# (精华)国家开放大学电大专科《网络系统管理与维护》形考任务2答案

来源：网络 作者：紫云飞舞 更新时间：2025-06-25

*国家开放大学电大专科《网络系统管理与维护》形考任务2答案形考任务2理解计算机病毒防范的常用方法，掌握安装和配置防病毒软件【实训目标】理解计算机病毒防范的常用方法，掌握安装和配置防病毒软件。【实训环境】1台服务器、1台工作站计算机。【实训内容...*

国家开放大学电大专科《网络系统管理与维护》形考任务2答案

形考任务2

理解计算机病毒防范的常用方法，掌握安装和配置防病毒软件

【实训目标】

理解计算机病毒防范的常用方法，掌握安装和配置防病毒软件。

【实训环境】

1台服务器、1台工作站计算机。

【实训内容】

假设您是一家公司的网络系统管理员，负责公司的网络安全管理工作。为此，请您完成以下工作：

1.部署网络版杀毒软件的控制中心。

2.设置控制中心，每天11点在线同步病毒库。

3.安装网络版杀毒软件的客户端程序。

4.设置控制中心，每天19点扫描客户端计算机。

（可以参考教材“3.2.6

防病毒软件配置”章节部分，完成以上四步操作）

5.使用服务器上的高级安全Windows防火墙功能，阻止对其53、80和443端口的访问。（可以参考教材“3.3.3

Windows防火墙的基本配置”章节部分，完成操作）

6.使用ccProxy代理软件，配置8080端口来代理企业内网用户访问Web服务。（可以参考教材“3.6

代理服务”章节部分，完成操作）

实习步骤：

由于天网防火墙有正式版（收费的版本，服务好，功能强）和试用版（免费，用的人很多，高级功能受一些限制）之分，本人支持正版软件，所以这里就以正式版为例给大家介绍，试用版的界面和操作基本都一样，使用试用版的可以参考类似的操作。

安装完后要重起，重起后打开天网防火墙就能起到作用了。默认情况下，它的作用就很强大了。但有时它苛刻的IP规则也带来了很多不便，后面再说。所以，如果没什么特殊要求的，就设置为默认就OK了，安全级别为中就好。

一、普通应用（默认情况）略

二、防火墙开放端口应用

如果想开放端口就得新建新的IP规则，所以在说开放端口前，我们来说说怎么新建一个新的IP规则，如下图1，在自定义IP规则里双击进行新规则设置。此主题相关图1如下：

图1

IP规则

点击增加规则后就会出现以下图所示界面，我们把它分成四部分。

此主题相关图片如下图2：

图2

IP规则修改

1）图六1是新建IP规则的说明部分，你可以取有代表性的名字，如“打开BT6881-6889端口”，说明详细点也可以。还有数据包方向的选择，分为接收，发送，接收和发送三种，可以根据具体情况决定。

2）就是对方IP地址，分为任何地址，局域网内地址，指定地址，指定网络地址四种。

3）IP规则使用的各种协议，有IP，TCP，UDP，ICMP，IGMP五种协议，可以根据具体情况选用并设置，如开放IP地址的是IP协议，QQ使用的是UDP协议等。

4）比较关键，就是决定你设置上面规则是允许还是拒绝，在满足条件时是通行还是拦截还是继续下一规则，要不要记录，就看你自己想怎么样了，具体看后面的实例。如果设置好了IP规则就单击确定后保存并把规则上移到该协议组的置顶，这就完成了新的IP规则的建立，并立即发挥作用。

三、打开端口实例

在介绍完新IP规则是怎么建立后，我们就开始举例说明，毕竟例子是最好的说明。大家也许都知道BT使用的端口为6881－6889端口这九个端口，而防火墙的默认设置是不允许访问这些端口的，它只允许BT软件访问网络，所以有时在一定程度上影响了BT下载速度。当然你关了防火墙就没什么影响了，但机器是不是就不安全了？所以下面以打开6881－6889端口举个实例。

1）在图1双击后建立一个新的IP规则后在出现的下图3里设置，由于BT使用的是TCP协议，所以就按下图3设置就OK了，点击确定完成新规则的建立，我命名为BT。

此主题相关如下图3：

图3

BT的IP规划设置

设置新规则后，把规则上移到该协议组的置顶，并保存。然后可以进行在线端口测试是否BT的连接端口已经开放的。

此主题相关如下图4：

图4

保存设置规则

四、应用自定义规则防止常见病毒

上面介绍的是开放端口的应用，大体上都能类推，如其他程序要用到某些端口，而防火墙没有开放这些端口时，就可以自己设置，相信大家能搞定。下面来介绍一些实例的应用，就是封端口，让某些病毒无法入侵。

1、防范冲击波

冲击波，这病毒大家熟悉吧？它是利用WINDOWS系统的RPC服务漏洞以及开放的69、135、139、445、4444端口入侵。

如何防范，就是封主以上端口，首先在图八里见到的“禁止互联网上的机器使用我的共享资源”这项的起用（就是打勾）就已经禁止了135和139两个端口。

下边是禁止4444端口的图九

此主题相关如下图5：

图5

禁止TCP4444端口

下面是禁止69和445端口的图，图6为69，图7为445

此主题相关图片如下：

图6

禁止TCP69端口

图7

禁止TCP445端口

建立完后就保存，记得保存，很多人就是不记得保存。保存完后就可以防范冲击波了，补丁都不用打，爽吧？

2、防范冰河木马

冰河，熟悉了吧？也是比较狠的病毒哦，它使用的是UDP协议，默认端口为7626，只要在防火墙里把它给封了，看它还能怎么样？具体见下图8。

此主题相关图片如下：

图8

禁止UDP端口7626

如你掌握一些病毒的攻击特性及其使用的端口就可以参照上面的方法设置，其实设置都差不多，大家可以参照，可以大大防范病毒和木马的攻击！

五、下面介绍怎么打开WEB和FTP服务

相信不少朋友都使用了FTP服务器软件和WEB服务器，放火墙不仅限制本机访问外部的服务器，也限制外部计算机访问本机。

所以我们为了WEB和FTP服务器能正常使用就得设置防火墙，首先在图八把“禁止所有人连接”前的勾去掉。

以下是WEB和FTP的IP规则供大家参考上图9为WEB，下图10为FTP。此主题相关图片如下：

图9

开放WEB服务

图10

开放FTP服务

六、常见日志的分析（仅供参考）

使用防火墙关键是会看日志，看懂日志对分析问题是非常关键的，大家看下图，就是日志记录，上面记录了不符合规则的数据包被拦截的情况，通过分析日志就能知道自己受到什么攻击。下面我们就来说说日志代表的意思。此主题相关图片如下：

图11

日志记录

看上图，一般日志分为三行，第一行反映了数据包的发送、接受时间、发送者IP地址、对方通讯端口、数据包类型、本机通讯端口等等情况；第二行为TCP数据包的标志位，共有六位标志位，分别是：URG、ACK、PSH、RST、SYN、FIN，在日志上显示时只标出第一个字母，他们的简单含义如下：

ACK：确认标志

提示远端系统已经成功接收所有数据

SYN：同步标志

该标志仅在建立TCP连接时有效，它提示TCP连接的服务端检查序列编号FIN：结束标志

带有该标志位的数据包用来结束一个TCP会话，但对应端口还处于开放状态，准备接收后续数据。

RST：复位标志，具体作用未知

其他不知道了，呵呵

第三行是对数据包的处理方法，对于不符合规则的数据包会拦截或拒绝，对符合规则的但被设为监视的数据包会显示为“继续下一规则”。

下面举些常见典型例子来讲讲：

记录1：[22：30：56]202、121、0、112

尝试用PING来探测本机

TCP标志：

S

该操作被拒绝

该记录显示了在22：30：56时，从IP地址202、121、0、112

向你的电脑发出PING命令来探测主机信息，但被拒绝了。

人们用PING命令来确定一个合法IP是否存在，当别人用PING命令来探测你的机器时，如果你的电脑安装了TCP/IP协议，就回返回一个回音ICMP包，如果你在防火墙规则里设置了“防止别人用PING命令探测主机”如图八里设置，你的电脑就不会返回给对方这种ICMP包，这样别人就无法用PING命令探测你的电脑，也就以为没你电脑的存在。如果偶尔一两条就没什么大惊小怪的，但如果在日志里显示有N个来自同一IP地址的记录，那就有鬼了，很有可能是别人用黑客工具探测你主机信息，他想干什么？谁知道？肯定是不怀好意的。

记录2：[5：29：11]61、114、155、11试图连接本机的http[80]端口

TCP标志：S

该操作被拒绝

本机的http[80]端口是HTTP协议的端口，主要用来进行HTTP协议数据交换，比如网页浏览，提供WEB服务。对于服务器，该记录表示有人通过此端口访问服务器的网页，而对于个人用户一般没这项服务，如果个人用户在日志里见到大量来自不同IP和端口号的此类记录，而TCP标志都为S（即连接请求）的话，完了，你可能是受到SYN洪水攻击了。还有就是如“红色代码”类的病毒，主要是攻击服务器，也会出现上面的情况。

记录3：[5：49：55]31、14、78、110

试图连接本机的木马冰河[7626]端口

TCP标志：S

该操作被拒绝

这就是个害怕的记录啦，假如你没有中木马，也就没有打开7626端口，当然没什么事。而木马如果已植入你的机子，你已中了冰河，木马程序自动打开7626端口，迎接远方黑客的到来并控制你的机子，这时你就完了，但你装了防火墙以后，即使你中了木马，该操作也被禁止，黑客拿你也没办法。但这是常见的木马，防火墙会给出相应的木马名称，而对于不常见的木马，天网只会给出连接端口号，这时就得\*你的经验和资料来分析该端口的是和哪种木马程序相关联，从而判断对方的企图，并采取相应措施，封了那个端口。

记录4：[6：12：33]

接收到228、121、22、55的IGMP数据包

该包被拦截

这是日志中最常见的，也是最普遍的攻击形式。IGMP（Internet

Group

Management

Protocol）是用于组播的一种协议，实际上是对Windows的用户是没什么用途的，但由于Windows中存在IGMP漏洞，当向安装有Windows

9X操作系统的机子发送长度和数量较大的IGMP数据包时，会导致系统TCP/IP栈崩溃，系统直接蓝屏或死机，这就是所谓的IGMP攻击。在标志中表现为大量来自同一IP的IGMP数据包。一般在自定义IP规则里已经设定了该规则，只要选中就可以了。

记录5：[6：14：20]192、168、0、110的1294端口停止对本机发送数据包

TCP标志：F

A

继续下一规则

[6：14：20]

本机应答192、168、0、110的1294端口

TCP标志：A

继续下一规则从上面两条规则看就知道发送数据包的机子是局域网里的机子，而且本机也做出了应答，因此说明此条数据的传输是符合规则的。为何有此记录，那是你在图八里防火墙规则中选了“TCP数据包监视”，这样通过TCP传输的数据包都会被记录下来，所以大家没要以为有新的记录就是人家在攻击你，上面的日志是正常的，别怕！呵呵！

防火墙的日志内容远不只上面几种，如果你碰到一些不正常的连接，自己手头资料和网上资料就是你寻找问题的法宝，或上防火墙主页上看看，这有助于你改进防火墙规则的设置，使你上网更安全。

七、在线升级功能

现在天网不断推出新的规则库，作为正式版用户当然可以享受这免费升级的待遇，只要在天网界面点击一下在线升级，不到2分钟就可以完成整个升级过程，即快捷又方便。此主题相关如图12：

图12

在线升级

点击后出现一个在线升级网络设置的提示框，如果你没有使用代理上网的就不用设置，直接下一步安装规则包，这样就完成升级了。此主题相关如图13：

图13

在线升级设置1

图13

在线升级设置2

图13

在线升级设置3

升级后防火墙的自定义规则就会多了很多条防御木马的规则，这下可好了不用自己乱设置，只要使用自定义级别就可以了。不过选用自定义后，记得要把自定义里的IP规则选勾保存规则，这样日志才会有记录的。

八、总结

给大家说了也不知道大家能不能看懂，其实防火墙的作用就是隐藏自己真实IP的同时，监控各个端口，并给出日志，让大家分析并找出相应的对策，灵活应用防火墙能给自己机子带来比较高的安全性。当然有些病毒木马是诱导用户主动访问而感染的，就要靠自己提高安全意识来防范了。总之，互联网大了，用的人多了，什么样的人都有，所以给自己机子上装个防火墙是必不可少的基本防御！

五、实训思考题：

1、什么是防火墙？其有什么作用？

2、防火墙有哪些类型？

3、学习设置其它软件防火墙的设置（如瑞星防火墙）。

本DOCX文档由 www.zciku.com/中词库网 生成，海量范文文档任你选，，为你的工作锦上添花,祝你一臂之力！