南昌大学软件学院

实验报告书

课 程 名 ： 网络安全技术

题　　目： 个人防火墙技术试验

实验类别 【验证】

班　　级： 信息安全 193 班

学　　号： 8003119100

姓　　名： 丁俊

评语：

实验态度：认真（　）　一般（　）　较差（　）
实验结果：正确（　）　部分正确（　）错（　）
实验理论：掌握（　）　熟悉（　）　了解（　）生疏（　）
操作技能：较强（　）　一般（　）　较差（　）
实验报告：较好（　）　一般（　）　较差（　）

成绩：＿＿＿＿＿＿　　指导教师： 鄢志辉

一、实验目的

防火墙是网络安全的第一道防线，按防火墙的应用部署位置分类，可以分为边界防火墙、个人防火墙和分布式防火墙三类。通过实验深入理解防火墙的功能和工作原理，掌握个人防火墙的工作原理和规则设置方法，掌握根据业务需求制定防火墙策略的方法。

二、实训内容

基本要求了解各种不同类型防火墙的特点，根据不同的业务需求制定防火墙策略，并制定、测试相应的防火墙的规则等。

三、实验环境（本次上机实践所使用的平台和相关软件）

Win7操作系统

四、实验原理

防火墙的实现技术

(1) 包过滤技术

包过滤是防火墙的最基本过滤技术，它对内外网之间传输的数据包按照某些特征事先设置一系列的安全规则进行过滤或筛选。包过滤防火墙检查每一条规则直至发现数据包中的信息与某些规则能符合，则允许或拒绝这个数据包穿过防火墙进行传输。如果没有一条规则能符合，则防火墙使用默认规则，一般情况下，要求丢包。

这些规则根据数据包中的信息进行设置，包括：

●IP 源地址；

●IP 目标地址；

●协议类型（TCP 包、UDP 包和 ICMP 包）；

●TCP 或 UDP 包的目的端口、源端口；

●ICMP 消息类型；

●TCP 选项；

●TCP 包的序列号、IP 校验和等；

●数据包流向：in 或 out；

●数据包流经的网络接口；

●数据包协议类型：TCP、UDP、ICMP、IGMP 等；

●其他协议选项：ICMP ECHO、ICMP ECHO REPLY 等；

●数据包流向：in 或 out。

因为包过滤只需对每个数据包与相应的安全规则进行比较，实现较为简单，速度快、费用低，并且对用户透明，因而得到了广泛的应用。这种技术实现效率高，但配置复杂，易引起很多问题，对更高层协议信息无理解能力，而且不能彻底防止地址欺骗。包过滤技术防火墙原理如图 7-1 所示。

图 7-1 包过滤防火墙原理示意图

(2) 地址翻译 NAT 技术

NAT 即网络地址翻译技术，它能够将单位内网使用的内部 IP 地址翻译成合法的公网 IP，使内网使用内部 IP 的计算机无须变动，又能够与外网连接。

对于局域网的主机使用 10.0.0.0、172.16.0.0、192.168.0.0 三个内部 IP 网段时，当内网主机要与外部网络进行通信，就要在网关处，由 NAT 将内部 IP 地址翻译为公网 IP 地址，从而在外部公网上正常使用。当外部公网响应的数据包返回给 NAT 后，NAT 再将其翻译为内部的 IP 地址，发给内网的主机，从而实现内网主机与外网的正常通信，解决了 IPv4 地址不足的问题。同时，由于外网主机只能看到数据包来自 NAT 翻译后的公网 IP，而看不到内网主机的内部 IP，所以 NAT 可保护及隐藏内网计算机。

NAT 有三种类型：静态 NAT、动态地址 NAT、网络地址端口转换 NAPT。静态 NAT 是将内部网络中的每个主机永久的映射成外部网络中的某个合法的地址。而动态地址 NAT 则是在外部网络中定义了一系列的合法地址，采用动态分配的方法映射到内部网络。NAPT 则是把内部地址映射到外部网络的一个 IP 地址的不同端口上。

(3) 应用级网关

应用级网关即代理服务器，代理服务器通常运行在两个网络之间，它为内部网的客户提供 HTTP、FTP 等某些特定的因特网服务。代理服务器相对于内部网的客户来说是一台服务器，对于外部网的服务器来说，它又相当于客户机。当代理服务器接收到内部网的客户对某些因特网站点的访问请求后，首先会检查该请求是否符合事先制定的安全规则，如果允许，代理服务器会将此请求发送给因特网站点，从因特网站点反馈回的响应信息再由代理服务器转发给内部网的客户。代理服务器会将内部网的客户和因特网隔离。

对于内外网转发的数据包，代理服务器在应用层对这些数据进行安全过滤，而包过滤技术与 NAT 技术主要在网络层和传输层进行过滤。由于代理服务器在应用层对不同的应用服务进行过滤，所以可以对常用的高层协议做更细的控制。

由于安全级网关不允许用户直接访问网络，因而使效率降低，而且安全级网关需要对每一个特定的因特网服务安装相应的代理服务软件，内部网的客户要安装此软件的客户端软件，此外，并非所有的因特网应用服务都可以使用代理服务器。应用级网关技术防火墙原理如图 7-2 所示。

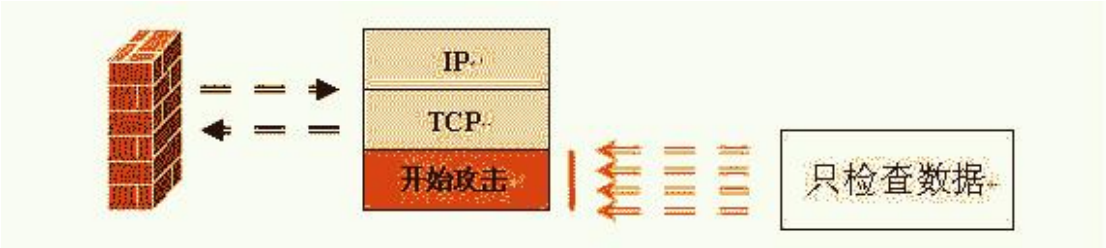


图 7-2 应用级网关防火墙原理示意图

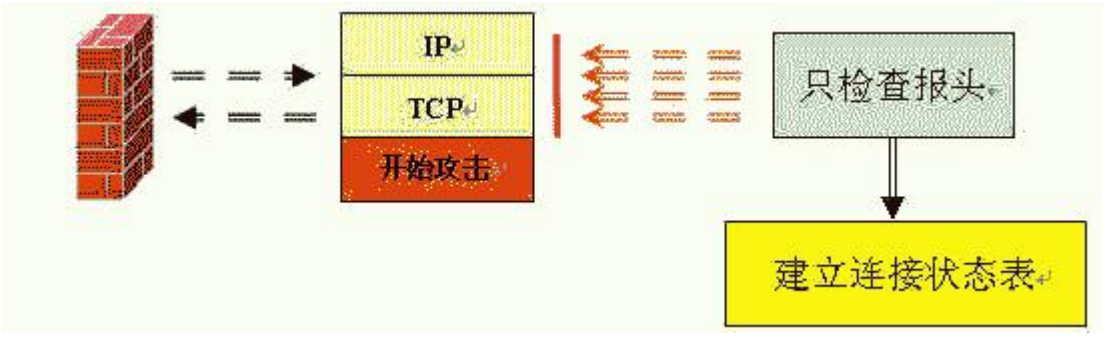
(4) 状态检测技术

状态检测防火墙不仅仅像包过滤防火墙仅考查数据包的 IP 地址等几个孤立的信息，而是增加了对数据包连接状态变化的额外考虑。它在防火墙的核心部分建立数据的连接状态表，将在内外网间传输的数据包以会话角度进行检测，利用状态表跟踪每一个会话状态。

例如，某个内网主机访问外网的连接请求，防火墙会在连接状态表中加以标注，当此连接请求的外网响应数据包返回时，防火墙会将数据包的各层信息和连接状态表中记录的从内网到外网每天信息相匹配，如果从外网进入内网的这个数据包和连接状态表中的某个记录在各层状态信息一一对应，防火墙则判断此数据包是外网正常返回的响应数据包，会允许这个数据包通过防火墙进入内网。按照这个原则，防火墙将允

许从外部响应此请求的数据包以及随后两台主机间传输的数据包通过，直到连接中断，而对由外部发起的企图连接内部主机的数据包全部丢弃，因此状态检测防火墙提供了完整的对传输层的控制能力。

状态检测防火墙对每一个会话的记录、分析工作可能会造成网络连接的迟滞，当存在大量安全规则时尤为明显，采用硬件实现方式可有效改善这方面的缺陷。状态检测防火墙原理如图所示。



状态检测防火墙示意图

五、实验步骤

Windows 7 防火墙设置，依次打开“计算机”——“控制面板”——“Windows 防火墙”，如下图 1 所示：

图 1

5.1 打开和关闭 Windows 防火墙

点击图 1 左侧的打开和关闭 Windows 防火墙(另外点击更改通知设置也会到这个界面)，如下图 2：

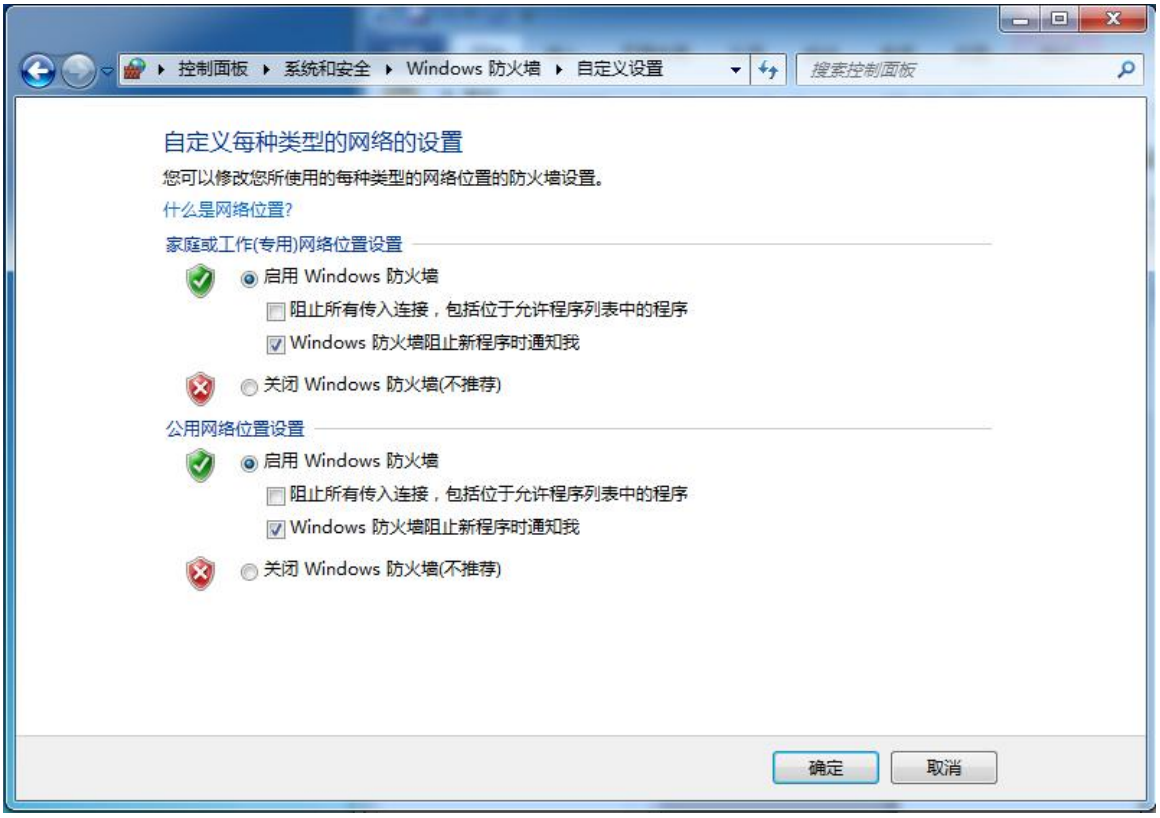


图 2

从上图 2 可以看出，私有网络和公用网络的配置是完全分开的，在启用 Windows 防火墙里还有两个选项：

1、“阻止所有传入连接，包括位于允许程序列表中的程序”，这个默认即可，否则可能会影响允许程序列表里的一些程序使用。

2、“Windows 防火墙阻止新程序时通知我”这一项对于个人日常使用肯定需要选中的，方便自己随时作出判断响应。

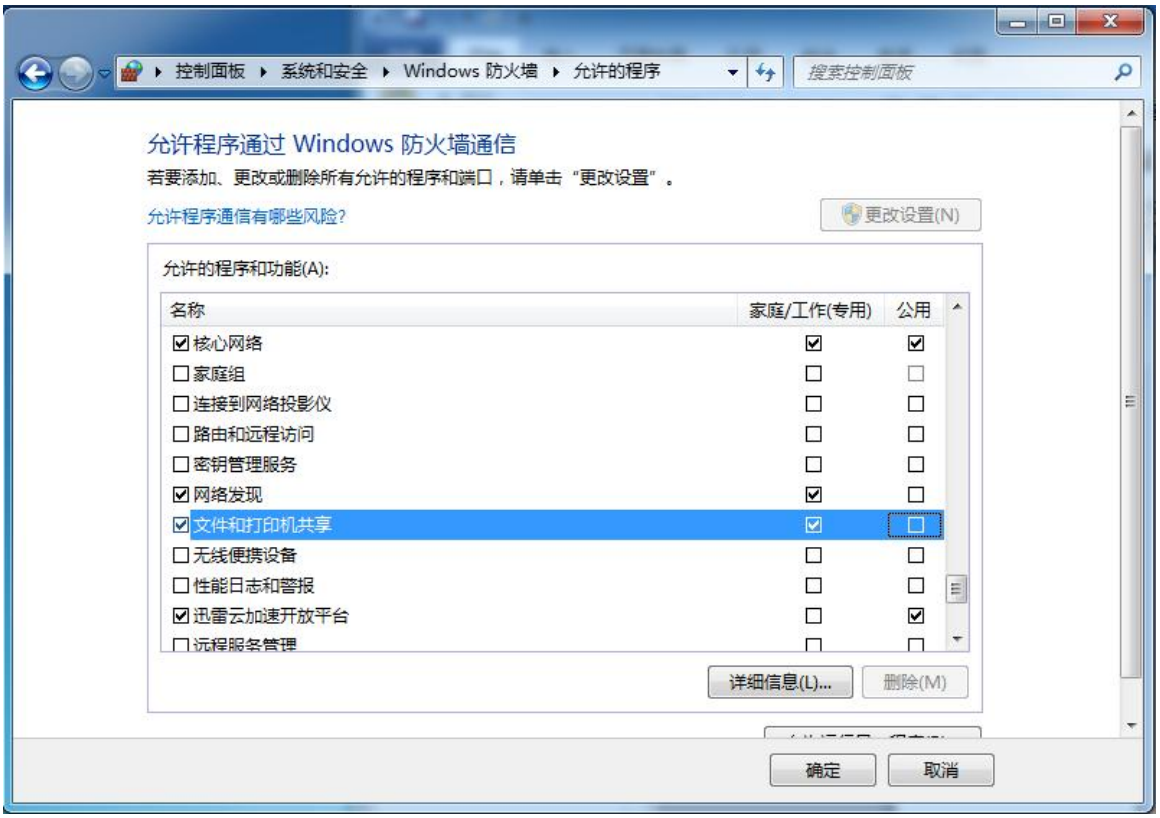
如果需要关闭，只需要选择对应网络类型里的“关闭 Windows 防火墙（不推荐）”这一项，然后点击确定即可。

5.2 还原默认设置

如果自己的防火墙配置的有点混乱，可以使用图 1 左侧的“还原默认设置”一项，还原时，Windows 7 会删除所有的网络防火墙配置项目，恢复到初始状态，比如，如果关闭了防火墙则会自动开启，如果设置了允许程序列表，则会全部删除掉添加的规则。

5.3 允许程序规则配置

点击图 1 中上侧的“允许程序或功能通过 Windows 防火墙”，如下图：



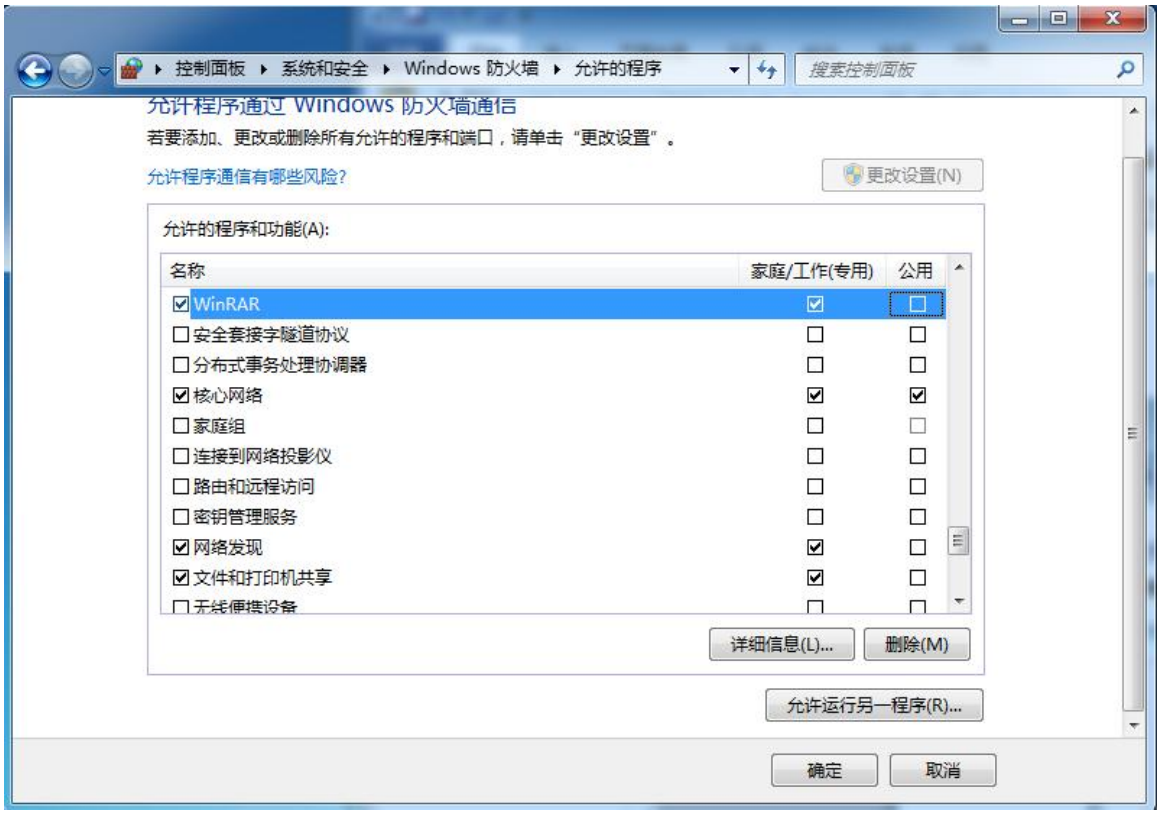
设置允许程序列表或基本服务，

1、常规配置没有端口配置，所以也不再需要手动指定端口 TCP、UDP 协议了，因为对于很多用户根本不知道这两个东西是什么，这些配置都已转到高级配置里，对于普通用户一般只是用到增加应用程序许可规则。

2、应用程序的许可规则可以区分网络类型，并支持独立配置，互不影响，这对于双网卡的用户就很有作用。

如果是添加自己的应用程序许可规则，可以通过下面的“允许允许另一程序”按钮进行添加，方法跟早期防火墙设置类似，点击后如下图：

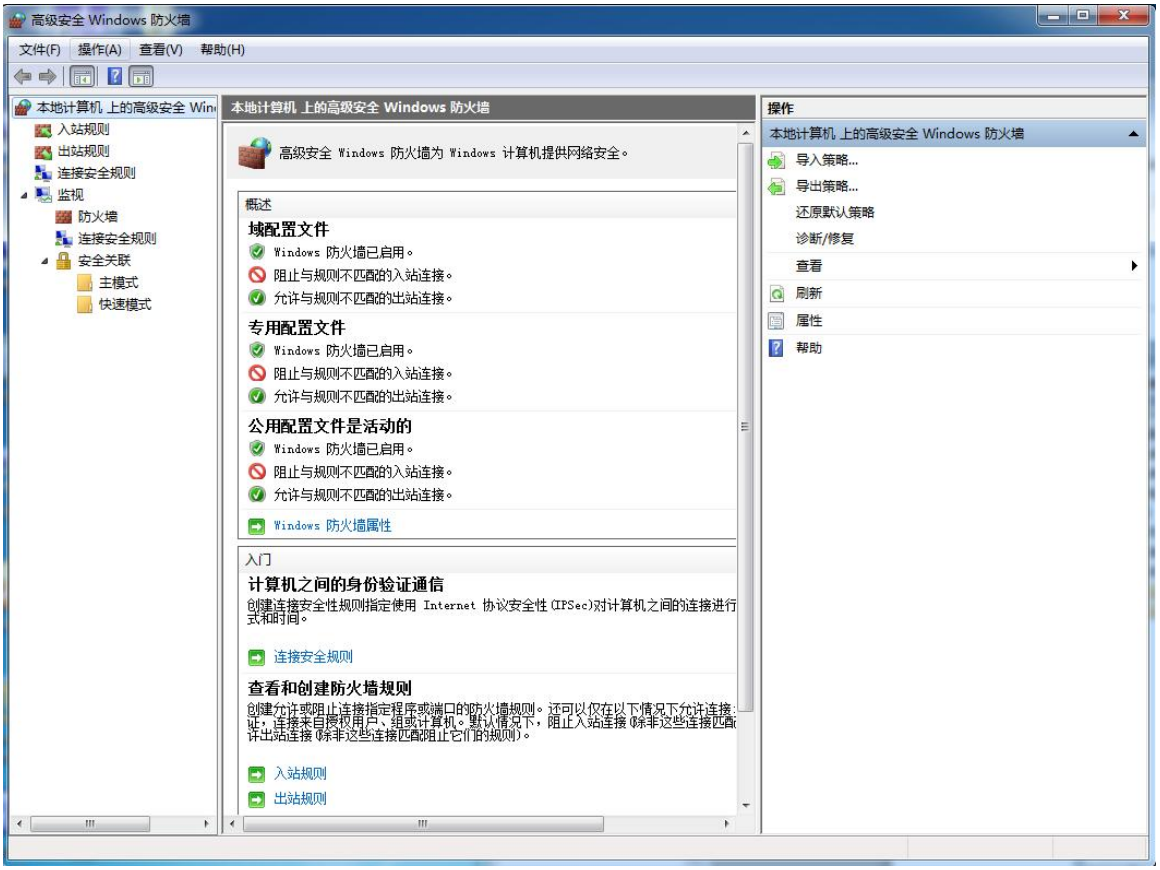
选择将要添加的程序名称（如果列表里没有就点击“浏览”按钮找到该应用程序，再点击”打开“），下面的网络位置类型还是私有网络和公用网络两个选项，不用管，我们可以回到上一界面再设置修改，添加后如下图：



添加后如果需要删除（比如原程序已经卸载了等），则只需要在上图中点选对应的程序项，再点击下面的“删除”按钮即可，当然系统的服务项目是无法删除的，只能禁用。

5.4 高级安全 Windows 防火墙

依次点击“计算机”——“控制面板”——“Windows 防火墙”，点击控制界面左侧的“高级设置”，即可看到如下界面，几乎所有的防火墙设置都可以在这个高级设置里完成。



右侧最下面的“属性”是显示高级安全设置防火墙属性（点击上图中间的“Windows 防火墙属性”也可以，只是显示的标题有点差异），如下图：

防火墙属性设置里，总体分成四大块，这个四种配置类型都是独立配置独立生效的。

域配置文件

域配置文件主要是面向企业域连接使用，普通用户也可以把它关闭掉。

专用配置文件

专用配置文件是面向家庭网络和工作网络配置使用，大家最常使用。

公用配置文件

公用配置文件是面向公用网络配置使用，如果在酒店、机场等公共场合时可能需要使用。

看一下左侧的控制树，大部分都是防火墙规则设置功能，可以创建防火墙规则以便阻止或允许此计算机向程序、系统服务、计算机或用户发送流量，或是接收来自这些对象的流量，规则标准只有三个：允许、条件允许和阻止，条件允许是指只允许使用 IPSec 保护下的连接通过。

入站规则	可以为入站通信或。可配置规则以指定计算机或用户、程序、服务或者端口和协议。可以指定要应用规则的网络适配器类型：局域网 (LAN)、无线、远程访问，例如虚拟专用网络 (VPN) 连接或者所有类型。还可以将规则配置为使用任意配

	置文件或仅使用指定配置文件时应用。
出站规则	为出站通信创建或修改规则，功能同入站规则。
连接安全规则	使用新建连接安全规则向导，创建 Internet 协议安全性（IPSec）规则，以实现不同的网络安全目标，向导中已经预定义了四种不同的规则类型（隔离、免除身份验证、服务器到服务器和隧道），当然也创建自定义的规则，为了便于管理，请在创建连接规则时指定一个容易识别和记忆的名称，方便在命令行中管理。
监视	监视计算机上的活动防火墙规则和连接安全规则，但 IPSec 策略除外。
防火墙	仅显示活动的防火墙规则，可以通过右键点击选项卡选择属性，查看每个选项卡的常规、程序和端口和高级特性。
连接安全规则	显示当前活动的连接安全规则，属性查看可以通过鼠标右键选择属性或点击右侧的工具栏的属性进行查看。
安全关联下的主模式	主模式协商是通过确定一个加密保护套件集、交换密钥材料建立共享密钥以及验证计算机和用户身份，最终在两台计算机之间建立一个安全的通道。监视主模式 SA 可以查看哪些对等计算机连接到本机，以及该 SA 正在使用的保护套件。
安全关联下的快速模式	快速模式协商在两台计算机之间建立安全通道，以保护在两台计算机之间交换的数据。一对计算机之间只有一个主模式 SA，但可以有多个快速模式 SA，监视快速模式 SA 可以查看当前哪些对等计算机连接到本机，哪些保护套件在保护正在交换的数据。可以通过双击列表项目查看快速 SA 信息，

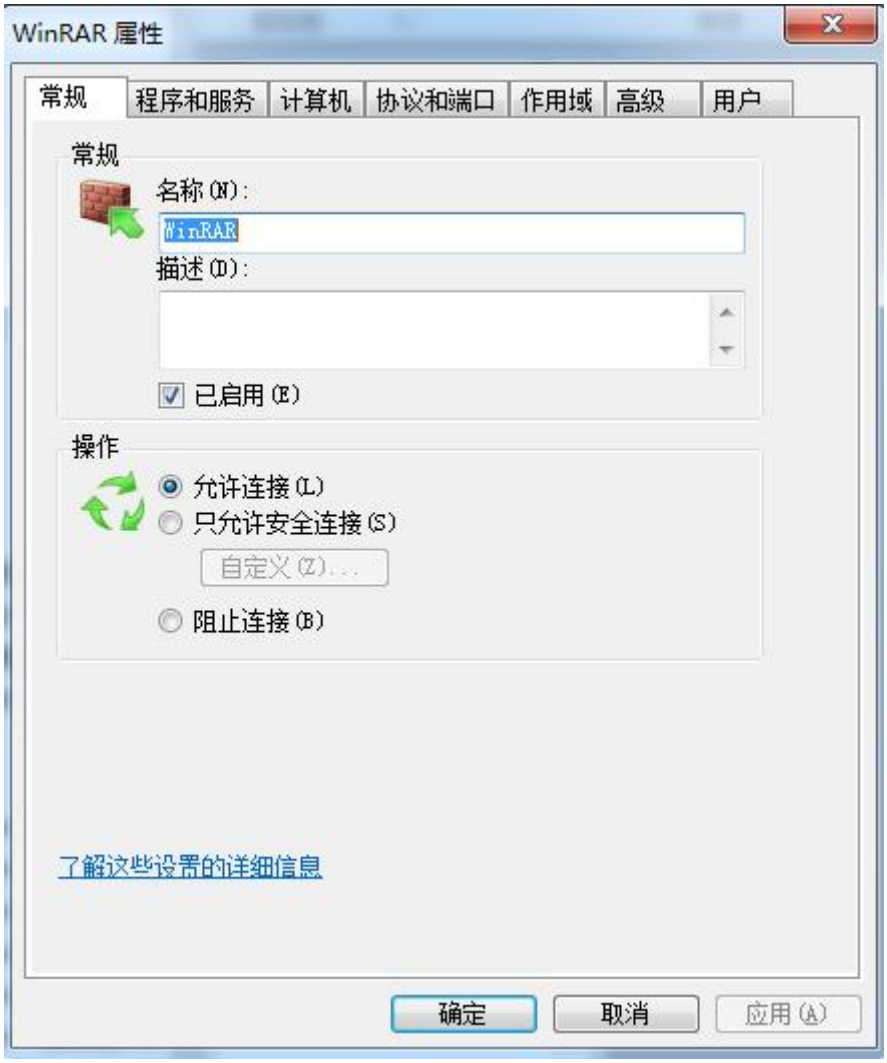
以上列表简述了高级安全 Windows 防火 MMC 管理单元的控制台导航配置大概情况。

1、如何禁用或启用规则

方法：只需要在需要禁用或启动的规则上，鼠标右键选择启用或禁止规则即可，或点击右侧的操作栏进行规则启用或禁止。

2、入站规则和出站规则

入站和出站管理方法基本相同，在 Windows 防火墙的“允许程序或功能通过 Windows 防火墙”中每增加或减少一个设置项，都会反应到入站或出站规则中来，这些规则从整体上看可以分成两个部分，一是用户规则，比如我们手动增加的允许程序规则就属于用户规则，还有一些系统预定义规则，预定义规则大部分都是系统已经预先设置好的，而且很多设置都是不允许修改的，点击上一篇增加的 WinRAR 程序允许规则（鼠标右键选择属性或直接左键双击）。



上图的属性设置可以看出手动增加的程序规则几乎都可以完全定制，而系统的预定义规则中的“程序和服务”与“协议和端口”两个部分几乎都不可以修改，系统规则也会明确黄色头标注明，大部分系统规则，我们只需要启用或禁止即可。

在允许程序或服务管理中，每增加一条程序或启用一个服务，我们可以在高级安全管理界面里看到可能会 N 条规则，规则记录数的多少是跟程序或服务实际使用的协议数有关

系，比如上文增加的 WINRAR 记录如果只选择专用网络，则会默认增加适合专网 TCP、UDP 两条规则记录，当然这些规则全部都可以在属性界面修改掉。

下表列出了上图中几个选项卡的具体设置情况，因为相关抓图太多了，无法一一展示出来，只能用文字粗略描述一下，可以随时在界面中查看帮助文件，防火墙帮助文件非常完善：

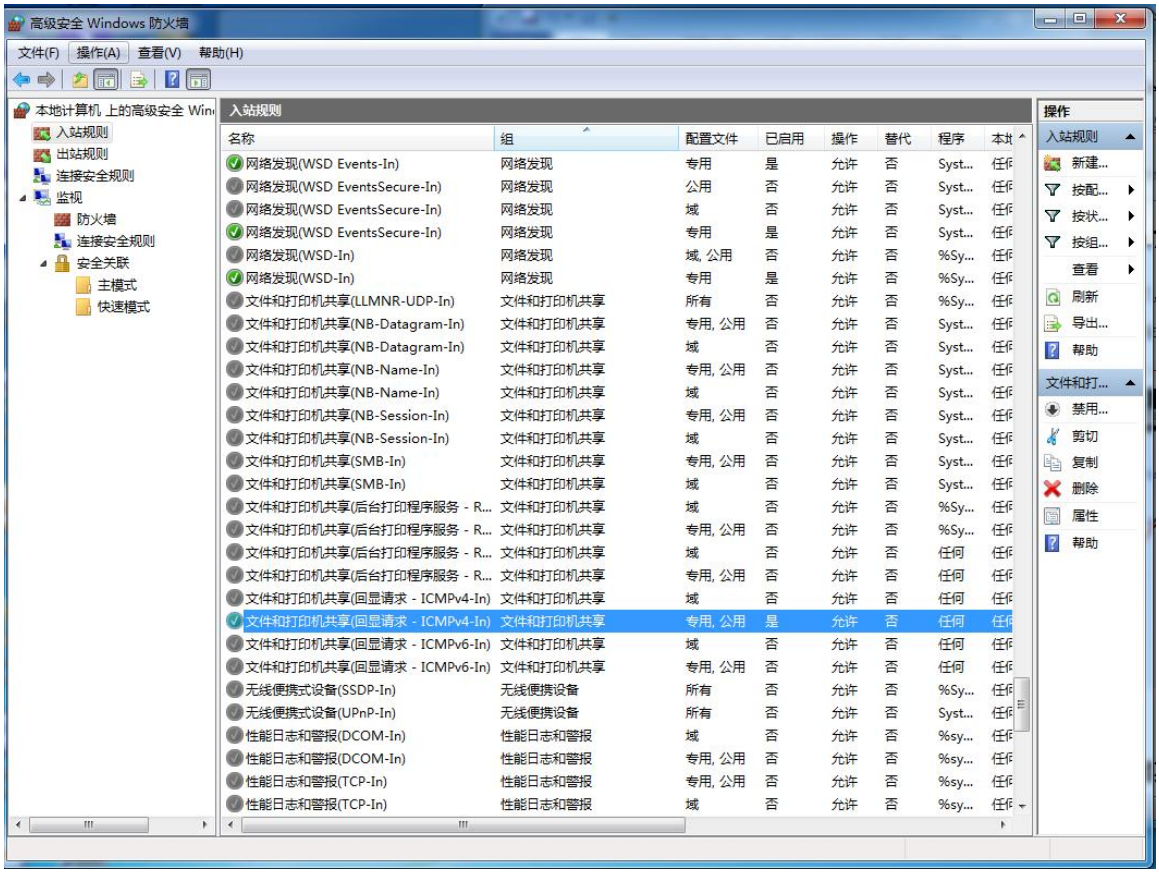
常规	该部分包含规则的标识信息，可以启动或禁用规则，名称最好唯一方便 netsh 管理，操作部分只有三个选项，允许、允许安全、阻止。如果要使用仅允许安全的连接选项，则 IPSec 设置必须在单独的连接安全规则中定义。
程序和服务	程序部分包含如何匹配来自程序的网络数据包信息，两个选择一个是符合指定条件的所有程序（条件就是指其它选项卡设置的条件），还有一个就是指定程序，常规增加的规则都是指定程序。用户程序一般都会标示完整的路径，而系统程序则可能只显示 system。 服务是用来匹配来来自计算机上所有程序和服务、仅服务或指定服务的数据包。设置中有四个选项，一级比一级严格，最后一个应用于具有下列服务短名称的服务一项属于筛选作用。
计算机	该部分可以指定允许或阻止执行该规则的连接的计算机或组帐户。
协议和端口	协议就是指网络流量筛选的协议。
作用域	本地 IP 地址由本地计算机用于确定规则是否适用。规则仅适用于通过配置为使用一个石碇本地 IP 地址的网络适配器匹配规则。 远程 IP 地址则指定应用规则的远程 IP 地址，如果目标 IP 地址是列表中的地址之一，则网络流量匹配规则。
高级	高级部分可以修改应用此防火墙规则的配置文件和接口类型。 配置文件的适用连接范围，Windows 7 可以根据网络适配器的网络位置应用相应的配置文件，支持三种配置文件（域、专用和公用）。 接口类型是指定应用连接安全规则的接口类型，支持所有、局域

	网、远程和无线的任意组合。 边缘遍历可以允许计算机接受未经请求的入站数据包，这些数据包已通过边缘设备（NAT 路由器或防火墙）。
用户	用户部分可以用来设置指定哪些用户或用户组可以连接到计算机。

5.5 win7 防火墙开启 ping

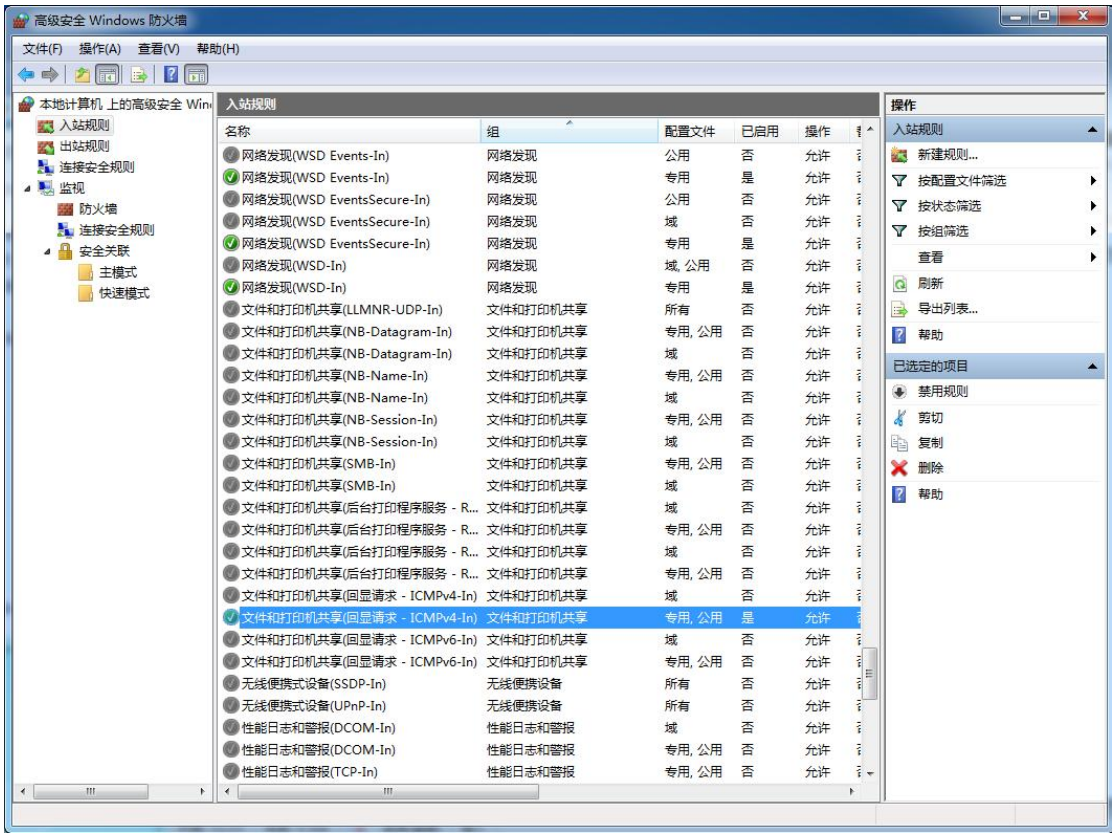
默认情况下，Windows7 出于安全考虑是不允许外部主机对其进行 Ping 测试的。但在局域网环境中，Ping 是测试网络情况的常用手段，如何允许 Windows7 的 ping 测试回显呢?

打开：控制面板 -> 系统和安全 -> windows 防火墙，接下来操作如下图：

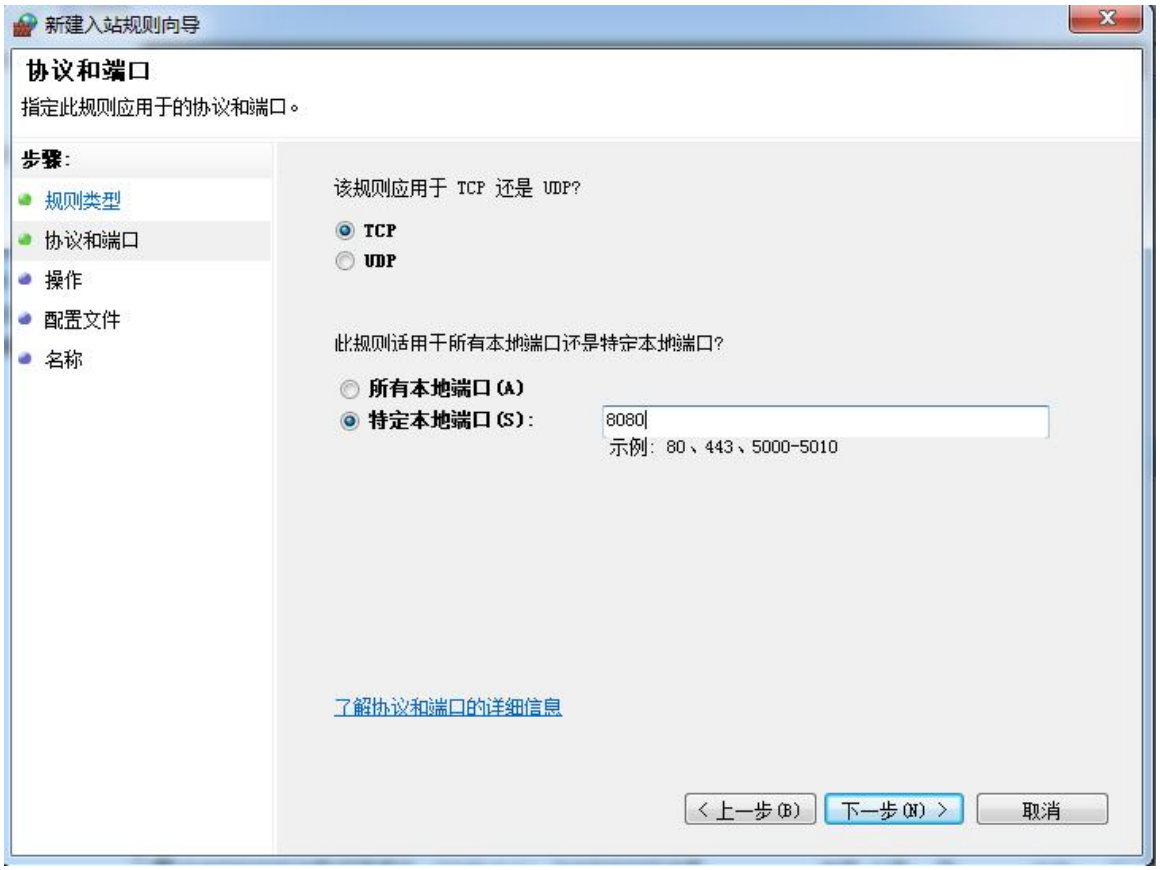


5.6 开放某个端口号

设置入站规则（入站规则：别人电脑访问自己电脑；出站规则：自己电脑访问别人电脑），点击“新建规则”。



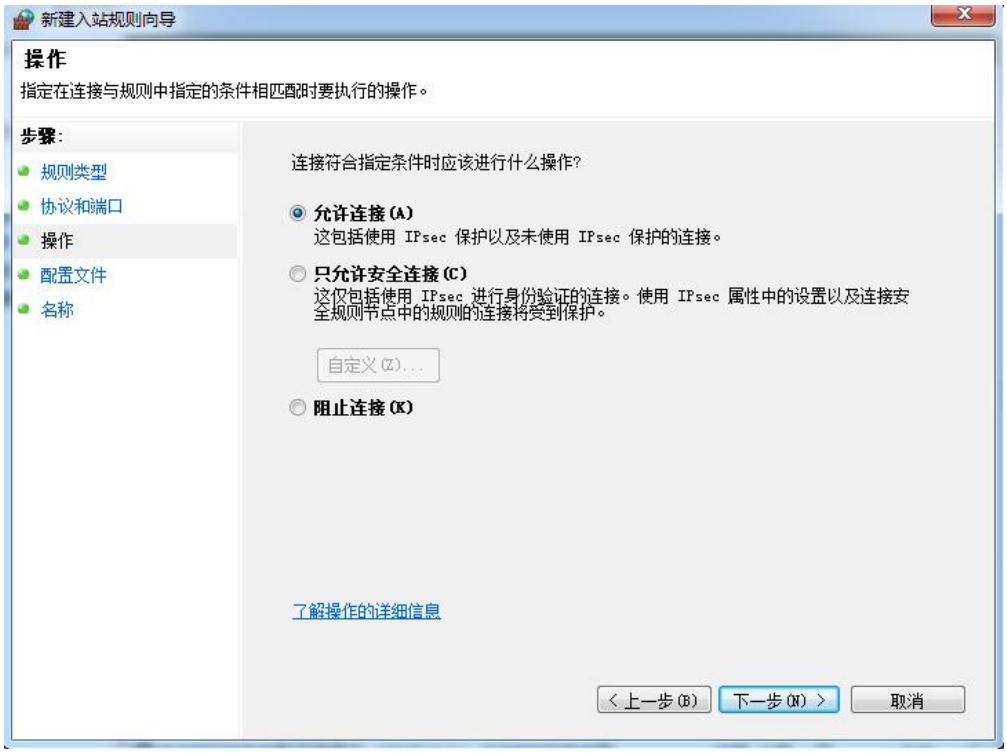
点选“端口”，单击 “下一步”，如下图所示。

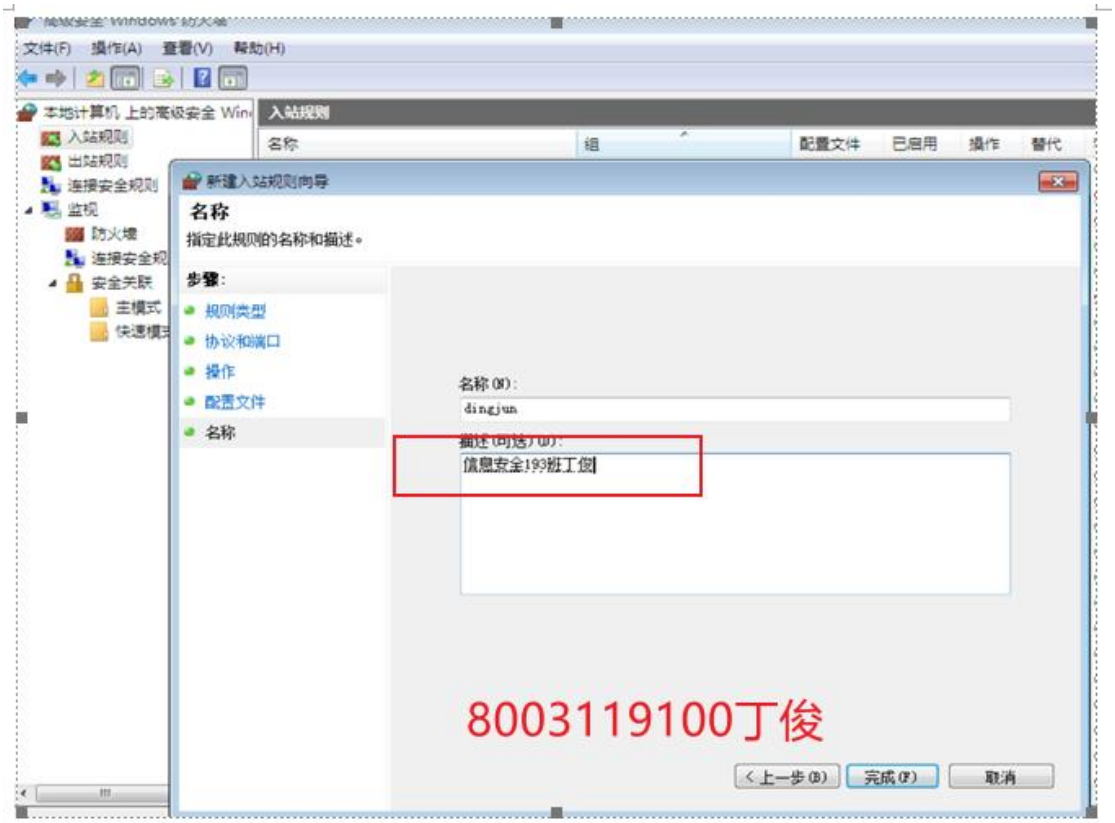


6、选择相应的协议，如添加 8080 端口，我们选择 TCP，在特定本地端口处输入 8080。

7、选择“允许连接”，点击“下一步”按钮。

8、勾选“域”，“专用”，“公司”，点击“下一步”按钮，如下图所示。





五、结果分析与实验体会（试验中遇到的问题及解决过程，产生的错误及原因分析，试验体会和收获）

这一次再一次学习了防火墙的出站入站规则以及防火墙高级设置的使用，再一次的巩固了防火墙知识，获益匪浅。