连。内网和外网的数据交换必须通过隔离装置，以便保护安全的内部网络。

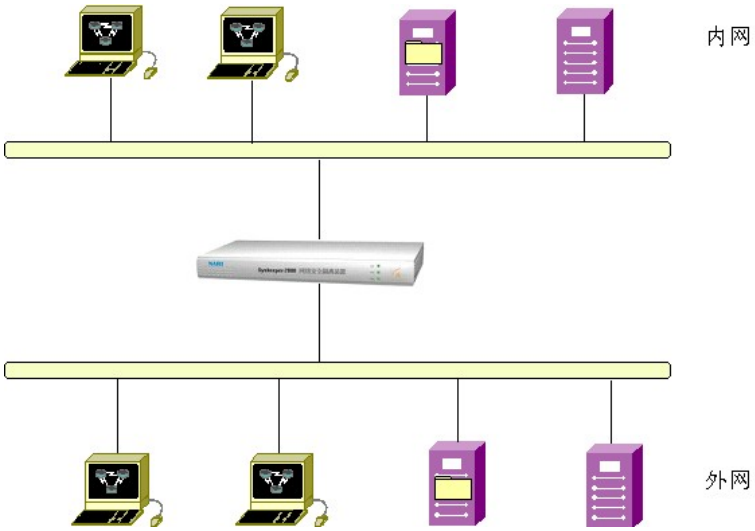

图 5　隔离装置安装网络拓扑图

三、配置隔离装置

3.1 规则配置

1、由于隔离装置的配置是通过配置终端的串口与隔离装置进行通讯的，所以首先必须配置终端串口。使用随机附带的串口配置线将配置终端的串口与隔离装置的**外网配置口(Console)**连接起来。然后点击‘**串口配置**’菜单，在‘**端口**’选项下选择串口的 COM 端口(图 6)。

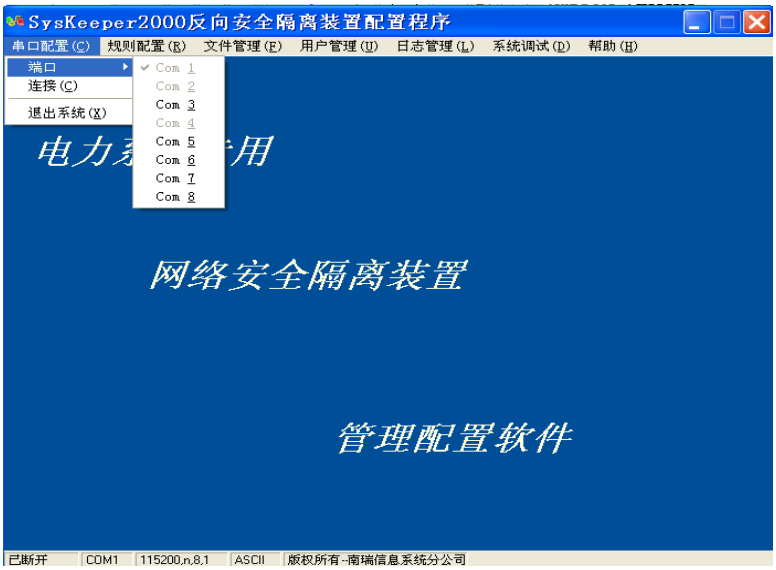

图 6

2、点击‘**连接**’选项。如果连接成功，系统将会提示成功连接串口(图 7)；如果连接失败，系统也会提示连接串口失败(图 8)。程序会反复重连 5 次，5 次都失败后，程序会自动退出。用户应该参考《附录 5.1 串口故障诊断》一节仔细检查串口设置。排除故障后，再次重试连接。

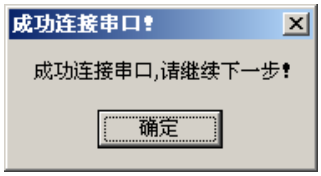

图 7

图 8

3、点击‘**规则配置**’菜单下的‘**配置规则**’选项(图 9)，系统会提示输入用户名和口令(图 10)进行权限认证。隔离装置默认的系统管理员用户名/口令是**root/root**。**用户在使用隔离装置后，请立刻修改系统管理员口令。**

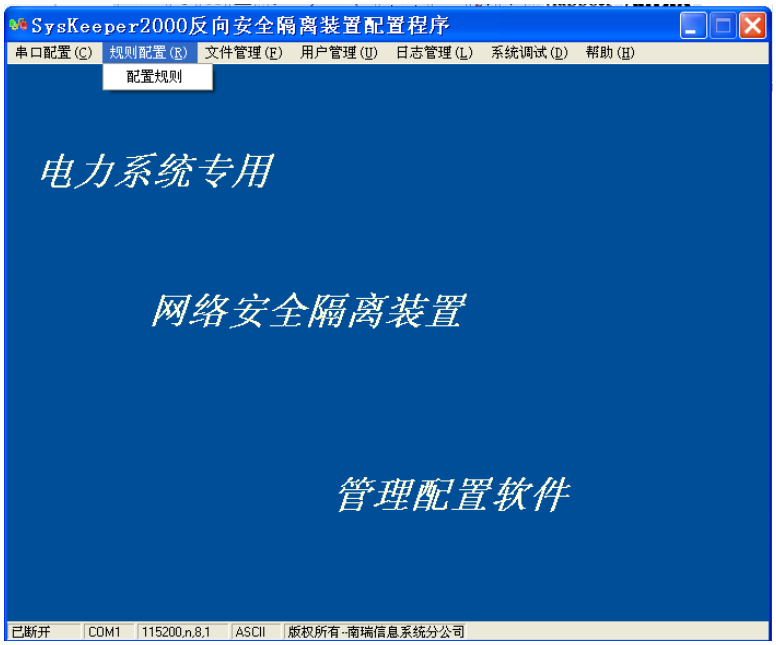

图 9

图 10

4、用户登录成功后，隔离装置会自动导出已存在的配置规则(图 11)，导出成功后进入‘配置系统规则’主界面(图 12)配置用户规则。**(注意：从安全角度考虑，本地不保留规则配置文件，每次启动时都从隔离装置导出)**

图 11

图 12

数据综合过滤功能能够为隔离装置提供基本的安全保障，根据系统管理员预先设定的规则检查数据包以决定哪些数据容许通过，哪些数据不能通过，这样可以保护内部安全网络不受外部攻击，为内部安全网络提供基本的安全保障。

数据过滤依据：

- 数据包的源端地址，目的端地址。
- 数据包的源端口号，目的端口号。
- IP 地址和 MAC 地址是否绑定。

综合过滤规则提供网络安全隔离装置允许还是拒绝 IP 包的依据,隔离装置对收到的每一个数据包进行检查，从它们的包头中提取出所需要的信息，如源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议类型等，再与已建立的规则逐条进行比较，并执行所匹配规则的策略，或执行默认策略。

规则配置中，IP 地址的形式为 X.X.X.X，X 的范围取 0-255。端口配置内网侧服务端监听的端口。虚拟路由选择此条规则是否是虚拟路由规则。网卡可以选择 eth0、eth1,分别对应隔离装置上的 eth0、eth1 两个以太网口。

常用操作步骤说明

- **添加**

  增加新的规则。当用户增加了新的规则后，点击‘**添加**’按钮即可将规则添加到配置软件的规则队列中。

- **修改**

  对已有的规则进行编辑修改。选择要修改的规则，修改规则中的参数后，点击‘**修改**’按钮，确认修改；否则不会保存修改过的参数。

- **删除**

  删除一条已有的规则。选择要删除的规则，点击‘**删除**’按钮，则选定的规则将被删除；如果需要删除全部规则，点击‘**删除全部**’按钮即可。特别需要注意的是，在规则删除完成后，须点击‘**保存**’按钮，然后点击‘**导入装**

置’按钮，这样才能正真将隔离装置中的相应规则删除。

- **复制**

根据一条已有的规则复制出一条新的规则。选择要复制的规则，点击‘**复制**’按钮，会复制出一条与原规则相似的规则，所不同的是规则名称。在复制规则中修改相应的各项内容。修改完毕后，点击**‘修改’**按钮确认修改。

- **保存**

保存操作收集各个参数的输入数据，将规则文件保存到配置终端的内存中，还能够将规则保存在本地用户指定的规则文件中。当用户对隔离装置的规则配置完成后，点击**‘保存配置’**按钮，提示用户已保存的规则总数并将规则文件保存在配置终端内存中。如果需要保存在本地用户指定的规则文件中，点击**‘保存本地’**按钮，将规则保存在本地的规则文件中。

- **导入**

将规则文件导入到隔离装置。在规则配置完成后，点击**‘保存配置’**按钮，保存规则文件。然后点击**‘导入装置’**按钮，将规则导入到隔离装置的安全存储区中。

- **导出**

导出存储在隔离装置内的规则配置文件。点击**‘装置导出’**按钮，出现导出系统规则进度条。导出规则成功后，系统会提示成功导出规则并保存，此时规则文件保存在配置终端的内存中。

- **载入**

载入存储在配置终端上的规则配置文件。点击**‘本地载入’**按钮，弹出规则配置文件选择对话框选择正确的配置规则文件。

5、所有的规则配置完成后，首先点击‘**保存配置**’按钮将配置文件保存到配置终端的内存中，然后点击‘**导入装置**’按钮将规则导入到隔离装置内以完成规则配置。导入成功后，系统会提示“已成功导入，请重新启动”,重新启动隔离装置使配置规则生效。**(注意:只需在外网配置口进行规则配置即可)**

注意：系统默认拒绝所有网络报文通过，只有在规则配置中允许的报文才可以通过。隔离装置不容许出现重复规则，当两条规则的重复时，会出现报警信息，提醒用户对规则进行修改。根据不同的隔离方案，规则有不同的配置，请参考《四、典型应用隔离方案规则设定范例》。

3.2 文件管理

1、反向隔离装置对传输的文件采用硬件智能 UsbKey 完成数字签名等操作，关于证书的生成请参见附录《UsbKey 的 API 使用指南》部分。点击‘**文件管理**’菜单下的‘**导入证书**’选项来导入 UsbKey 的数字证书。

2、如果传输的是 E 语言文件，反向隔离装置需要 E 语言的模式文件来对传输的 E 语言文件进行检查，E 语言的模式文件由使用者提供，具体格式请参见附录的《电力系统数据标记语言-E 语言规范(企标版)》部分。点击‘文件管理’菜单下的‘导入模式文件’选项来导入模式文件。

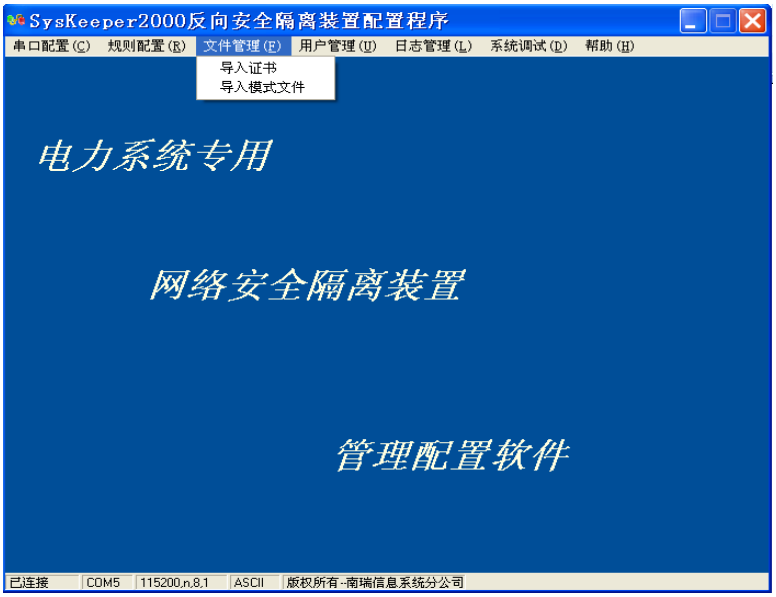

图 13

3.3 用户管理

为了更好地管理隔离装置，在隔离装置中可以设置两类用户：超级用户和普通用户。超级用户和普通用户的权限不同：超级用户可以增加、删除、修改隔离

装置的配置规则，可以增加或删除隔离装置的普通用户，可以查询隔离装置的日志等；普通用户只可以查看隔离装置的配置规则和日志等。**（注意：隔离装置现在只能设置一个超级用户 root）**

1、点击**‘用户管理’**菜单下的**‘修改口令’**选项修改用户口令(图 14)，用户必须首先登录以验证合法身份(图 15)。登录成功后，系统会自动弹出**‘修改口令’**窗口(图 16)，同时系统会自动锁定当前已经登录的用户名，用户只需输入新口令修改口令即可。**（注意：用户只需要登录隔离装置一次，只要与隔离装置的连接没有断开，登陆的用户权限一直有效）**。

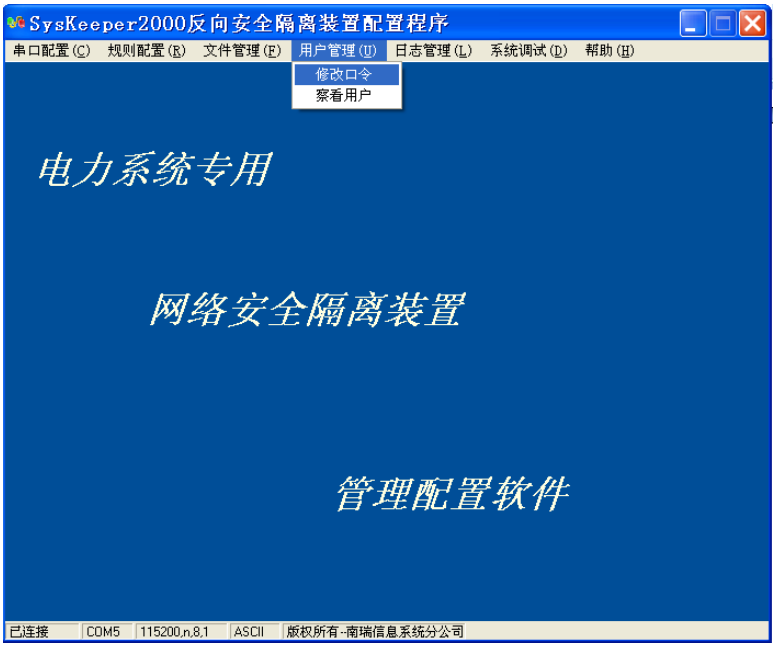

图 14

图 15

图 16

2、点击**‘用户管理’**菜单下的**‘察看用户’**选项察看用户(图 17)。察看用户需要使用超级用户 root 身份登录(图 18)。登录成功后，会出现导出用户列表进度条(图 19)。导出成功后会自动弹出**‘用户列表’**窗口(图 20)，超级用户在这里可以添加或删除普通用户。添加或删除用户后，系统会自动更新用户列表。**(注意：系统禁止删除超级用户 root)**

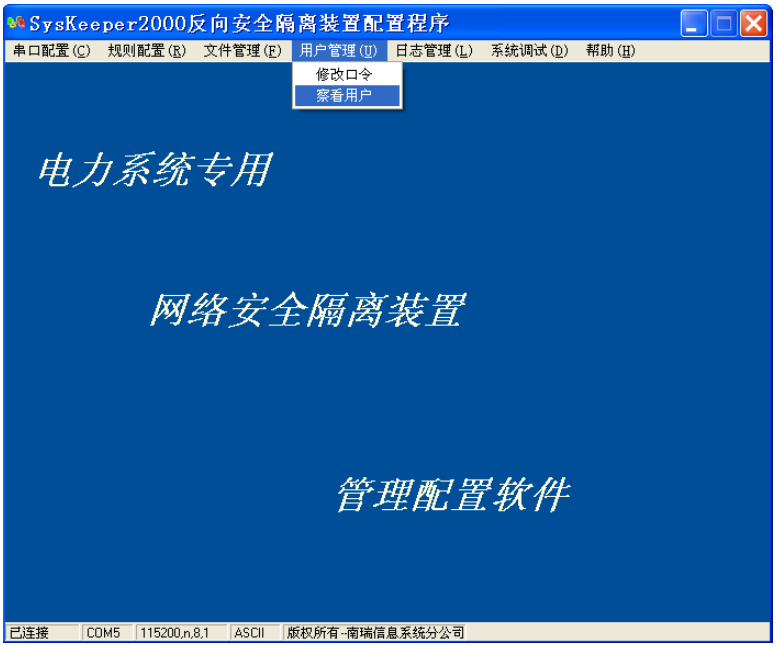

图 17

图 18

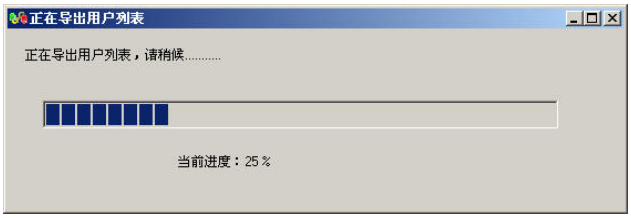

图 19

图 20

3.4 日志管理

‘日志管理’功能(图 21)查看隔离装置的运行日志，以供用户分析隔离装置的运行状况。登录成功后，会出现导出日志进度条(图 22)。导出成功后会自动弹出**‘日志列表’**窗口(图 23)。

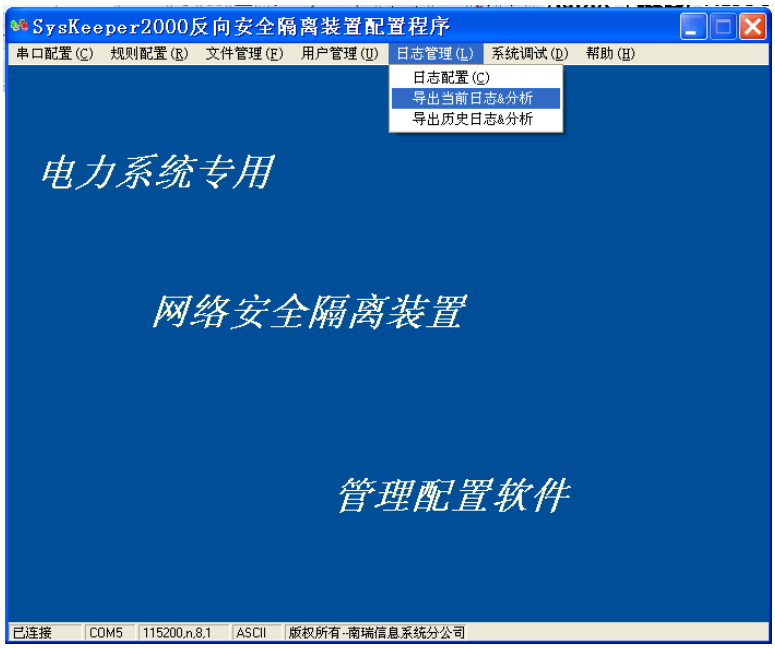

图 21

图 22

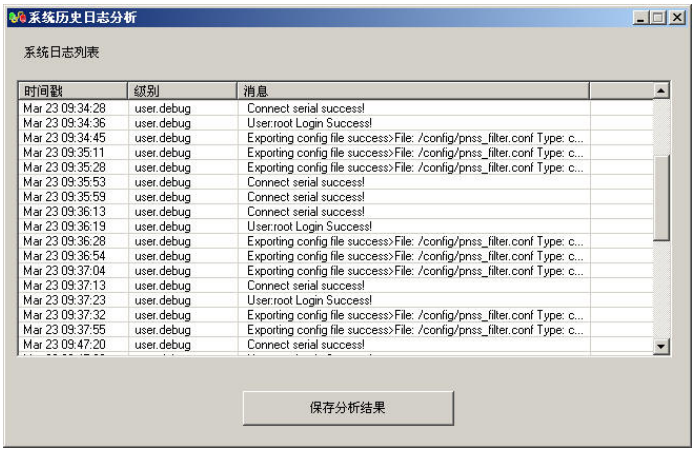

图 23

隔离装置也可以将系统日志输出到用户指定的计算机上保存。具体使用方法参考《附录 5.3 日志审计系统》。

3.5 系统调试

隔离装置提供了一个非常实用的系统诊断工具，用来诊断隔离装置与网络的连接是否正常。点击**‘系统调试’**菜单下的**‘系统诊断工具’**选项诊断网络连接情况(图 24)。

1） Ping 诊断命令：

“诊断命令”提供了“ping”命令。由于隔离装置没有 TCP/IP 协议栈，所以这个命令不是 Unix/Linux 下常用的调试网络的命令，而是采用专用报文构造的一个仿 ping 命令，用来诊断隔离装置是否与内外网络物理连接正常。

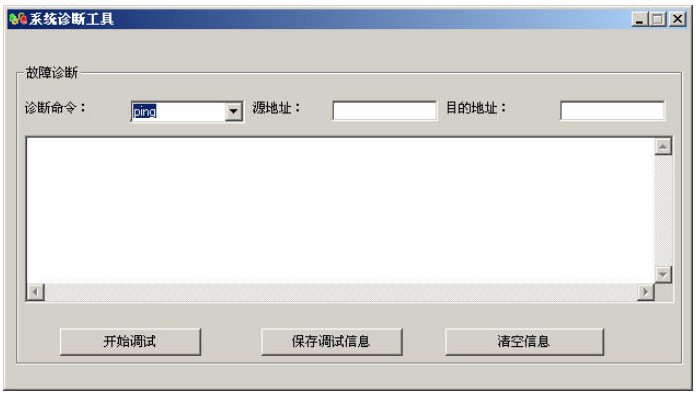

图 24 系统诊断工具

以下是一个网络连接诊断示例：

图 25 网络连接诊断示例图

内网主机真实地址为 10.144.1.1,虚地址为 202.102.1.2；外网主机真实地址为 202.102.1.1,虚地址为 10.144.1.2。假设隔离装置与内外网络已经连接好,并且在隔离装置内已经配置好规则。

具体诊断步骤如下所述:

a、首先测试隔离装置与内网的连接是否正常。将配置串口线连接到隔离装置的内网配置口,连接串口成功后,选择系统诊断界面中的 ping 命令,源地址输入**外网主机的虚地址**,目的地址输入**内网主机的真实地址**。本例中源地址输入 10.144.1.2,目的地址输入 10.144.1.1。

b、点击**‘开始调试’**按钮,系统会提示正在导出系统调试信息。如果诊断信息为 ping success: 10.144.1.1 to 10.144.1.1,则表示隔离装置与内网网络连接正常(图 26)。否则诊断信息应为 ping error。

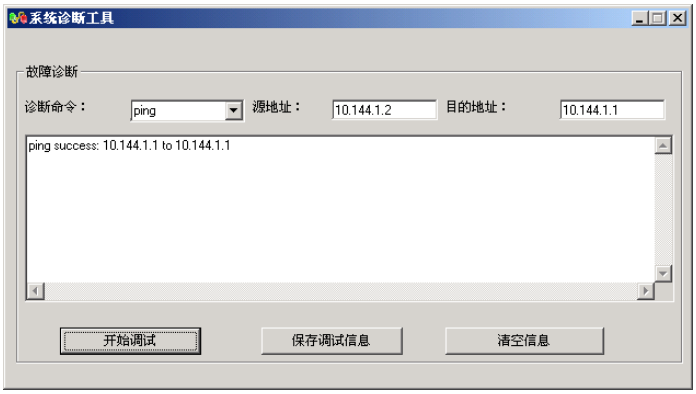

图 26 网络连接诊断结果

c、测试隔离装置与外网的连接是否正常,与测试内网连接类似。将配置串口线连接到隔离装置的外网配置口，源地址应该输入**内网主机的虚地址**(202.102.1.2)，目的地址输入**外网主机的真实地址**(202.102.1.1)。

2) **远程 Ping 诊断命令：**

为了方便用户进行网络链路诊断，隔离装置支持有限的远程 ping 诊断。具体诊断步骤如下所述：

a、首先测试隔离装置与内网的连接是否正常。在内网通信计算机（如上图所示的计算机 10.144.1.1）上打开命令行窗口，运行 ping 命令，目标地址为外网的虚拟 IP 地址(10.144.1.2),ping 命令的长度选择为 996 个字节。

Windows 操作系统：ping 10.144.1.2 －l 996

Unix 操作系统：ping 10.144.1.2 －s 996

如果能 ping 通外网的虚拟地址，则表示隔离装置与内网网络连接正常。否则请检查隔离装置与内网的网络连接。

b、测试隔离装置与外网的连接是否正常,与测试内网连接类似。在外网的通信计算机（如上图所示的计算机 202.102.1.1）上打开命令行窗口，运行 ping 命令，目标地址为内网的虚拟 IP 地址（202.102.1.2），ping 命令的长度选择为 996 个字节。如果能 ping 通内网的虚拟地址，则表示隔离装置与外网网络连接正常，否则请检查隔离装置与外网的网络连接。

四、典型应用隔离方案规则设定范例

4.1 两个网络通过二层交换机连接

网络环境描述：

内网主机为服务端，IP 地址为 192.168.0.1，虚拟 IP 为 10.144.0.2；外网主机为客户端，IP 地址为 10.144.0.1，虚拟 IP 为 192.168.0.2，假设 Server 程序数据接收端口为 9898,隔离装置内外网卡都使用 eth0。在二层交换的环境下，通信规则的配置原则如下：外网虚拟 IP 地址须与内网 IP 地址为同一网段，内网虚拟 IP 地址须与外网 IP 地址为同一网段，且虚拟地址必须在真实网络环境中没有被其它的主机和业务系统占用。

图 27

实际通信规则配置：

图 28

注意：如果隔离装置两边主机是同一网段，虚拟IP地址与真实的IP地址相同。例如主机C(10.144.100.1)，与主机D(10.144.100.2)进行通信，此时可以把主机C的虚拟IP地址设置为 10.144.100.1，主机D的虚拟IP地址设置为 10.144.100.2。

4.2 两个网络通过路由器连接

网络环境描述：

内网主机为服务端，IP 地址为 192.168.0.5；外网主机为客户端，IP 地址为 10.144.0.6, 假设 Server 程序数据接收端口为 8000，隔离装置内外网卡都使用 eth0。路由器为内外网之间的网关，路由器与隔离装置内网口连接的网段的网关地址为 10.144.0.1。此这种网络环境下进行规则配置时，需要同时配置两条规则：一条规则为外网主机与内网主机之间**实际通信规则**，另外一条为**虚拟路由规则**。

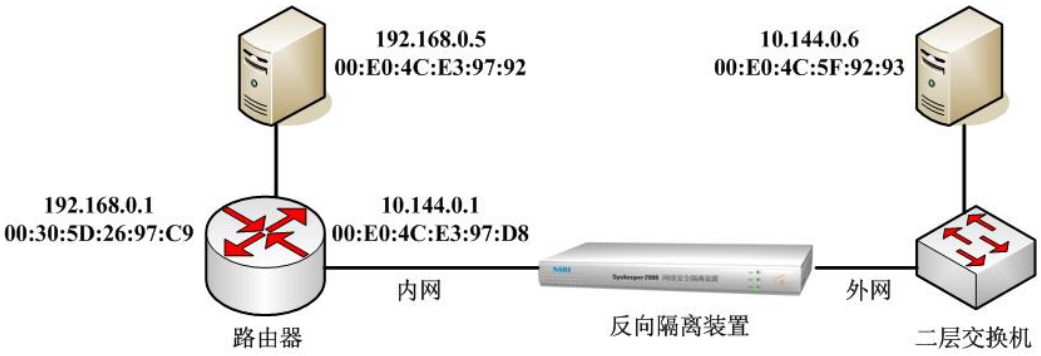

图 29

在路由环境下，通信规则的配置原则如下：在隔离装置的外网侧为二层交换环境，因此配置规则与上例二层环境的配置相同，即外网的 IP 地址与内网的虚拟 IP 为同一网段（本例内网虚拟 IP 地址配置为 10.144.0.3）；在隔离装置的内网侧为路由环境，外网的虚拟 IP 必须与隔离装置内网侧相连接的路由器网段为同一网段（本例外网虚拟 IP 地址配置为 10.144.0.2）。

实际通信规则配置：

图 30

虚拟路由规则的配置原则如下：与路由器相连接侧必须设置虚拟路由选项，

本例中需在隔离装置的内网侧设置虚拟路由选项，即将相应的内网虚拟路由选项选则为“是”，对应的外网虚拟 IP 设置为路由器的网关地址（本例中配置为 10.144.0.1）；外网虚拟路由选项选择为“否”，对应的内网虚拟 IP 与通信规则中相同（本例中配置为 10.144.0.3）。

虚拟路由规则：

图 31

注意：如果隔离装置的内网侧为三层交换机（启用路由功能），外网侧为二层交换机环境，则规则的设置与上述路由环境完全一致。

4.3 两个网络通过三层交换机连接

网络环境描述：

内网 101 号网段主机为服务端，IP 地址为 **192.1.101.1**，外网 1 号网段主机为客户端，IP 地址为 **172.17.1.104**，假设内网 Server 程序数据接收端口为 **9898**，隔离装置内外网卡都使用 eth0。内网划分为 2 个网段（20 号网和 101 号网），外网也划分为 2 个网段（1 号网和 4 号网），三层交换机做了路由使得这两个网段可以互通。隔离装置的内网口与内网 20 号网段相连，连接端的三层交换机网关地址为 **192.1.20.254**；隔离装置的外网口与外网 4 号网段相连，连接端的三层交换机网关地址为 **172.17.4.16**。在规则设置时，需要设置两条规则：第一条规则为外网主机与内网主机实际通信的规则。另外一条为**虚拟路由规则**，在与隔离装置相连接侧，必须设置虚拟路由规则，本例中需在隔离装置的内网侧和外网侧，同时设置虚拟路选项，即将相应的虚拟路由选项都设置为“是”。

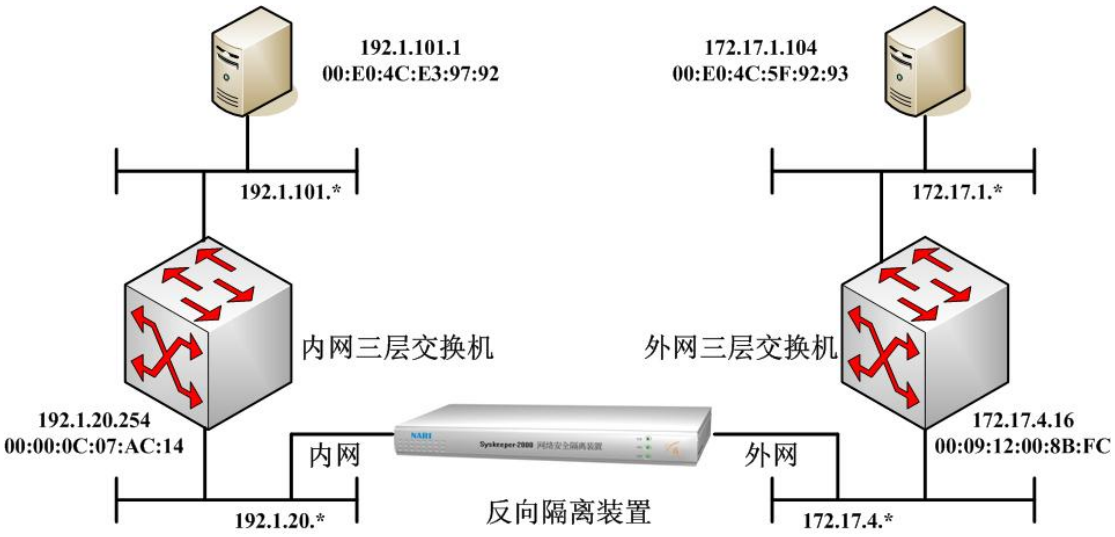

图 32

在三层交换环境下，通信规则的配置原则如下：在隔离装置的内、外网侧均为三层路由交换环境，外网的虚拟 IP 地址必须与隔离装置内网侧相连接的三层交换机网段为同一网段(本例中外网 1 号网段主机 **172.17.1.104** 的虚拟 IP 设置为内网 20 号网段的 IP 地址 **192.1.20.31**)；内网的虚拟 IP 地址必须与隔离装置外网侧相连接的三层交换机网段为同一网段（本例中内网 101 号网段主机 **192.1.101.1** 的虚拟 IP 设置为外网 4 号网段的 IP 地址 **172.17.4.31**)。

实际通信规则配置：

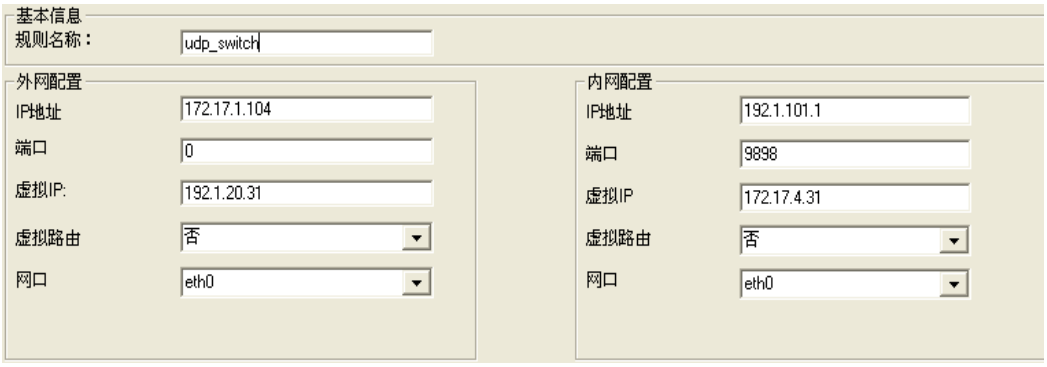

图 33

虚拟路由规则的配置原则如下：与三层交换机相连接侧必须设置虚拟路由选项，本例中需在隔离装置的内外网侧同时设置虚拟路由选项，即将相应的内、外网虚拟路由选项选则为“是”，内网对应的外网虚拟 IP 设置为与隔离装置内网侧相连接的三层交换机网关地址（本例中配置为 192.1.20.254)；外网对应的内网虚拟 IP 设置为与隔离装置外网侧相连接的三层交换机网关地址（本例中配置为

172.17.4.16)。

虚拟路由规则配置：

图 34

4.4 两个网络通过二层交换机双机双网连接

网络环境描述：

内网主机为服务端，两块网卡的 IP 地址为 192.168.0.8/192.168.1.8，虚拟 IP 分别设置为 10.1.0.9/10.1.1.9；外网主机为客户端，两块网卡的 IP 地址为 10.1.0.8/10.1.1.8，虚拟 IP 分别设置为 192.168.0.9/192.168.1.9，同网段的 IP 相互通讯，程序默认通过 0 号网段通讯，0 号网段不通的情况下切换到 1 号网段进行通讯。两台隔离装置双机热备（采用交叉连接线将外网双机热备接口 Failover 连接起来），配置规则相同。假设 Server 程序数据接收端口为 9898。

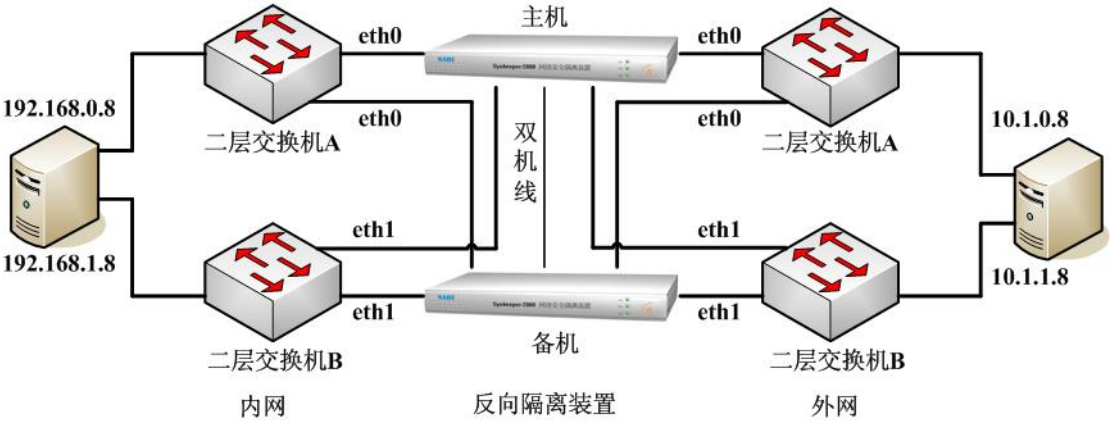

图 35

在二层交换双机双网的环境下，通信规则的配置原则如下：热备份主机和备机的配置规则完全相同。在主备机的配置规则中，需要配置两条实际通信规则，

一条规则通过 eth0 接口进行通信，另外一条通过 eth1 接口进行通信，具体的虚拟 IP 设置可以参考二层交换机环境下单隔离装置通信规则配置原则。

实际通信规则配置 1：

图 36

实际通信规则配置 2：

图 37

五、附录

5.1 串口故障诊断

用户在配置隔离装置的时候，如果出现串口连接反复失败的情况，可能是由于以下原因造成，请按照以下步骤对串口进行诊断：

1、串口的 COM 端口选择不正确。查看串口配置线与计算机的哪一个串口连接。一般来说计算机自带的串口 A 为 COM1，串口 B 为 COM2。如果是使用串口卡或 USB 转串口线额外增加的串口，需要打开“设备管理器”，在端口选项下具体查看串口使用的 COM 端口，确认 COM 端口选择正确。

2、隔离装置配置串口故障。将超级终端的速率设置为‘115200’，数据流控制设置为‘无’。重新启动隔离装置，在超级终端窗口观察隔离装置的启动信息。如果能够观察到启动信息并且没有反复重启现象，说明配置计算机串口与隔离装置串口连接正确；如果内外网有一个不能观察到启动信息，说明此配置串口故障；如果内外网都不能观察到启动信息，请确定计算机串口能够正常使用。

3、配置计算机串口兼容性不好。如果能够观察到启动信息并且没有反复重启现象，但是使用配置软件始终无法连接到隔离装置，请在配置计算机的“设备管理器”的端口选项下将相应的 COM 端口速率设置为‘115200’，数据流控制设置为‘无’后再次重试。

4、隔离装置负荷较重。隔离装置负荷较重时，CPU 使用率过高，串口通讯进程可能无法及时得到 CPU 响应。建议选择隔离装置负荷较轻时重试。

5、隔离装置反复重启。在超级终端窗口观察隔离装置的启动信息，确认隔离装置反复重启，请与本公司联系。

5.2 网络故障诊断

用户在使用隔离装置的时候，如果内外网无法正常通讯，请按照以下步骤对网络进行诊断：

1、确认隔离装置与网络物理连接正常。因为隔离装置支持双机热备功能，如果隔离装置与网络物理连接不正常，隔离装置会切换到备机模式。使用“超级终端”观察正向隔离装置内网的启动信息，如果有“I want change to main machine”信息显示，表示隔离装置工作在主机模式，隔离装置与网络连接正常；否则工作在备机模式，请仔细检查隔离装置与网络的物理连接。

2、确认内外网主机与隔离装置物理连接正常。隔离装置现在支持有限的 ping 诊断功能，具体诊断方法请参考本手册 3.5 节《系统调试》，如果诊断成功说明内外网主机与隔离装置物理连接正常。如果 ping 失败，请仔细检查内外网主机与网络的物理连接。

3、隔离装置规则配置参数错误。请仔细阅读第四章《典型应用隔离方案规则设定范例》一节，确认规则配置正确。或者寻求本公司的技术支持。

4、内外网通讯程序没有按照隔离装置的编程原则设计。请使用随机光盘上的测试软件测试内外网的数据通讯是否正常。

5.3 日志审计

隔离装置随机配置光盘上带有“日志审计系统”软件。可以接收隔离装置输出的系统日志，方便用户查看隔离装置的运行状态。

具体使用方法如下所述:

1、配置日志输出专用规则，保证内网日志服务器和隔离装置通讯正常。规则名为“**syslog**”，协议类型为 **UDP**，内网 IP 地址为日志服务器的 IP 地址，内网端口为 **514**，内网 MAC 地址、外网虚拟 IP 根据实际网络环境设置；内网虚拟 IP、外网 IP 地址、外网端口、外网 MAC 地址设置为合法参数即可。完成上述规则设置后，在日志服务器上能够 ping 通外网虚拟 IP，表示规则

设置正确，外网虚拟 IP 地址实际上就是软件中显示的日志发送主机的 IP。

2、将“日志审计系统”软件安装到内网日志服务器上，设置好日志文件的保存位置，启动软件开始接收系统日志。注意：“日志审计系统”软件接收端口锁定为 UDP 协议 514 端口，请保证日志服务器上此协议端口能够使用。

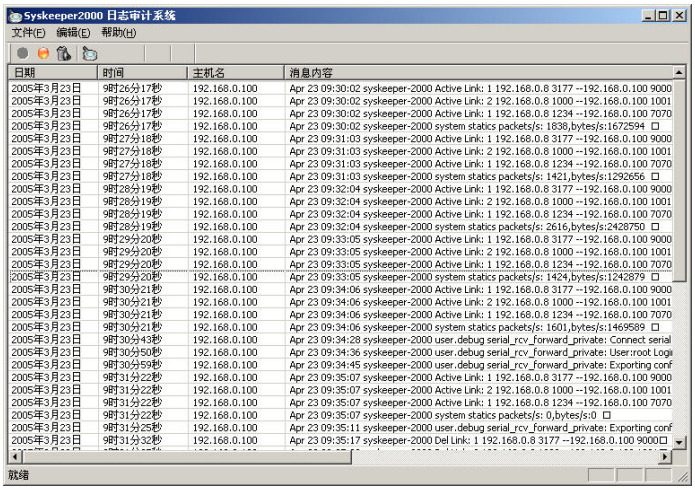

图 38 日志窗口

5.4 虚拟主机IP、静态NAT介绍

为了实现处于不同网段的主机之间的相互访问，隔离装置采用了虚拟 IP、静态 NAT 技术。所谓的虚拟 IP，就是在隔离装置中针对内外网的两台主机，虚拟出两个 IP 地址，内网主机虚拟出一个外网的 IP 地址，外网的主机虚拟出一个内网的 IP 地址，这样内网主机就可以通过访问外网主机的虚拟 IP 达到访问外网主机的目的，同时外网主机也可以通过访问内网主机的虚拟 IP 达到访问内网主机的目的。有了以上两个虚拟 IP 地址,内外网主机之间的通讯被映射为两个部分：内网对内网的通讯，外网对外网的通讯。具体示例如图 57 所示：

内网主机 IP 地址为 192.168.0.39，分配一个与外网主机在同一网段的虚拟 IP 地址 202.102.93.1；外网主机 IP 地址为 202.102.93.54，分配一个与内网主机在同一网段的虚拟 IP 地址 192.168.0.1。当内网主机上的 client 端向外网主机上的 Server 端发起 TCP 连接请求时，报文的源 IP 地址为 192.168.0.39，目的 IP 地址为外网主机的虚拟 IP 地址 192.168.0.1。经过隔离装置的 NAT 转换后，到达外网

的报文的源 IP 地址为内网主机的虚拟 IP 地址 202.102.93.1，目的 IP 地址为外网主机的 IP 地址 202.102.93.54。从外网主机到内网主机的 TCP 应答报文源 IP 地址是外网主机的 IP 地址 202.102.93.54，目的 IP 地址是内网主机的虚拟 IP 地址 202.102.93.1。经过隔离装置的 NAT 转换后，到达内网的应答报文的源 IP 地址是外网主机的虚拟 IP 地址 192.168.0.1，目的地址是内网主机的 IP 地址 192.168.0.39。

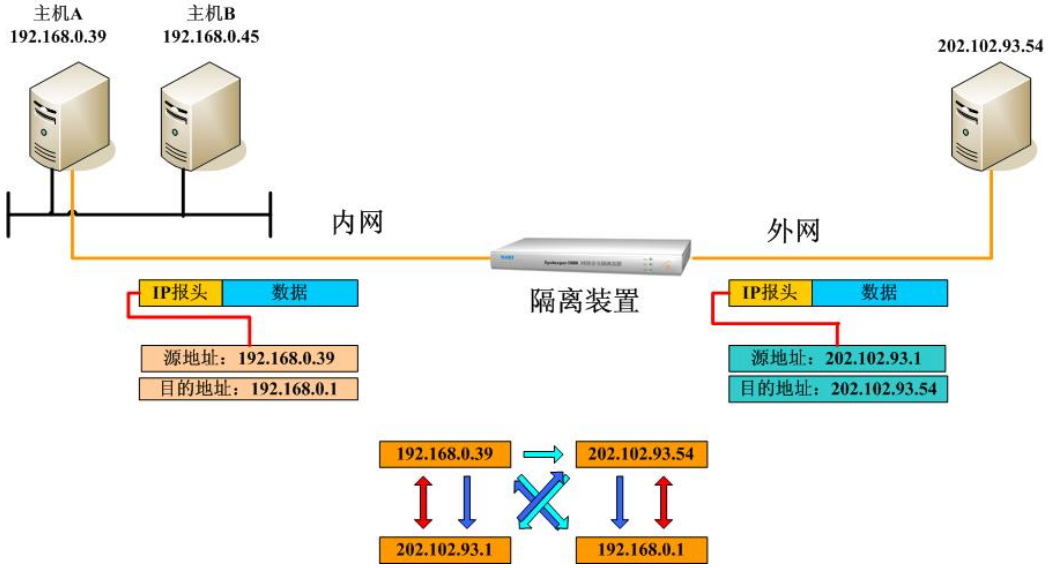

图 39　虚拟 IP 示意图

注意：

1、 在使用 NAT 功能时，外网主机可以有多个虚拟的 IP 地址与之对应。

2、 内网多台主机访问外网同一台主机时，外网主机虚拟 IP 可以只设置一个，但是内网每一台主机的虚拟 IP 地址必须不同。例如内网主机 B 也要和外网主机通信，IP 地址为 192.168.0.45。外网主机的虚拟 IP 地址可以设置为上例所示的虚拟 IP 地址 192.168.0.1，内网主机 B 的虚拟 IP 地址必须与主机 A 的虚拟 IP 地址不同，可以设置为 202.102.93.2。

3、 如果隔离装置两边主机是同一网段，虚拟 IP 地址与真实的 IP 地址相同。例如主机 C(10.144.100.1)，与主机 D(10.144.100.2)进行通信，此时可以把主机 C 的虚拟 IP 地址设置为 10.144.100.1，主机 D 的虚拟 IP 地址设置为 10.144.100.2。