NARI

SysKeeper-2000

网络安全隔离装置诊断调试手册

1. 网络调试

1.1 网络连接线的选择

隔离装置如果与计算机或者路由器连接，采用交叉线进行网络连接；如果与交换机或者集线器连接，则采用直连线进行连接。在网络连接线正确连接后，观察隔离装置后面板的网络接口指示灯是否点亮，如果网络指示灯点亮，表明网络连接正常，否则可能隔离装置网络接口故障。

1.2 通信链路调试

可以采用隔离装置配置软件的ping诊断工具测试或者直接在隔离装置两端的通信网关机上直接测试（**推荐采用第二种调试方式**）。

1) 首先确认隔离装置内外网均正确连接到网络中；

2) 在内网网关机（以内网诊断为例）上的命令行窗口中分别执行以下命令：

arp －d；（清空通信网关机上的 arp 地址表）；

ping 外网虚 IP；

arp －a；（查看通信网关机更新后的的 arp 地址表）

如果能得到隔离装置的虚拟 MAC 地址(前四位为 1234)，则说明内网网关机到隔离装置内网端的链路是正常的。（注：如果通信网关机与路由器直接连接，则会返回路由器的 MAC 地址，在此种连接方式下，建议采用专用的 ping 诊断工具进行调试，具体调试方法请参考安全隔离装置用户手册)。

3) 双进双出型隔离装置对 ping 报文的长度进行安全控制，在 ping 的时候增加长度参数（Windows 计算机：ping 外网虚 IP －l 996，UNIX 计算机：ping 外网虚拟 IP －s 996），如果链路可达则可以观察到返回的 ping 报文。

采用同样的测试方法，可以测试外网网关机到隔离装置外网端的链路是否正常。

2.隔离装置工作状态诊断

2.1 观察内、外网数据灯

在没有数据传输时，如果可以观察到隔离装置正面板内外网数据灯每隔 1~2 秒微弱的闪烁一下，则表明隔离装置工作状态正常；如果内外网数据灯都没有闪烁或者数据灯常亮且不能传输数据，则装置可能出现异常，请立刻与我们联系。

2.2 超级终端观察

隔离装置可以通过配置计算机的超级终端软件对系统的工作状况进行调试和观察。配置计算机超级终端的设置如下所述：

a)运行 Windows 开始—>程序—>附件—>通讯—>超级终端

b)输入超级终端名称：SysKeeper,选择计算机相应的 Com 端口（Com1）

图 1

c)配置超级终端属性：如下图所示。

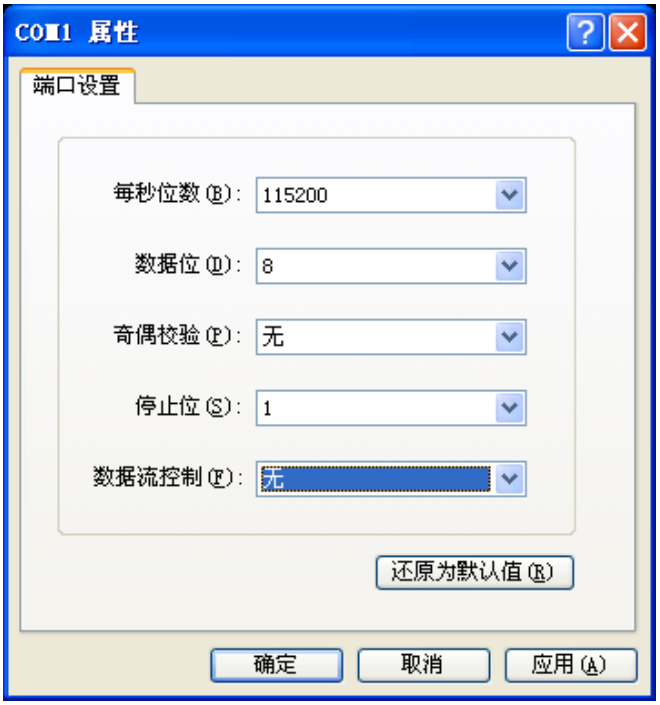

图 2

d)保存配置。

设置完成后，将配置计算机的串口和隔离装置的内网 Console 口连接－>打开前面设置的 SysKeeper 超级终端－>启动隔离装置电源－>观察隔离装置启动的输出信息。

如果不断重复输出启动信息，则表明装置在反复重启，请立刻与我们联系，如果启动信息为乱码，表明配置计算机或者隔离装置的串口通信有故障，请参考下一节的调试文档，并与我们及时联系，获得进一步的帮助。

提示：可以通过设置超级终端的“传送－>捕获文字”，把所有输出信息保存为文本文件，以作详细的调试分析。

3.串口工作状态诊断

3.1 物理连接

1）**专用配置线**

应使用配套的专用串口线配置隔离装置。

2）**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”，在端口选项下查看串口使用的 COM 端口，确认 COM 端口选择正确。

3）**串口配置线与隔离装置的连接**

正向隔离装置：配置计算机的串口和隔离装置的内网 Console 口连接；

反向隔离装置：配置计算机的串口和隔离装置的外网 Console 口连接。

3.2 不同型号隔离装置的配置软件版本

正向单 bit 隔离装置采用 V1.0-1bit 配置软件；

反向单 bit 隔离装置采用 V1.0-1bit 配置软件；

3.3 隔离装置负荷较大

当隔离装置正在传输大量数据时，隔离装置负荷较大，CPU 使用率较高，串口通讯进程可能无法及时得到 CPU 响应，建议暂停数据传输后再进行配置。

3.4 计算机的串口兼容性

某些型号计算机，特别是一些较老型号笔记本的串口与隔离装置串口兼容性较差，可能出现无法连接的现象，建议换用其它型号的计算机配置。

如果能够观察到启动信息并且隔离装置没有反复重启现象，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，

如果仍然无法连接，建议换用其它型号的计算机配置。

3.5 隔离装置的串口

在超级终端中观察：

如果隔离装置内外网串口有一个不能观察到启动信息，说明此配置串口故障，请立刻与我们联系；如果内外网都不能观察到启动信息，请确定计算机串口是否能够正常使用。

4.数据传输状态诊断

初步诊断装置没有故障(如可观察到内外网数据灯间隔数秒的闪烁、在超级终端可以观察到正常启动信息且没有不断重启的现象)，但仍无法传输数据，可按以下步骤进行进一步的诊断。

4.1 规则配置

1）确认规则的设置与实际网络环境、通讯程序是否一致，如源、目的 IP，端口，协议类型等，还需要确认规则中配置的网卡选择与实际的网络连接是否一致。具体配置方法请参考《网络安全隔离装置用户手册》。

2）确认配置隔离装置所用的虚 IP 未被其它网络设备使用，否则会造成 IP 地址冲突，导致无法传输数据。

3）当同时部署正、反向隔离装置时，应特别注意在正、反向隔离装置中配置的虚 IP 不能相同，否则会造成 IP 地址冲突，导致无法传输数据。

4）如果不能进一步确认规则配置是否正确，请导出配置信息并绘制网络拓扑图，与我们及时联系。

4.2 搭建最简测试环境

当网络环境较为复杂时，往往无法确认故障点位于网络中的哪个环节(如路由器、防火墙等)，则可把隔离装置内外网分别直接连接到两台计算机上一>配置

测试规则—>用配套光盘中的测试软件测试。

4.3 高级应用编程

按照二次安全防护的要求，SysKeeper-2000 网络安全隔离装置实现了 TCP 数据的单向传输控制，反向的 TCP 应答禁止携带应用数据，应用层的应答字节数最多为 1 个字节。所以经过隔离装置进行数据传输的应用软件，应遵守以下一些编程原则来进行应用程序的改造：

1. I/II 区与 III 区之间的应用程序禁止采用 SQL 命令访问数据库和基于 B/S 方式的双向数据传输。
2. I/II 区与 III 区之间的数据通信，传输的启动端由内网发起，反向的应答报文不容许携带数据，应用层的应答报文最多为 1 个字节。
3. 通信程序的服务端应特别需要注意初始化 SOCKET 为 TCP_NODELAY 或采用强制刷新缓冲区的 API 调用使应答数据立即送出，否则可能出现实际反向传输的应答数据超过 1 个字节而导致无法传输数据。
4. 另外需要注意的是穿越隔离的通讯程序应连接对端的虚 IP，而不是原来没有物理隔离时连接的对端真实 IP。

4.4 通信网关机配置

当内外网的通信网关机(Windows)启用了系统个人防火墙功能后可能造成配套的文件传输软件无法正常工作，可以关闭或重新设定防火墙；

经诊断初步判定隔离装置的故障情况后，需要记录装置的序列号及出厂日期，并与我公司及时联系，以方便我们进一步诊断。

NARI南京南瑞集团信息系统分公司

地址：南京市南瑞路 8 号　综合楼 6、7 楼
邮编：210003
电话：（025）83096601（市场部）
（025）83096702（安全产品部）
(025) 83096600-131
传真：（025）83450018 (025)83096701
E-mail：it_market@nari-china.com（市场部）
corba@vip.sina.com(技术支持)
http：//www.nari-china.com