第5章 个人防火墙配置实验

5.1 实验目的

个人防火墙配置实验要求熟练使用 Windows 系统自带的防火墙实现如下功能。

- 利用个人防火墙防范不安全的程序及端口。
- 利用个人防火墙配置连接安全规则。
- 利用命令行工具 netsh 配置防火墙。

5.2 实验环境

实验主机操作系统为 Windows 7。

5.3 实验工具

Windows 防火墙：防火墙是一项协助确保信息安全的设备，会依照特定的规则，允许或限制传输的数据通过。防火墙可以是一台专属的硬件，也可以是架设在一般硬件上的一套软件。顾名思义，Windows 防火墙就是在 Windows 操作系统中自带的软件防火墙。

5.4 实验内容

5.4.1 实验原理

1. 防火墙概述

在网络安全领域，防火墙指的是置于不同网络安全区域之间的、对网络流量或访问行为实施访问控制的安全组件或一系列安全组件的集合。防火墙的访问控制机制有点类似于大楼门口的门卫。本质上，防火墙在内部与外部两个网络之间建立一个安全控制点，并根据具体的安全需求和策略，对流经其上的数据通过允许、拒绝或重新定向等方式控制网

络的访问，达到保护内部网络免受非法访问和破坏的目的。

防火墙的防护作用发挥必须满足下列条件：一是由于防火墙只能对流经它的数据进行控制，因此在对防火墙设置时，必须让其位于不同网络安全区域之间的唯一通道上；二是防火墙按照管理员设置的安全策略与规则对数据进行访问控制，因此管理员必须根据安全需求合理设计安全策略和规则，以充分发挥防火墙的功能；三是由于防火墙在网络拓扑结构位置的特殊性及在安全防护中的重要性，防火墙自身必须能够抵挡各种形式的攻击。

防火墙在执行这种网络访问控制时，会有两种不同的安全策略：一是定义禁止的网络流量或行为，允许其他一切未定义的网络流量或行为，即默认允许策略；二是定义允许的网络流量或行为，禁止其他一切未定义的网络流量或行为，即默认禁止策略。从安全角度考虑，第一种策略便于维护网络的可用性，第二种策略便于维护网络的安全性，因而在实际情况中，特别是在面对复杂的网络时，安全性应该受到更高重视的情况下，第二种策略使用得更多，这也符合安全的“最小化原则”。

就目前的防火墙技术来看，防火墙并不能有效地应对以下安全威胁：一是来自网络内部的安全威胁；二是通过非法外联的攻击；三是计算机病毒；四是开放服务的漏洞；五是针对网络客户程序的攻击；六是使用隐蔽通道进行通信的特洛伊木马；七是网络钓鱼攻击和其他由于工程或不当配置等人为因素而导致的安全问题。通过引入网络数据深度检测技术，下一代防火墙将能有效应对上述第 3～6 种类型的安全威胁。

2. 常用防护墙技术

(1) 包过滤

包过滤是应用最为广泛的一种防火墙技术，通过对网络层和传输层包头信息的检查，确定是否应该转发该数据包，从而可将许多危险的数据包阻挡在网络的边界处。转发的依据是用户根据网络的安全策略所定义的规则集，对于那些危险的、规则集不允许通过的数据包，直接丢弃，只有那些确信是安全的、规则允许的数据包，才进行转发。规则集通常对下列网络层及传输层的包头信息进行检查：源和目的的 IP 地址、IP 的上层协议类型、TCP 和 UDP 的源及目的端口及 ICMP 的报文类型和代码等。根据规则集的定义方式不同，包过滤技术分为静态包过滤和动态包过滤两种。

静态包过滤检查单个的 IP 数据中的网络层信息和传输层信息，不能综合该数据包在信息流中的上下文环境，合理配置能够提供相当程度的安全能力。制订合理的规则集是静态包过滤防火墙的难点所在，通常网络安全管理员通过下面三个步骤来定义过滤规则：一是制定安全策略，通过需求分析，定义哪些流量与行为是允许的，哪些流量与行为是应该禁止的；二是定义规则，以逻辑表达式的形式定义允许的数据包，表达式中明确指明包的类型、地址、端口、标志等信息；三是用防火墙支持的语法重写表达式。静态包过滤速度快，但是配置困难，防范能力有限。

动态包过滤技术也称为基于状态检测包过滤技术，不仅检查每个独立的数据包，还会试图跟踪数据包的上下文关系。为了跟踪包的状态，动态包过滤防火墙在静态包过滤防火墙的基础上记录网络连接状态信息以帮助识别，如已有的网络连接、数据的传出请求

等。应用动态包过滤技术可截断所有传入的通信，而允许所有传出的通信，这是静态包过滤技术无法做到的功能。动态包过滤提供了比静态包过滤更好的安全性能，同时仍保留了其用户的透明特性。

(2) 应用代理

应用代理工作在应用层，能够对应用层协议的数据内容进行更细致的安全检查，从而为网络提供更好的安全特性。使用应用代理技术可以让外部服务用户在受控制的前提下使用内部网络服务。比如，一个邮件应用代理程序可以理解 SMTP 协议与 POP3 协议的命令，并能够对邮件中的附件进行检查。对于不同的应用服务必须配置不同的代理服务程序。

相比包过滤技术，应用代理技术可以更好地隐藏内部网络的信息、具有强大的日志审核和对可实现内容的过滤，但同时对于每种不同的应用层服务都需要不同的应用代理程序，处理速度慢，无法支持公开协议的服务。在实际应用中，应用代理更多地还是与包过滤技术结合起来协同工作。

(3) NAT 代理

NAT 是 Network Address Translation(网络地址转换)的缩写，用来允许多个用户分享单一的 IP 地址，同时为网络连接带来一定的安全性。NAT 工作在网络层，所有内部网络发往外部网络的 IP 数据包，在 NAT 代理处，完成 IP 包的源地址部分和源端口像代理服务器的 IP 地址和指定端口的映射，以代理服务器的身份送往外部网络的服务器；外部网络服务器的相应数据包回到 NAT 代理时，在 NAT 代理处，完成数据包的目标 IP 地址和端口向真正请求数据的内部网络中某台主机的 IP 地址和端口的转换。

NAT 代理一方面为充分使用有限的 IP 地址资源提供了方法，另一方面隐藏了内部主机的 IP 地址，且对用户完全透明。

(4) 网络数据深度检测

网络数据深度检测是指不仅对网络数据的协议及其状态进行检测，还对数据内部进行深入分析，包括特定的数据内容、数据流量行为特征等。根据检查内容的不同，网络数据深度检测可分为深度包检测(DPI)技术和深度流检测(DFI)技术。

DPI 技术不仅对数据包的 IP 层进行检查，还能对数据包内容进行检查，每个应用协议都有自己的数据特征，充分理解各种应用协议的变化规律和流程可以准确快速地识别出相应遵循的应用协议，从而达到对应用的精确识别和控制。

DFI 通过分析网络数据流量行为特征来识别网络应用的需要，及时分析某种应用数据流的行为特征并创建特征模型，检测的准确性取决于特征模型的准确性。一般 DFI 主要用于区分大类的应用，对于数据流特征不明显的且应用协议多变的应用则很难通过 DFI 技术进行识别。

3. 防火墙分类

(1) 个人防火墙

个人防火墙位于计算机与其所连接的网络之间，主要用于拦截或阻断所有对主机构成威胁的操作。个人防火墙是运用于主机操作系统内核的软件，根据安全策略制定的规

则对主机所有的网络信息进行监控和审查，包括拦截不安全的上网程序、封堵不安全的共享资源及端口、防范常见的网络攻击等，以保护主机不受外界的非法访问和攻击，其主要采用的是包过滤技术。

（2）网络防火墙

网络防火墙位于内部网络与外部网络之间，主要用于拦截或阻挡所有对内部网络构成威胁的操作。网络防火墙的硬件和软件都单独进行设计，由专用网络芯片处理数据包，并且采用专用操作系统平台，具有很高的效率，技术上集包过滤技术和应用网关技术于一身。

5.4.2 实验步骤

1. 查看个人防火墙的默认规则

打开 Windows 系统自带的防火墙，其界面如图 5-1 所示。

图 5-1 Windows 系统自带的防火墙

单击图 5-1 左侧的“高级设置”项，查看防火墙的出入站规则、连接安全规则，如图 5-2 所示，双击规则即可查看详情。

单击图 5-1 左侧的“允许应用或功能通过 Windows 防火墙”，可查看系统对程序通信是否允许的情况，如图 5-3 所示。

2. 添加出入站规则

添加出入站规则可实现对出入网络流量的管理，以添加对南京邮电大学官网的访问规则为例。首先，利用 ping 命令获取南京邮电大学的 IP 地址，如图 5-4 所示。

接着，建立新出站规则，使防火墙拒绝对该 IP 地址的出站请求，如图 5-5 所示。

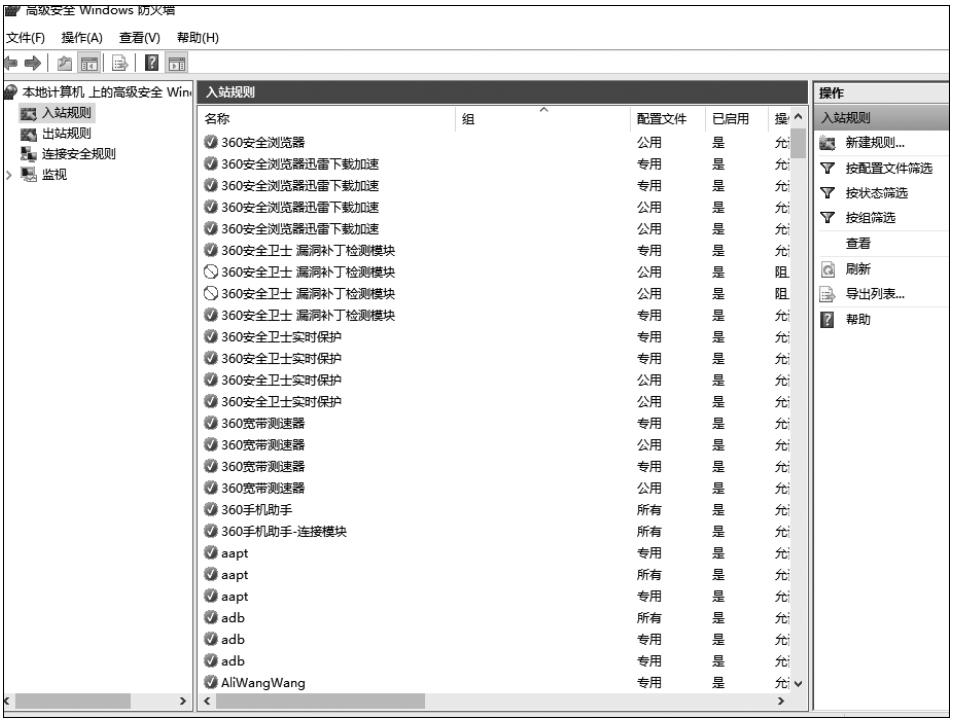

图 5-2　查看防火墙的出入站规则、连接安全规则

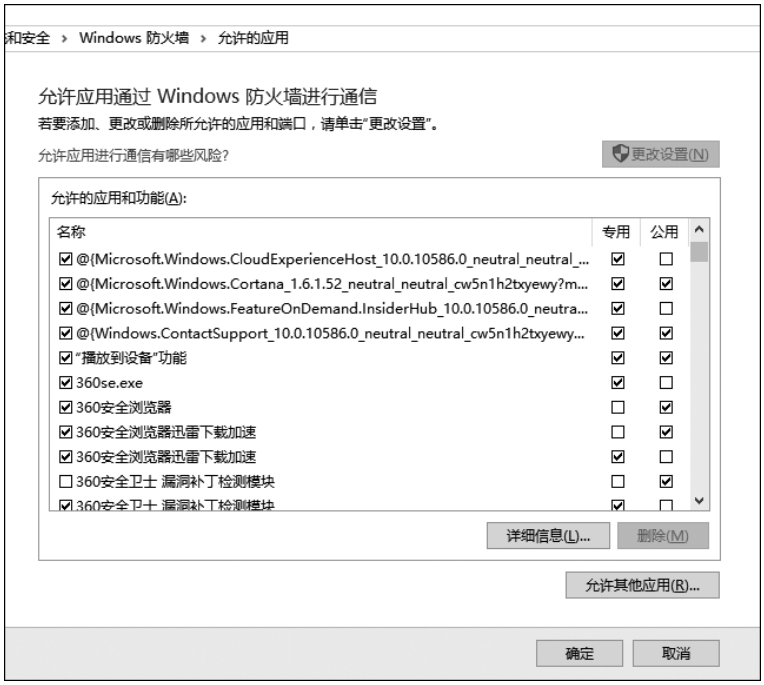

图 5-3　查看系统对程序通信是否允许的情况

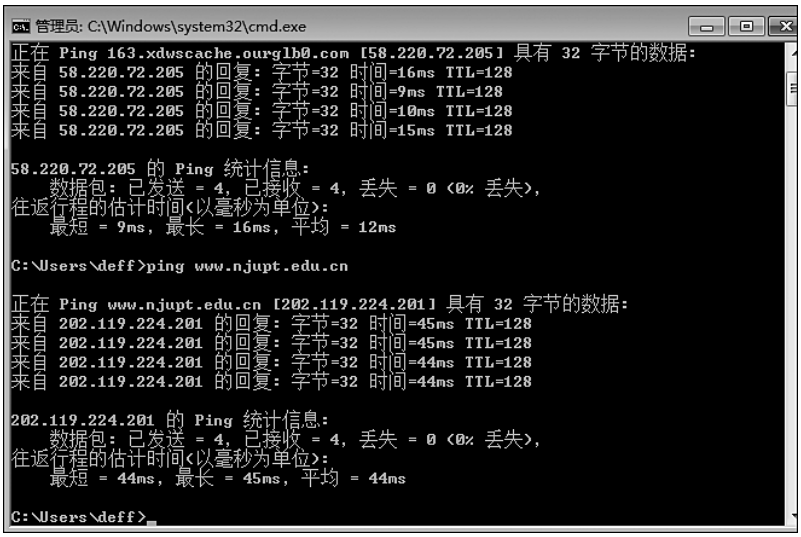

图 5-4　获取南京邮电大学的 IP 地址

图 5-5　建立新出站规则拒绝对该 IP 地址的出站请求

出站规则添加成功后,输入“202.119.224.201”将无法访问南京邮电大学官网,如图 5-6 所示。

3. 防范不安全的程序

添加程序及设置端口规则可实现对程序访问网络、端口访问网络的管理,以添加 360 浏览器对网络的访问规则为例。首先,添加程序出站规则,找到所要添加的程序路径,如图 5-7 所示。

图 5-6　出站规则添加成功

图 5-7　找到要添加的程序路径

接着，找到该程序，选择“阻止连接”，并对规则进行命名。规则添加成功后，返回出站规则界面，如图 5-8 所示。

由此，实现了对 360 浏览器访问网络功能的阻止，如图 5-9 所示。

4. 使用 netsh 配置防火墙

在提供界面操作的同时，Windows 系统的 netsh 文件还提供了命令行下对防火墙等

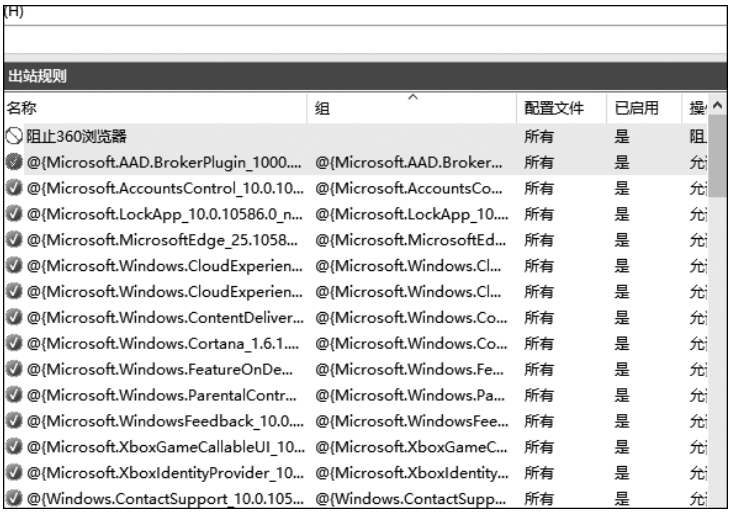

图 5-8　返回出站规则界面

图 5-9　实现了对 360 浏览器访问网络功能的阻止

许多网络设置的配置方法，便于远程管理。

(1) 查看防火墙

在命令行下打开 netsh 文件，输入“advfirewall firewall”，查看 firewall 命令，如图 5-10 所示。

输入“show rule name=all”，查看防火墙所有规则，如图 5-11 所示。

输入“firewall show logging”，查看防火墙配置记录，如图 5-12 所示。

(2) 防火墙的开启和关闭

在“netsh advfirewall firewall”环境下，输入“set allprofiles state on|off”，可实现防火

图 5-10　查看 firewall 命令

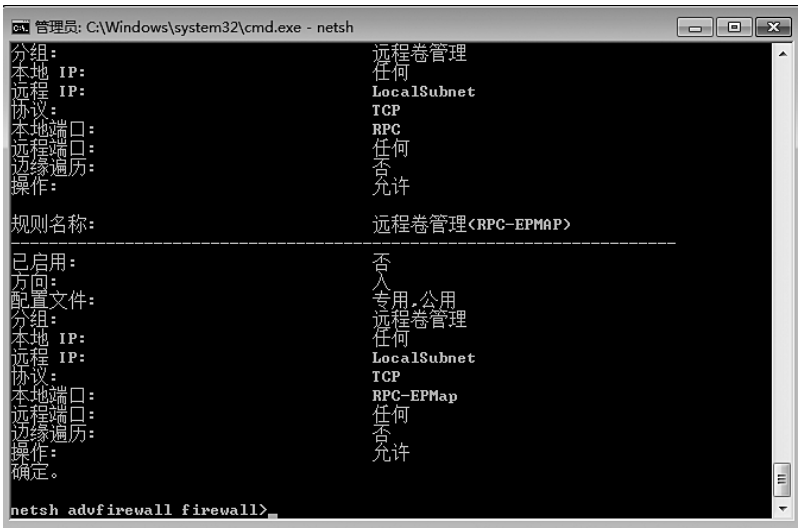

图 5-11　查看防火墙所有规则

墙的开启和关闭。

(3) 端口的开启和关闭

在“netsh advfirewall firewall”环境下，输入“firewall add|delete portopening TCP|UDP”加端口号，可实现对指定端口的开启或关闭。如开启 TCP 455 端口的命令为“firewall add portopening TCP 445 Netbios-ds”。

(4) 出入站规则配置

在“netsh advfirewall firewall”环境下，输入“show rule-”，可查看防火墙的所有规则；输入“add | delete rule name = < string > dir = in | out action = allow | block | bypass

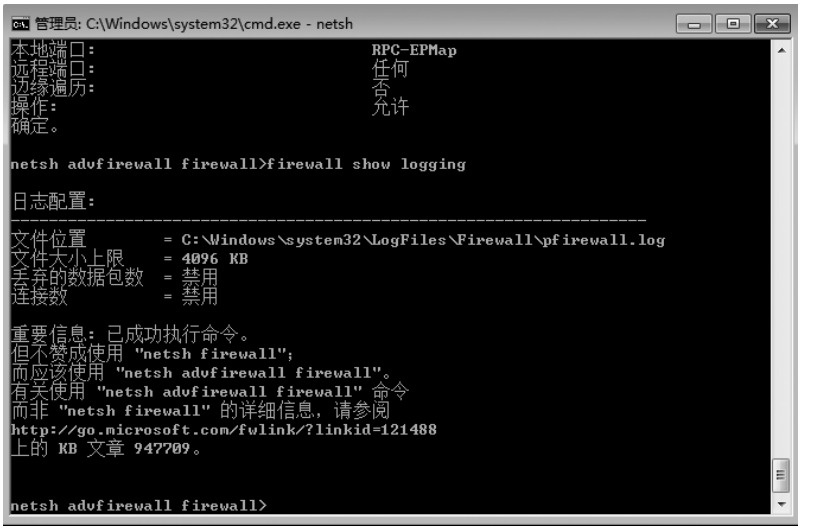

图 5-12　查看防火墙配置记录

[protocol=0-255]”,可在防火墙策略中添加或删除入站或出站规则。

5.5　实验结果分析与总结

防火墙是一种应用广泛的网络防护技术,在具体应用时,防火墙的部署和配置非常重要,部署不当或配置不当的防火墙不仅不能提供安全性,还会给网络管理员和用户带来安全上的错觉。本实验通过对个人防火墙的配置,使读者可以了解个人防火墙的工作原理,掌握配置方法。

5.6　思考题

在本次实验中,若对常见的网络功能进行限制,该如何设置? 典型的包过滤路由使用了什么信息? 理解防火墙的三个设计目标。

解析:

典型的包过滤路由使用源 IP 地址,目的 IP 地址,源端和自由端传输层地址,IP 协议域,接口。

三个设计目标分别如下。

① 所有入站和出站的网络流量都必须通过防火墙。

② 只有经过授权的网络流量,防火墙才允许其通过。

③ 防火墙本身不能被攻破,这意味着防火墙应该允许在安全操作系统的可信系统上。