

K/3 系统防火墙设置

本期概述

- | 本文档适用于 k/3 系统与防火墙的应用。
- | 学习完本文档以后，可以对 K/3 系统在防火墙中的设置有初步的了解。

版本信息

- | 2009 年 02 月 21 日 V1.0 编写人：何瑜
- | 2009 年 V1.1 修改人：

版权信息

- | 本文件使用须知

著作权人保留本文件的内容的解释权,并且仅将本文件内容提供给阁下个人使用。对于内容中所含的版权和其他所有权声明,您应予以尊重并在其副本中予以保留。您不得以任何方式修改、复制、公开展示、公布或分发这些内容或者以其他方式把它们用于任何公开或商业目的。任何未经授权的使用都可能构成对版权、商标和其他法律权利的侵犯。如果您不接受或违反上述约定,您使用本文件的授权将自动终止,同时您应立即销毁任何已下载或打印好的本文件内容。

著作权人对本文件内容可用性不附加任何形式的保证,也不保证本文件内容的绝对准确性和绝对完整性。本文件中介绍的产品、技术、方案和配置等仅供您参考,且它们可能会随时变更,恕不另行通知。本文件中的内容也可能已经过期,著作权人不承诺更新它们。如需得到最新的技术信息和服务,您可向当地的金蝶业务联系人和合作伙伴进行咨询。

著作权声明 著作权所有 2009 金蝶软件(中国)有限公司。
所有权利均予保留。

目 录

第一章 K/3系统防火墙设置	3
1.1 名词解释.....	3
1.2 防火墙端口设置.....	3
1.2.1 数据库服务器端口设置.....	3
1.2.2 中间层服务器端口设置.....	6

第一章 K/3 系统防火墙设置

1.1 名词解释

防火墙 (FireWall) 是通过创建一个中心控制点来实现网络安全控制的一种技术。通过在专用网和 Internet 之间的设置路卡、防火墙监视所有出入专用网的信息流,并决定哪些是可以通过的,哪些是不可以的。安全的防火墙意味着网络的安全。

端口 (Port) 计算机用于通讯所使用的通道,如 web 用的端口 80,开放的端口越多,则越容易被非法入侵。

TCP Transmission Control Protocol 的简称,是 Internet 上广为使用的一种计算机协议。

UDP User Datagram Protocol 的简称,Windows NT 常使用的协议。

DCOM 分布式组件对象模型。

1.2 防火墙端口设置

由于安全性的问题,防火墙一般只允许通过 Internet 信息数据交换使用特定端口(如 web 用 80),但是 K/3 客户端在访问服务器需要调用 DCOM 组件,而 DCOM 创建对象时使用的是 1024-65535 之间的动态端口,并且由于防火墙的 IP 伪装特性,这使 DCOM 在有防火墙的服务器上是不能进行正常连接的,那到底应该如何设置呢?下文将具体讲解 K/3 系统与防火墙的设置。

1.2.1 防火墙设置

一、由于开放的端口越多,系统的安全性就会越差,一般防火墙都关闭了大量端口,以防止非法入侵,但 DCOM 需要使用大量的端口,要解决二者的矛盾,可通过统一的 RPC 管理(远程过程调用)来解决,(由 RPC 统一进行创建 DCOM 对象所需的端口的映射处理)所以需在防火墙服务器上打开 RPC 端口 135。

二、数据库服务端口是 1433,如果数据库服务器和中间层服务器分开安装,一定要在防火墙上开放 1433 端口,否则数据库连接会不正常。

三、开放任意五个连续端口(1024-65535 之间)为 DCOM 调用
具体操作如下:

1、运行 DCOMCNFG.EXE,打开如图 1 所示的界面;

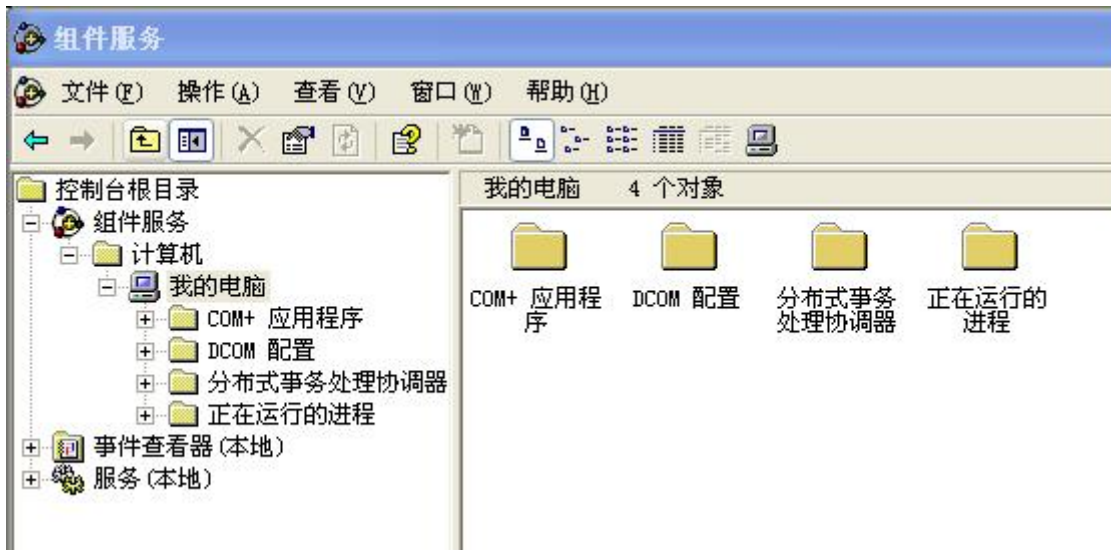


图 1

- 2、依次点开【组件服务】-【计算机】-【我的电脑】，右键单击【我的电脑】-【属性】，打开属性页面，选择【默认协议】页签；如图 2 所示。



图 2

- 3、单击【面向连接的 TCP/IP】 【属性】 【添加】按钮，添加端口范围（至少 5 个以上），例如：4000-4005，当然如果使用其他连续 5 个端口也可以，最后单击【确定】

按钮保存，并重新启动计算机以确保设置生效。如图 3 所示。

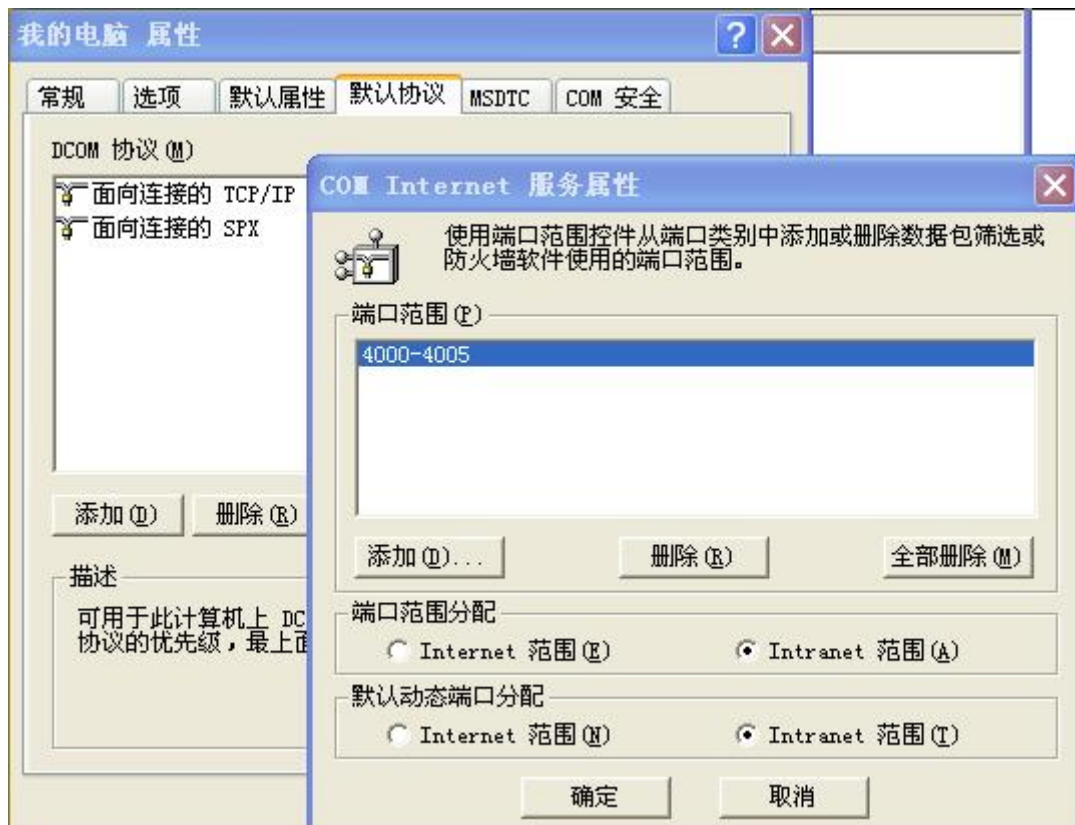


图 3

注意：这里只是创建了 DCOM 端口范围，如果有防火墙还需要将这些端口在防火墙中设置允许通过。

下面是 WINDOWS 自带的防火墙端口设置实例。

打开本地连接属性 高级 设置 例外，单击【添加端口】按钮，如图 4 所示：

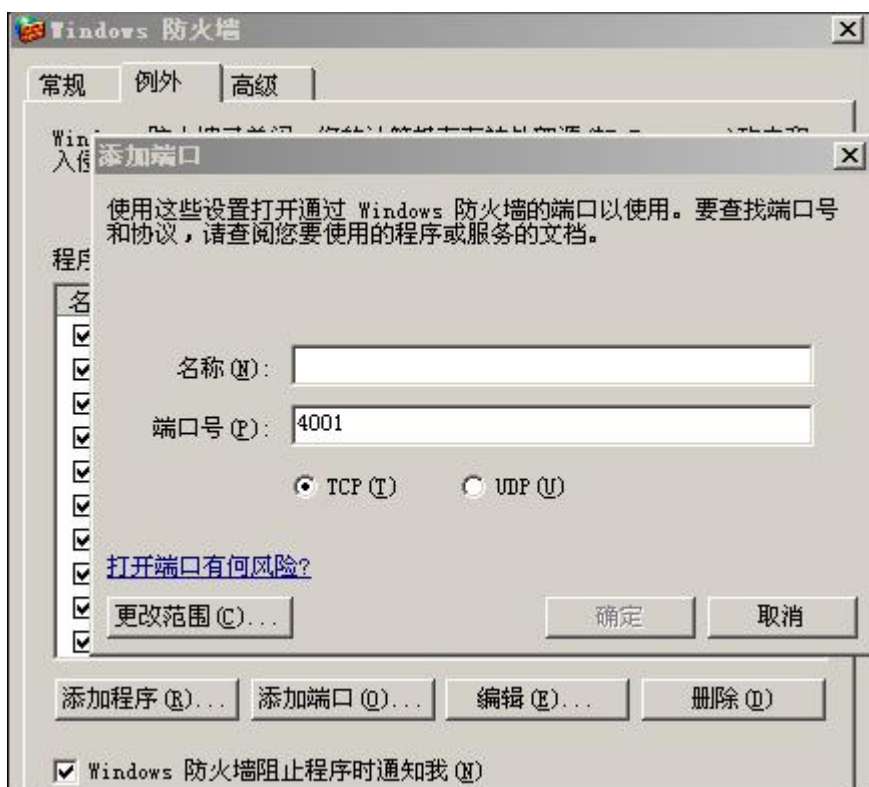


图 4

总结：

数据库服务器需要开放的端口如下：

- a) TCP 端口：135(RPC 端口)、1433(数据库服务端口)、4000、4001、4002、4003、4004、4005 任意连续的 5 个端口 (COM Internet 端口范围)
- b) UDP 端口：无

1.2.2 中间层服务器端口设置

一、中间层服务器同样需要开放 135 (RPC 服务) 端口。

二、连续 DCOM 动态端口 (1024-65535 之间)，数量视服务器 EBO 组件包而定，但建议不少于 35 个。

具体端口指定操作如下：

1、运行 DCOMCNFG.EXE，打开如图 5 所示的界面；

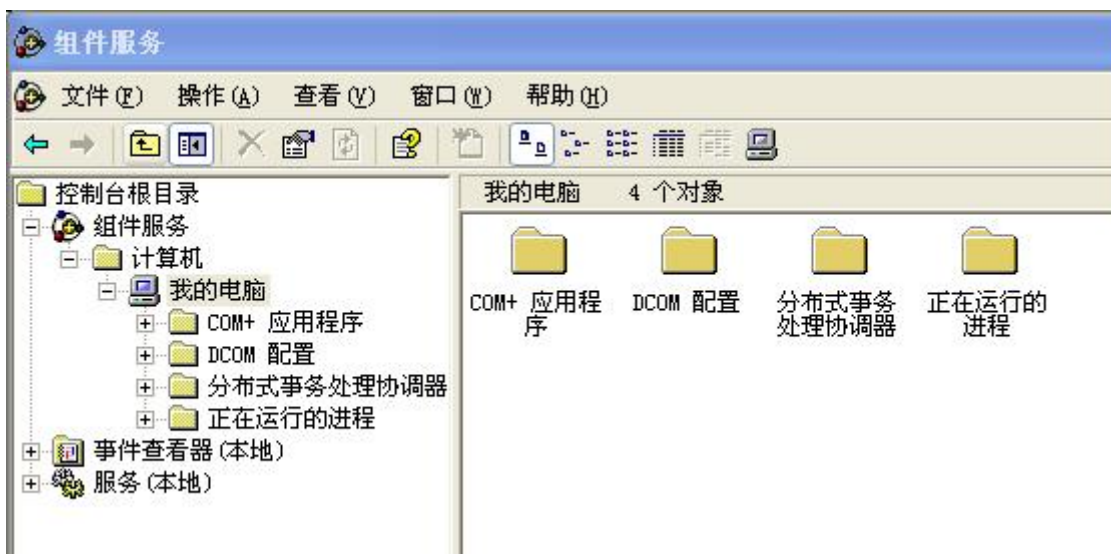


图 5

- 2、依次点开【组件服务】-【计算机】-【我的电脑】，右键单击【我的电脑】-【属性】，打开属性页面，选择【默认协议】页签；如图 6 所示。

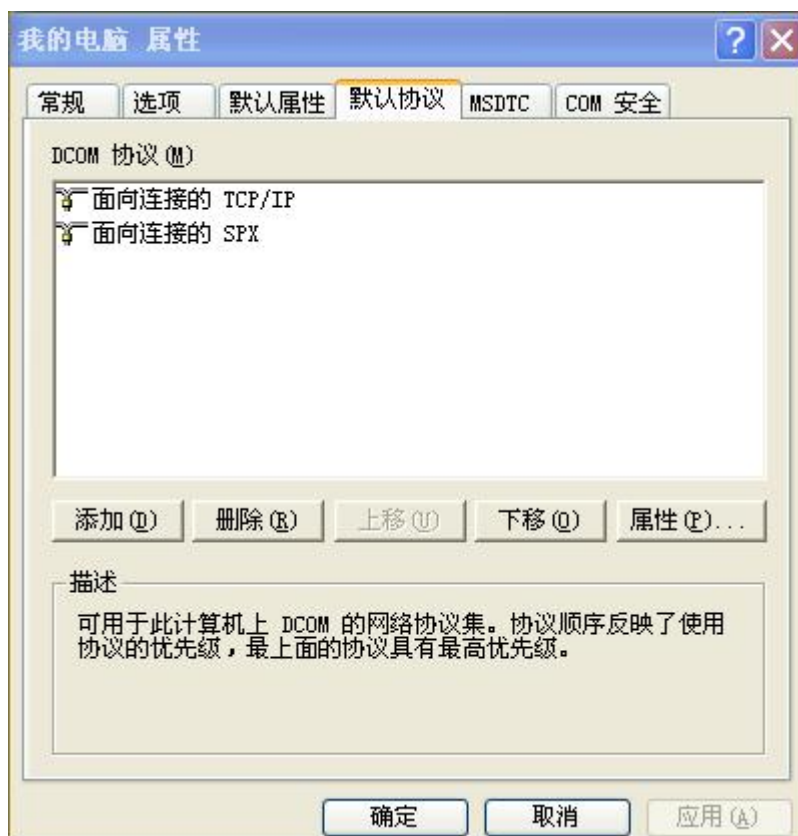
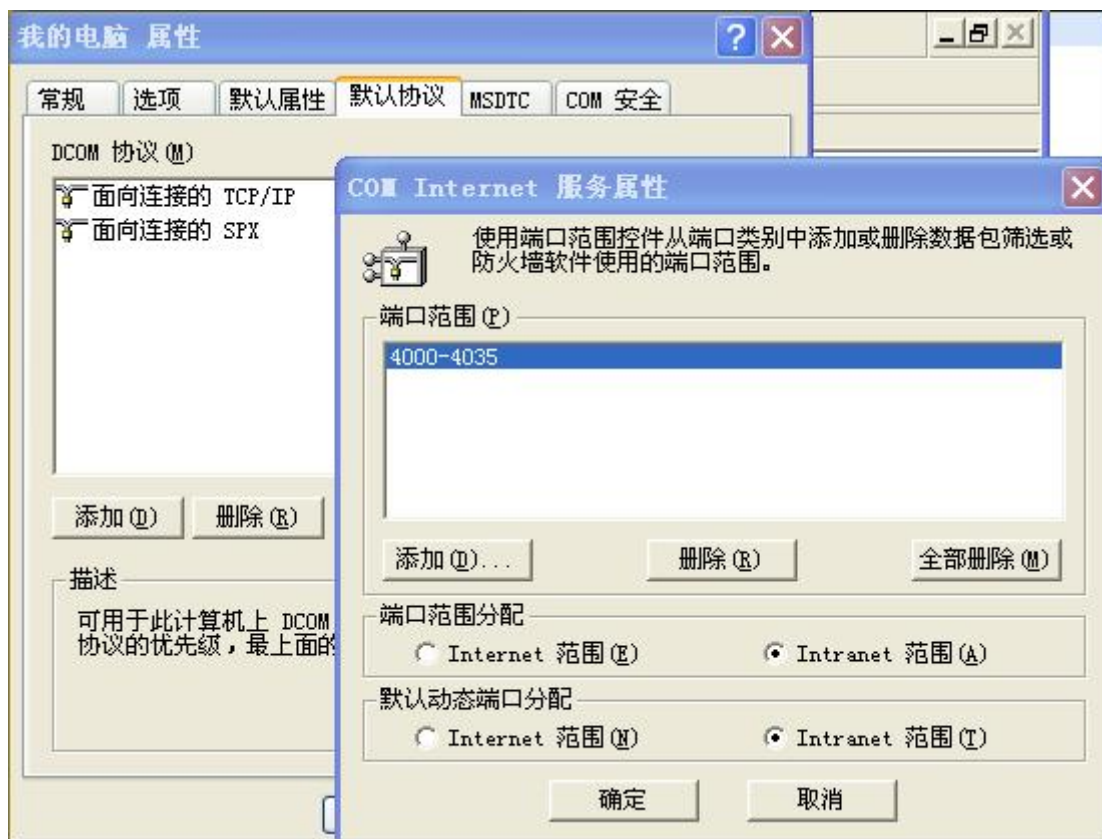


图 6

3、选择默认协议 面向连接的 TCP/IP 属性 添加端口范围（至少 35 个以上,有多少个组件包,就必须设置开放相同数量连续端口),例如:4000-4035,当然如果使用其他连续 35 个端口也可以,最后确定保存并重新启动计算机。



同样,这里只是指定了 DCOM 端口范围,如果有防火墙还需要将这些端口在防火墙中设置允许通过。

总结:

为中间层开放的端口:

A、TCP 端口:135 (RPC 服务)、4000、4001、4002、...、4035 或任意连续 35 个端口 (COM Internet 端口范围)

UDP 端口:无