

# 中国万网独享主机安全使用手册

尊敬的万网用户：

为了提高您所使用主机的安全性，同时为了减少因误操作带来的损失，请注意以下事项。

## 系统安全：

1. 保存好**系统密码**并定期进行修改。
2. 开启**系统自动更新**功能。
3. 开启杀毒软件，经常**更新病毒库**，定期扫描病毒。
4. 做好网站的**注入漏洞检查**，做好网站目录访问权限控制。
5. 慎重**安装硬件驱动**，以免损坏操作系统。
6. 不要**安装路由和远程访问服务**，可能会导致无法远程连接。
7. 慎重**安装防火墙**。
8. 关闭**不需要的服务**，防止远程入侵。
9. 启用**TCP/IP筛选功能**，关闭危险端口，防止远程扫描、蠕虫和溢出攻击。
10. 修改%system32%目录下的**默认程序命令名字**，防止溢出和远程操作。

## 网络安全：

1. 不要**禁用网卡**，否则即使重启计算机也无法启用网卡。
2. 禁止占用其它**IP地址**，由此引起的后果需您自行承担。
3. 为了避免网络中其它主机的**ARP欺骗**攻击，我们已在网关上绑定了您的**IP**和**mac**地址，请自行下载客户端程序在您的主机绑定网关的**IP**和**mac**地址。

## 数据安全：

1. 建议把**软件安装、数据定时备份**放在D区。
2. 建议将您的数据放在D区，并在本地**保留数据备份**，以免硬件损坏造成数据丢失。

附：服务器服务简单配置说明

**服务器安全的宗旨：最小的权限 + 最少的服务 = 最大的安全**

## 系统安全

1. 建议您保存好系统密码并定期修改；设置一个复杂的密码组合[字母+数字+特殊符号+16位以上]，并定期或不定期更换密码组合规律。

选择“我的电脑” → 右键“管理”。如图1



图1

“本地用户和组” → “用户”找到你的那个管理员账号。如图2



图2

右键点击设置密码。那个提示WINDOWS的一个安全警告，并不影响你的使用。如图3



图3

直接输入新密码，点击确定后，修改密码成功。如图4



图4

2. 建议开启系统自动更新功能；根本有效的安全维护之道,简单易行.防止系统本身和附加软件BUG导致的远程溢出攻击和蠕虫攻击。

选择“我的电脑” → 右键“属性” 。如图5



图5

“系统属性” → “自动更新”，建议您选择每天凌晨进行更新操作。如图6



图6

### 3. 开启杀毒软件，经常更新病毒库，定期扫描病毒。（以系统自带诺顿杀毒软件为例）

①. 选择“开始→程序→Symantec Client Securiry →Symantec AntiVirus 客户端”，进入管理页面。如图

7

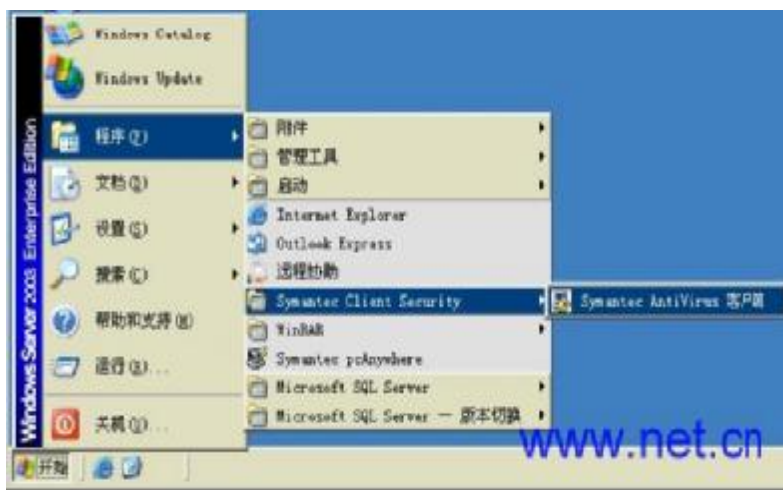


图7

在 Symantec AntiVirus 的"文件"菜单上,单击"调度更新"。如图8



图8

在"调度病毒定义更新"对话框中,选中"启用调度的自动更新"。(注意:这既更新了病毒定义也更新了安全风险定义)如图9

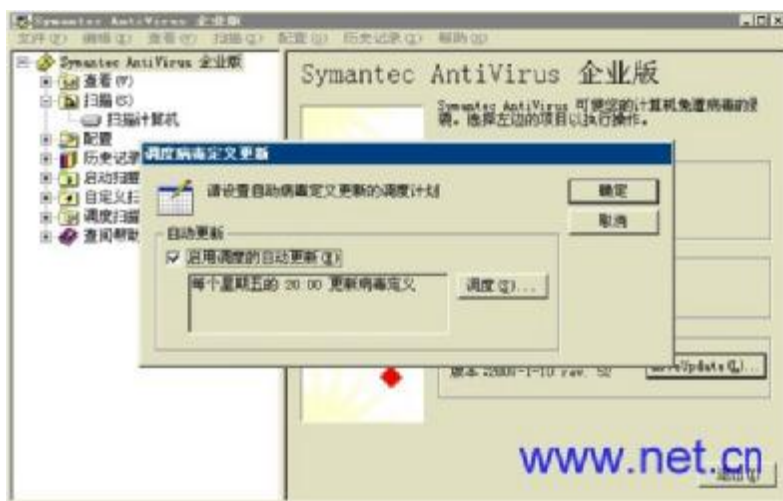


图9

在"调度病毒定义更新"对话框中，单击"调度"，可以根据情况选择自动更新频率和时间，点击确定即可，建议您选择每天凌晨进行更新操作。如图10

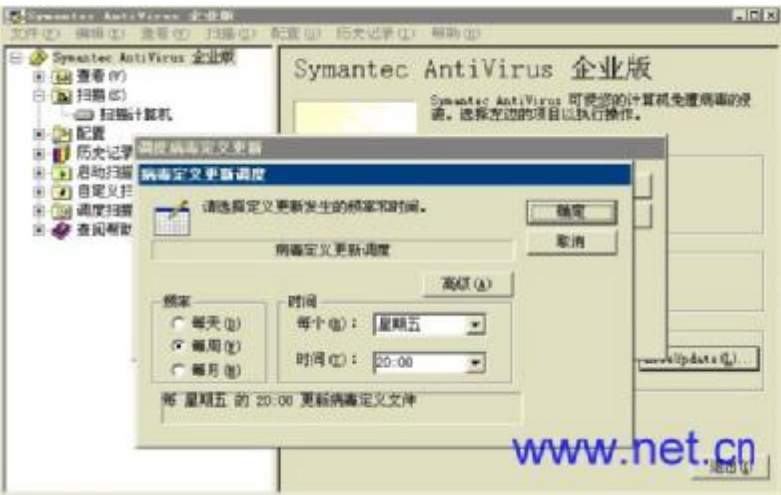


图10

②设置完自动更新病毒库后，进行设置诺顿的定时扫描。

在 Symantec AntiVirus 的"编辑"菜单上，单击"新建调度扫描"。 如图11



图11

输入“名称”和“说明”，点击下一步。如图12



图12

选择扫描的频率和时间，选好后点击下一步。（建议选择每天凌晨进行病毒的查杀，那时登陆到服务器的人肯定很少了，有利扫描的速度，也不影响上传、下载的用户的速度）如图13



图13

选择需要扫描病毒的磁盘，建议全部选中，保存后设置完毕。如图14



图14

#### 4. 请注意做好网站的注入漏洞检查，同时做好网站目录访问权限控制。

- ①.对每个网站单独设立帐户进行管理，设置访问权限为本帐户所在目录，禁止跨帐户访问其它网站目录。
- ②.定期维护WEB服务器，仔细检查web目录下的文件，定期比较备份文件和web目录文件，以及时发现web木马文件。
- ③. 硬盘设置为NTFS格式，但切记不要运行不明程序，防止NTFS流攻击。（服务器默认为NTFS）
- ④. 了解和防止SQL注入、暴库、上传、远程文件包含等严重的漏洞，关注网站程序的最新漏洞信息，并及时打补丁。

提示：根据网站的实际情况，可以选择禁止服务器fso组件，防止webshell木马的远程操作：

#### 5. 请慎重安装硬件驱动，以免损坏操作系统。

#### 6. 不要安装路由和远程访问服务，会导致无法远程连接。

打开“开始”菜单→“设置选项”中的“控制面板”选项，点击“管理工具”进入，打开“路由和远程访问”选项。如图15



图15

默认相关服务是停止状态，建议您不要启用相关服务。如图16



图16

## 7. 请慎重安装防火墙。

如果需要安装防火墙，建议使用WINDOWS自带的防火墙，注意在启用防火墙前一定要先设定好“例外”，至少要添加好远程连接的端口（如TCP3389、5631等端口）后再开启，以免开启后所有端口全部被禁止连接。

打开“开始”菜单→“设置选项”中的“控制面板”选项，点击“Windows 防火墙”进入。**(万网建议使用Windows自带的防火墙，建议不要安装其他防火墙软件)**如图17



图17

在“常规”选项卡中选择“启用”，“不允许例外”选项绝对不要选择。如图18



图18

在“例外”选项卡中，首先要选中“pcanywhere”“远程桌面”的所有服务，以便可以正常远程连接服务器。

如图19



图19

可以通过点击下面的“添加程序”和“添加端口”，手工添加你自定义的服务，比如添加FTP服务的21端口。

如图20



图20

确定后就可以正常使用选中的服务，而不会受到防火墙的屏蔽。如图21



图21

在“高级”选项卡中，网络连接设置最好全部选中，然后点击ICMP的“设置”按钮。如图22



图22

进入ICMP设置，**icmp**的全称是**internet control messenge protocol**，**internet**控制信息协议，一般通过**icmp**的反馈信息来确定网络的状态，比如连接服务器通不通，是否有拥塞等等。实际例子中，比如**ping**一个服务器**ip**地址，就是**icmp**把**ping**的结果返回给**ping**命令的发送着，从而让发送着知道网络和服务器的状态。实际上**icmp**的作用很多的，可以适当的打开或关闭某些功能。当选定鼠标所指的选项时，下方会出来相应的描述信息，可以安装我们的要求进行配置，建议您至少选中“允许转入回显请求”，以便判断服务器的运行状态。

如图23



图23

8.关闭不需要的服务，防止远程入侵。

比如:server服务，Remote Registry服务，Task Scheduler服务等，既提高服务器性能，又可以提高安全性质。(注:具体要关闭的服务比较多，请根据实际情况设置)

打开“开始”菜单→“设置选项”中的“控制面板”选项，点击“管理工具”进入，打开“服务”选项。如图24



图24

在“服务”对话框中，显示全部服务器的加载服务，请您根据情况进行服务的启动和停止。如图25

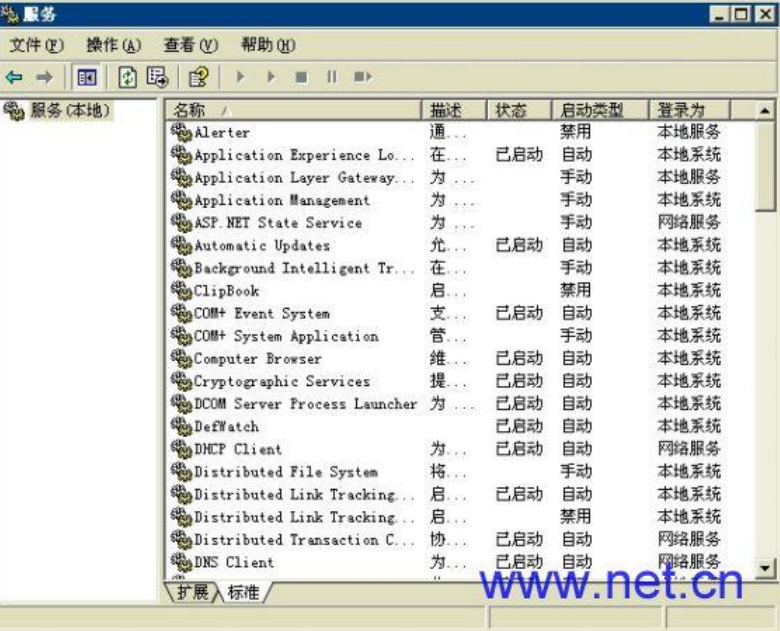


图25

请注意iis的www（World Wide Web Publishing Service）服务必须要设置为自动启动（默认是手工启动），否则服务器重启后，设置站点将不能正常访问。

设置方法：双击World Wide Web Publishing Service选项。如图27



图27

打开World Wide Web Publishing Service属性对话框，启动类型选择：自动，确定保存即可。如图28



图28

9.启用TCP/IP筛选功能，关闭危险端口，防止远程扫描、蠕虫和溢出攻击。

独享服务器开放的端口：

443 (https) 、80(web服务) 、21(ftp服务) 、5631(Pcanywhere) 、1433(Mssqlserver)

22(Ssh)、110,25(mailserver) 、3306(Mysqlserver)、3389 (远程桌面连接)

防火墙除了开放常用端口（见常用端口配置表），另有**40个**活动端口供用户使用，为**TCP30000—30020**和**UDP 30000—30020**；其他端口都是封闭的,如果需要一些没有开放的端口,那么请映射到上述高端端口。

打开“开始”菜单→“设置选项”中的“控制面板”选项，点击“网络连接”进入，双击“本地连接”，点击“属性”按钮。如图29



图29

在“本地连接属”性对话框，选中“Internet协议(TCP/IP)”,双击进入。如图30

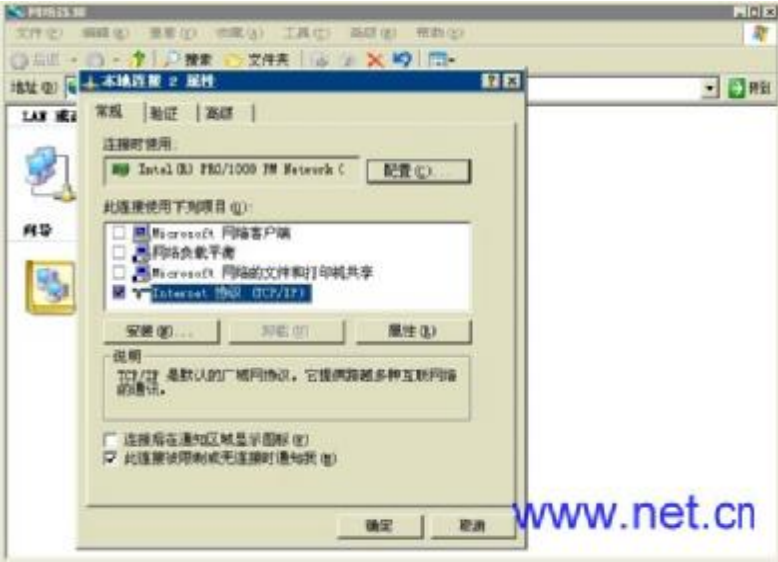


图30

在“Internet协议(TCP/IP)属性”对话框，点击下面的“高级”按钮。如图31



图31

在“高级TCP/IP设置”里选中“选项”菜单的“TCP/IP筛选”，双击进入“TCP/IP筛选”对话框。如图32



图32

首先选中“启用TCP/IP筛选”，选择“只允许”，点击TCP端口栏的添加按钮，输入TCP端口：80，点击确定，添加所有端口完毕后，确定所有对话框后，系统会自动提示您要重启服务器，重启服务器后新设置端口就可以生效。如图33



图33

## 10. 修改%system32%目录下的默认程序命令名字,防止溢出和远程操作。

必要修改的有net.exe、net1.exe、cmd.exe、msconfig.exe、regedit.exe、ping.exe等,请根据您的实际情况进行设置。

## 11. 安装必要的网络管理或监控软件,实时监控攻击事件。

比如Sniffer和HoneyPot软件,监控Hack攻击,收集证据,及时处理。

# 网络安全

## 1. 千万不要禁用网卡, 否则即使重启计算机也无法启用网卡。

打开“开始”菜单→“设置选项”中的“控制面板”选项, 点击“网络连接”进入, 双击进入“本地连接”对话框, 可以看到相关设置。如图34



图34

2.禁止占用、添加其它IP地址，由此引起的后果需您自行承担。

3.为了避免网络中其它主机的ARP欺骗攻击，我们已在网关上绑定了您的IP和mac地址，请自行下载客户端程序在您的主机绑定网关的IP和mac地址。下载地址：  
<http://service.hichina.com/ziliao/> → 软件下载→arpbind 文件

打开“开始”菜单→“设置选项”中的“控制面板”选项，点击“网络连接”进入，双击进入“本地连接”对话框，点击“属性”选项，在“本地连接属性”对话框，选中“Internet协议(TCP/IP)”，双击进入“Internet协议(TCP/IP)属性”对话框，可以查看到相关设置。如图35



图35

## 数据安全

1. 建议把软件安装、数据定时备份放在D区。
2. 建议将您的数据放在E区，并在本地保留数据备份（不要备份在其他盘符下），以免硬件损坏造成数据丢失。

## 服务器服务简单配置说明

Windows系统FTP配置说明：

<http://service.hichina.com/jszc/ShowArticle.asp?ArticleID=1629>

Windows系统IIS6.0配置说明：

<http://service.hichina.com/jszc/ShowArticle.asp?ArticleID=1627>

Windows2003远程桌面的配置及应用：

<http://service.hichina.com/jszc/ShowArticle.asp?ArticleID=1564>

Serv-U配置说明：（需自行安装设置）

<http://service.hichina.com/jszc/ShowArticle.asp?ArticleID=1633>

独立服务器win2003系统站点常见问题解答：

<http://service.hichina.com/jszc/ShowArticle.asp?ArticleID=1867>

更多精彩内容，欢迎登录：<http://service.hichina.com/jszc/ShowClass.asp?ClassID=30&page=1>  
查看