

# 整机隔离方案

— —

虚拟机仅主机(**Host-Only**)模式

安全上网的方法

精 简 版

二零一三年十月五日

前 言 .....	3
一、 在主机中的设置 .....	6
(一) Host-only 网卡的设置 (仅主机网络) .....	6
➤ 虚拟机软件是 VirtualBox (虚拟机软件是 VMware 请看后续部份) .....	6
➤ 虚拟机软件是 VMware (如果是 VirtualBox 请看前一部份) .....	7
(二) 运行“设置.bat” .....	9
(三) 主机防火墙设置 .....	11
A. 主机 IPSEC (必设置) .....	11
B. 第三方防火墙的设置 (必选 ZA 或 COMODO 之一) .....	12
(四) 主机破网软件需开启监听 0.0.0.0 或无界分享 .....	15
➤ 自由门/逍遥游 端口: 8580/8581 .....	15
➤ 无界浏览 端口: 443 .....	17
➤ TorManager2.7 两类端口: http(https): 8118; Socks5: 9050 .....	17
二、 在虚拟机中的设置 .....	19
(一) 运行“设置.bat” .....	19
(二) 虚拟机内防火墙设置 .....	20
A. 虚拟机 IPSEC (必设置) .....	20
B. 第三方防火墙的设置 (必选 ZA 或 COMODO 之一) .....	20
(三) 虚拟机里上网软件设置代理 .....	20
➤ IE 浏览器 .....	20
➤ Firefox(火狐) .....	22
三、 联网测试 .....	24
四、 附加功能: 不隐藏 IP 登陆国内网站 .....	24
结 语 .....	26

# 前言

为了便于大家快速上手,《整机隔离之虚拟机仅主机(Host-Only)方案》现推出精简版;精简版与完整版的主要区别是去掉了手动设置部份、详细验证、下载链接及一些详细解释与说明;如果需要进一步了解,请到论坛查看完整版本。

以下将最常见问题总结回答如下:

**问:我已经用虚拟机的 NAT 模式上网了,这与 Host-only 上网模式有什么不同?**

答:安全程度不同。NAT 模式的虚拟机上网与在主机直接上网所面临的风险是相同的。比如有误连正义网站、主机 DNS 泄露、透过虚拟机控制利用主机内程序的严重安全隐患。而 Host-only 上网模式由于其不同的运行原理而杜绝了这些风险,同时整机隔离 Host-only 方案中主机与虚拟机各设两道防火墙,严格控制了网络走向,因此有利的保护了上网安全。

**问:如果保证破网软件能正常运行,保证浏览器等上网软件代理设置正确,是否主机用破网软件上网与整机隔离方案中用虚拟机上网的安全性是一样?**

答:不一样。主机直接用浏览器上网,如果不慎被探测隐私,探测到的是主机的真实信息;而整机隔离方案中用虚拟机上网被探测到的是虚拟机的信息,且虚拟机可很方便的恢复快照或克隆成新的虚拟机,能有利的保护隐私与防止不利因素。况且所谓的“误操作”不是人有意做的,恰恰是在没有意识到的情况下发生的,此方案可避免此类损失。

**问:我能同时用 NAT 模式,同时又用 Host-only 整机隔离模式上网吗?**

答:不要这样做。为了安全我们建议卸载 NAT 网卡,避免虚拟机未经原设定路线而短路走了 NAT 模式,将有安全隐患。同时原用于 NAT 模式的虚拟机也建议不要用于 Host-only 模式中,避免隐私信息交叉污染,最好建立一个新的虚拟机。

**问:我已经用精简模式上网了,是否需要学习完整版教程?**

答:精简版针对一般用户安全上网,如果有更多的需求,比如虚拟机中还需运行其它上网软件,或主机中的破网软件还有其它 IP 与端口的上网请求等,那么基于精简版的防火墙设置就不适用了。因此需要根据完整版教程及防火墙的设置方法来修改相应设置才能正常上网。另外,完整版还有更多的安全防护,也可以根据情况采用。

**问:我完全按照教程实施的,但虚拟机就是上不了网怎么回事?**

答:首先要按教程中的流程逐一的检查各个环节,多数情况是某个环节疏忽了。当然个人的系统千差万别,也可能会有个例。建议这种情况到禁书网翻墙软件版提问与反馈,如果属于较普遍现象还可以帮助完善本方案。

**问:我用整机隔离方案的虚拟机上正义网站,用主机上常人网站或安装常人软件可以吗?**

答:不要这样做。整机隔离方案安全的前提是:主机一定要保持干净。因此如果要使用常人软件或上常人网,可使用不同的电脑,或同一台电脑安装双系统。如果主机不能保持干净,本方案则不能保证安全。

**问:我每次启动虚拟机前都恢复快照,这样的情况下虚拟机上网结束后是否无需用无影无踪擦除?**

答:如果每次使用虚拟机前恢复快照还是建议使用后擦除痕迹,因为在下次使用前的这段时间里还是有隐患;或者每次关闭虚拟机前恢复快照亦可。

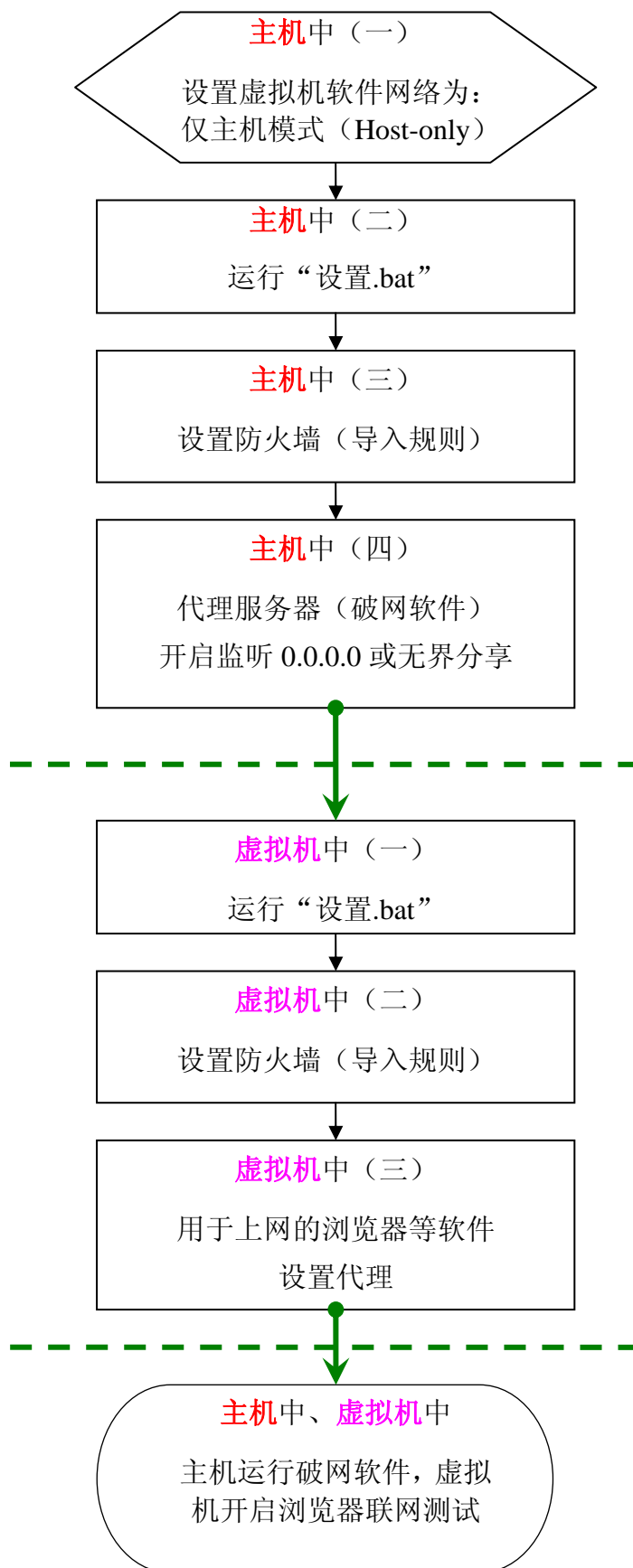
**问：这个方案是否可以完全隐藏 IP？是否可以用于网络讲真相？**

**答：本方案仅推荐用于一般的安全上网，避免误操作带来的风险，不要直接用于网络讲真相。**隐藏 IP 的程度是与探测 IP 的技术相对的，在使用本方案上网时通常体现破网软件的对应 IP，但是由于应对的网络环境不同，主机真实 IP 的安全程度也是不同的。一旦虚拟机中了木马，有可能会把虚拟机的虚拟硬件信息及可探测到的未加密信息传出；同时整机隔离方案的虚拟机原本是用来在纯净系统中建立一个不受信任的隔离测试系统环境，如果用户把之当成信任系统使用，这些信息是否会连带出主机或个人信息不可预测，因此不要盲目利用本方案进行网络讲真相，可以使用本方案用于上明慧网等正义网站，比在主机里单独依靠破网软件+浏览器上网更安全。网络讲真相还需要更深入全面的安全防护措施及配套方案。在明确的网络讲真相方案推出前，这个方案可用于一些不带有敏感信息的测试，但不要直接用于网络讲真相。

**在实施本方案相关设置前请做以下准备：**

1. 主机能正常联网（联网方式不限，宽带/ADSL/3G 等）；
2. 主机中安装虚拟机软件（VirtualBox 或 VMware），建立虚拟机并安装操作系统（WINXP 或 WIN7）；
3. 主机与虚拟机中安装防火墙（ZA 或 Comodo），杀毒软件自行安装，本方案无特别要求；
4. 从信任网站下载正版破网软件（自由门/逍遥游/无界/Tormanager2.7，Tormanager2.7 尚未发表，请到禁书网论坛查询）；
5. 下载三个文件：ZJGL\_jingjian\_X.rar（整机隔离教程精简版）、shezhi\_X.rar（设置.bat）、FHQ\_daoru.rar（防火墙导入规则），以上 X 均指不同版本代号，下载最新发表的即可；
6. 整机隔离教程完整版与防火墙设置方法请到禁书网论坛查询。

# 流程图



# 一、在主机中的设置

## (一) Host-only 网卡的设置（仅主机网络）

➤ 虚拟机软件是VirtualBox（[虚拟机软件是VMware请看后续部份](#)）

注意：VirtualBox 与 VMware 虚拟机软件任选一款即可，无需两个都安装。

### A. Host-Only 网络模式设置

1. 如果虚拟机之前已设置好，只设置网络部份可点击网络进行设置。



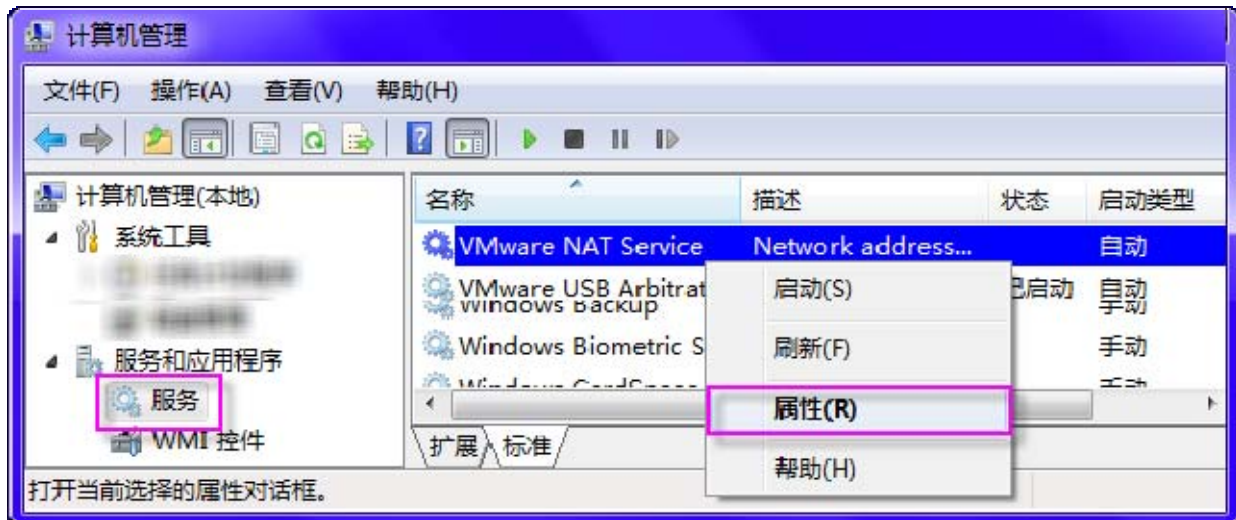
2. 在网络 → 网络连接 1，勾选启用网络连接，连接方式选 Host-only Adapter（仅主机适配器），其余选项按系统默认即可；



## ➤ 虚拟机软件是VMware（如果是VirtualBox请看前一部份）

### A. 禁用 NAT 服务

- a) 说明：NAT 网卡即使卸载，NAT 模式也是可以上网的。因此这里需禁用 NAT 服务（NAT 网卡可自行决定是否卸载）：在**计算机**点右键点**管理**，之后在**服务和应用程序**—**服务**中找到 VMware NAT Service，点右键、点**属性**：



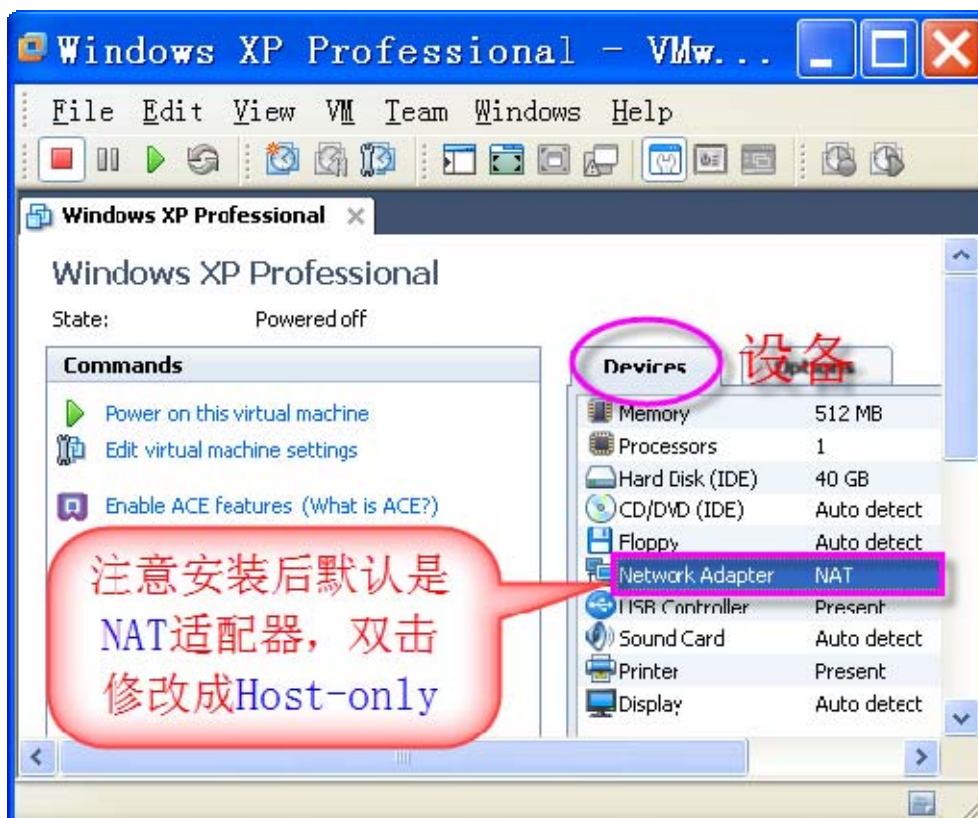
- b) 在常规页签的启动类型右侧，点小箭头选择禁用，点应用，点确定：



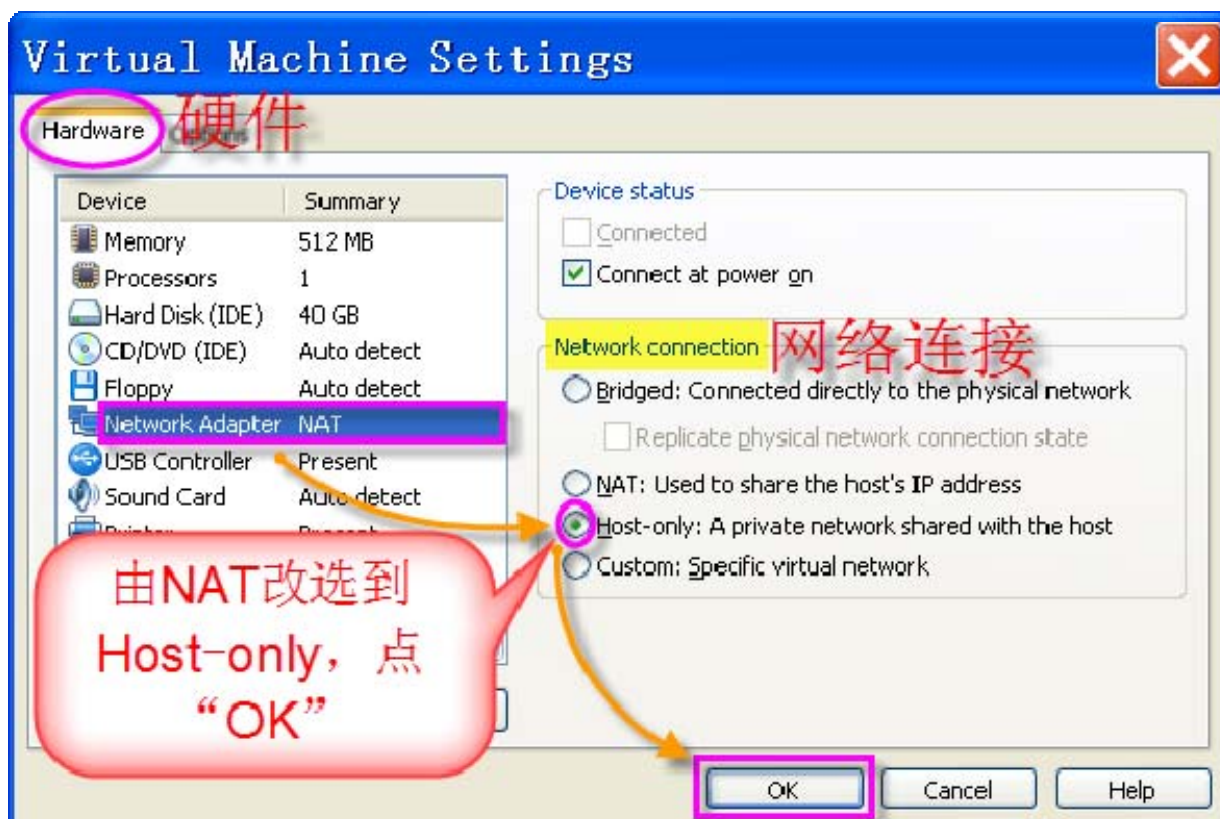
### B. VMware Host-Only 网络模式设置

1. 启动 VMware 软件，打开一个已建立的虚拟机，在 **Devices**（设备）双击 **Network Adapter NAT**（网络适配器 NAT），准备修改成 Host-only。



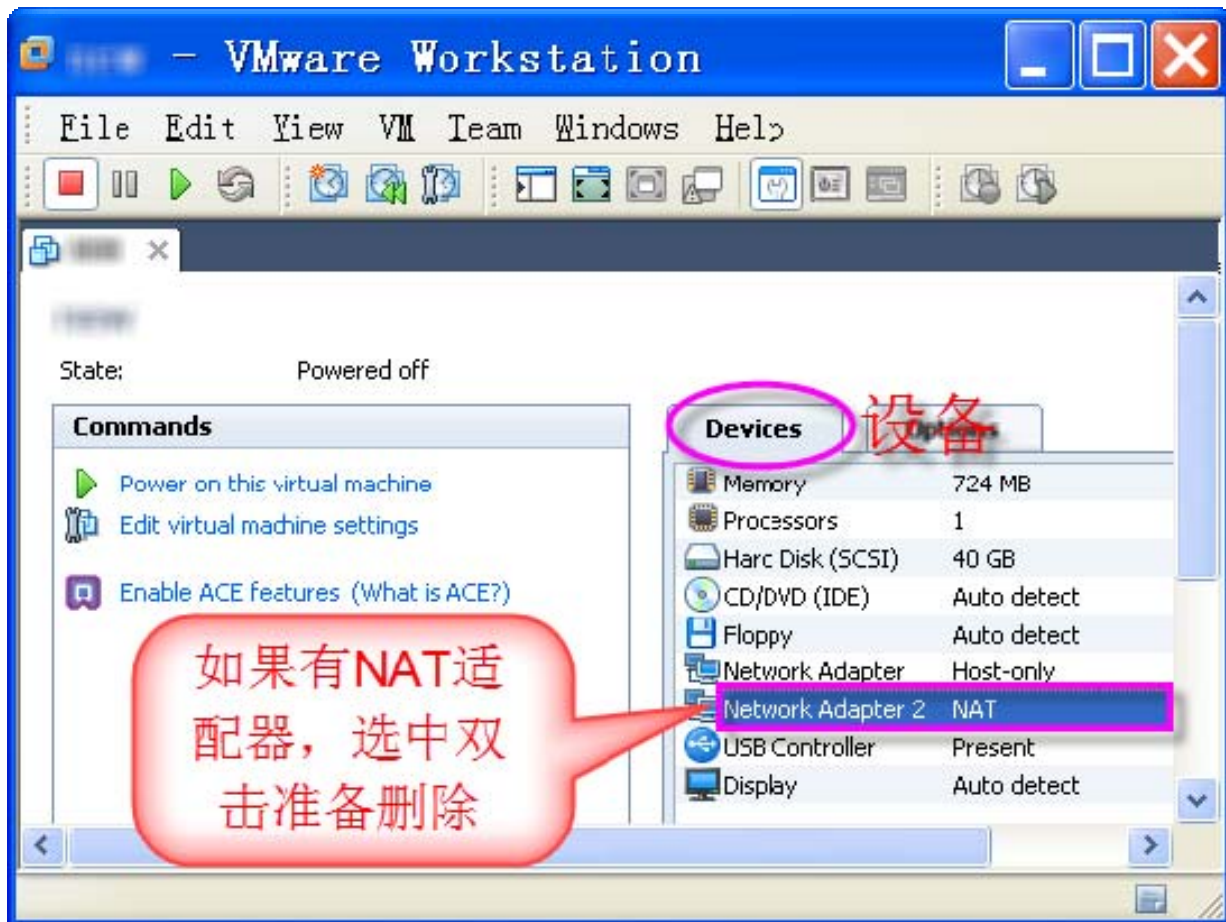


2. 在 **Hardware**（硬件），双击 **Network Adapter NAT**（网络适配器 NAT），在右侧 **Network Connection**（网络连接），由原来的 **NAT** 选项，更改成 **Host-only**，点 **OK**：

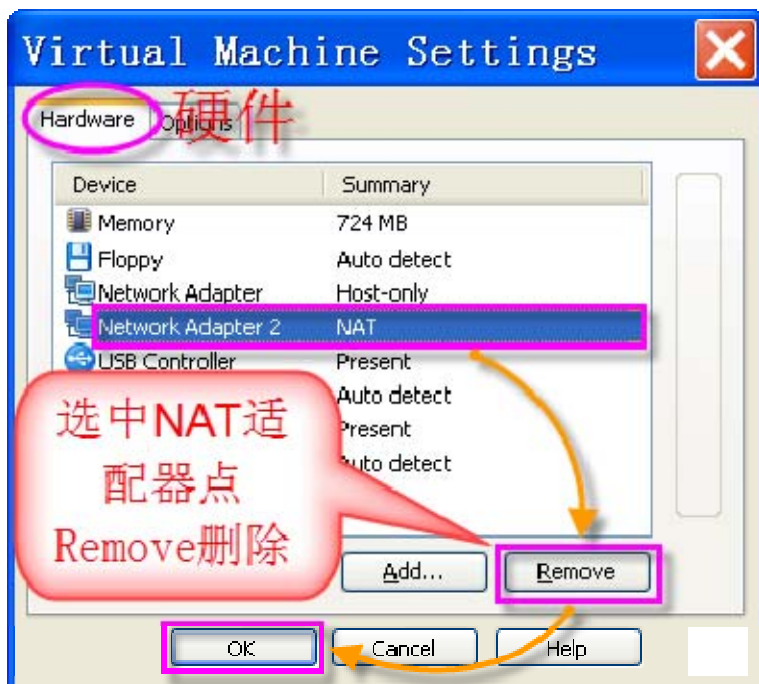


3. 如果虚拟机原来同时设置了 NAT 与 Host-only 适配器，要把 NAT 删除（很重要，否则虚拟机网络走 NAT 可能会造成 IP 泄露等）。方法是双击 **Network Adapter(2) NAT**：





4. 点击 Network Adapter (2) NAT，点 **Remove**（移除），点 **OK**：



## （二）运行“设置.bat”

说明：（1）shezhi\_X.rar 解压后的 shezhi\_X.bat 即“设置.bat”（如果后缀是.txt 请改为.bat）；

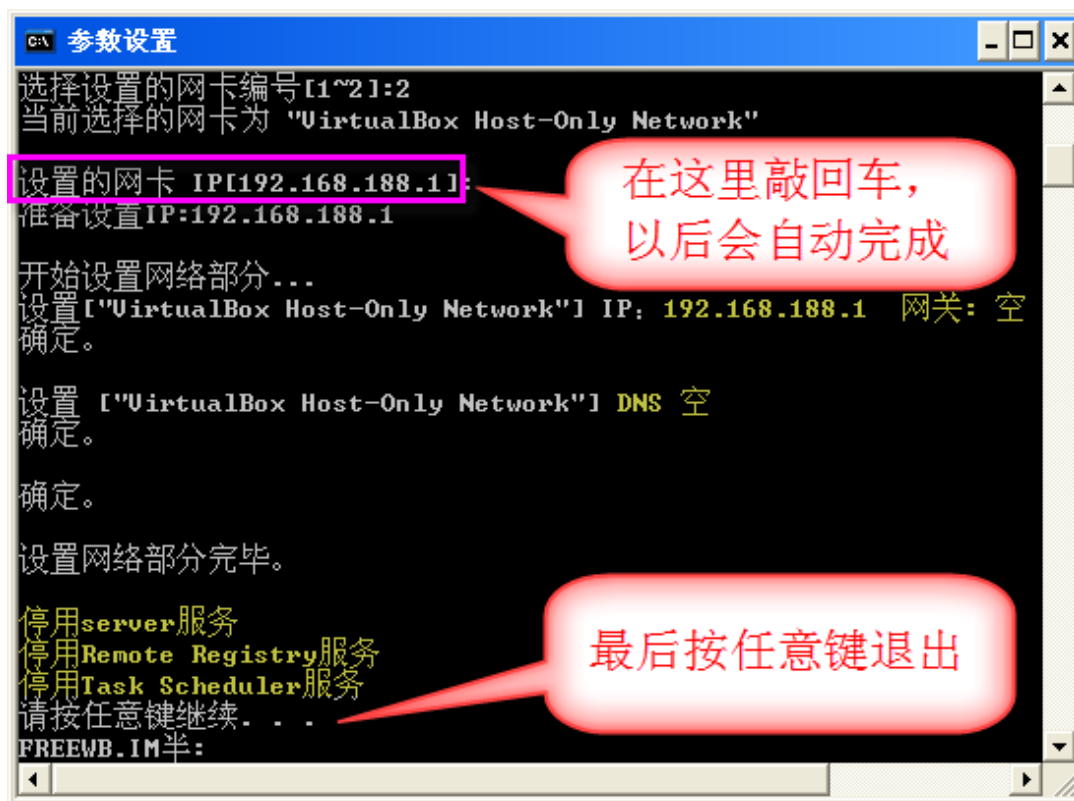
（2）WINXP 直接运行“设置.bat”； WIN7 需以管理员身份运行“设置.bat”；

1. 查看 VirtualBox Host-only Network(VirtualBox),或 VMware Network Adapter VMnet1 (VMware) 左侧对应的数字, 填写到**选择设置的网卡编号**后, 回车。



注意: 设置时以实际 VirtualBox Host-only Network 或 VMware Network Adapter VMnet1 左侧的编号为准, 不要直接把图示的编号填入。

2. 出现设置的网卡 IP 时,直接回车则按默认 IP 设置(如需更改此 IP 请参考教程完整版):



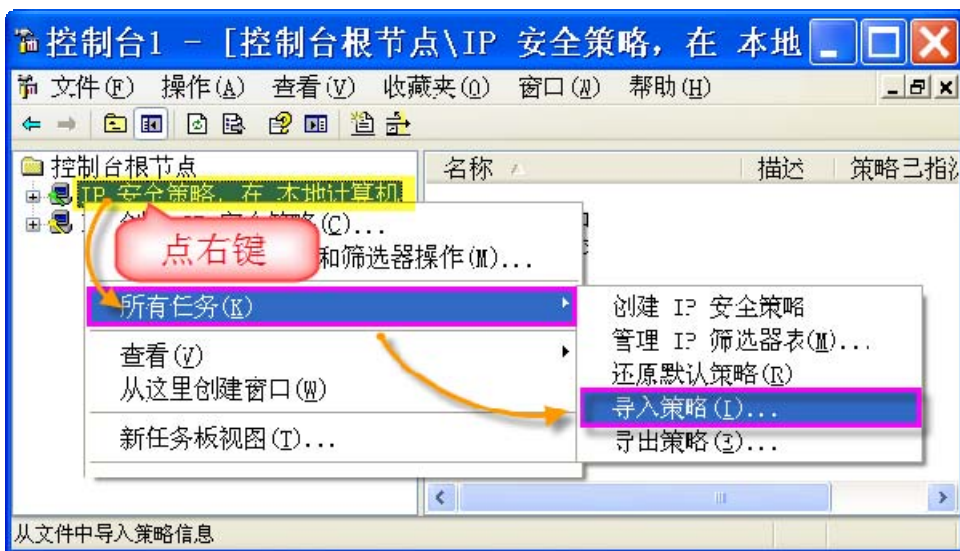
3. 如果出现“网段已经存在, 更换一下网段”, 说明主机中有网卡与此网段冲突, 找到冲突的网卡改成其它网段后, 再从新运行“设置.bat”。**设置完成需从新启动计算机。**

### （三）主机防火墙设置

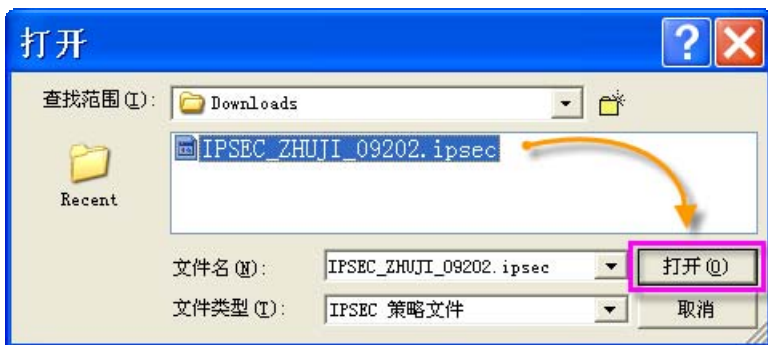
#### A. 主机 IPSEC（必设置）

导入方法：WINXP/WIN7 系统开始 → 设置 → 控制面板 → （WIN7 系统和安全）→ 管理工具 → 本地安全策略 → IP 安全策略、在本地计算机；

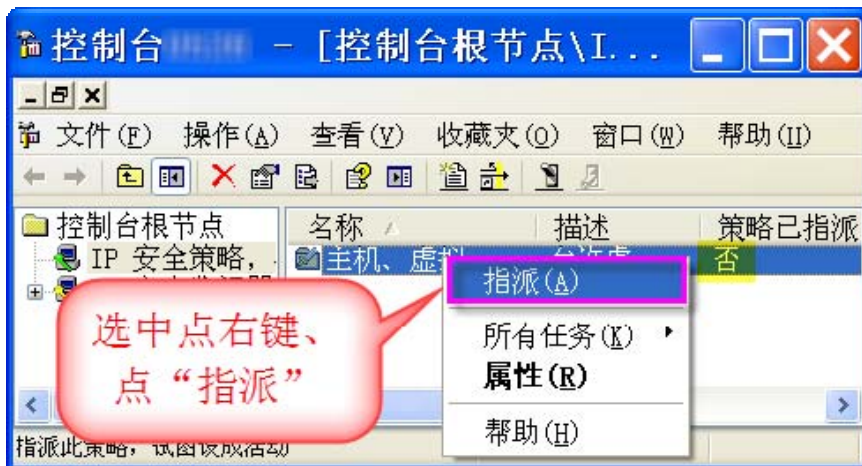
1. 在 IP 安全策略、在本地计算机点右键 → 所有任务 → 导入策略；WIN7 出现询问“导入策略……你想继续吗”点是：



2. 找到 IPSEC\_ZHUJI\_X.ipsec（之前将下载的压缩包 FHQ\_Daoru.rar 解压到文件夹），点打开（X 代表不同的更新版本）：

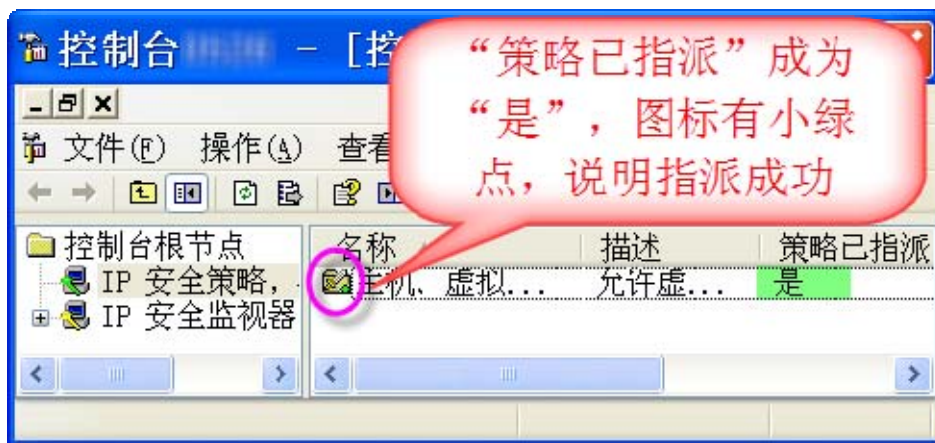


3. 选中导入的策略，点右键、点指派（Win7 点分配）：





4. 正常后策略已指派会显示是，图标有绿色小点；指派不成功请参考[教程完整版](#)解决：



([返回虚拟机IPSEC](#))

## B. 第三方防火墙的设置（必选 ZA 或 COMODO 之一）

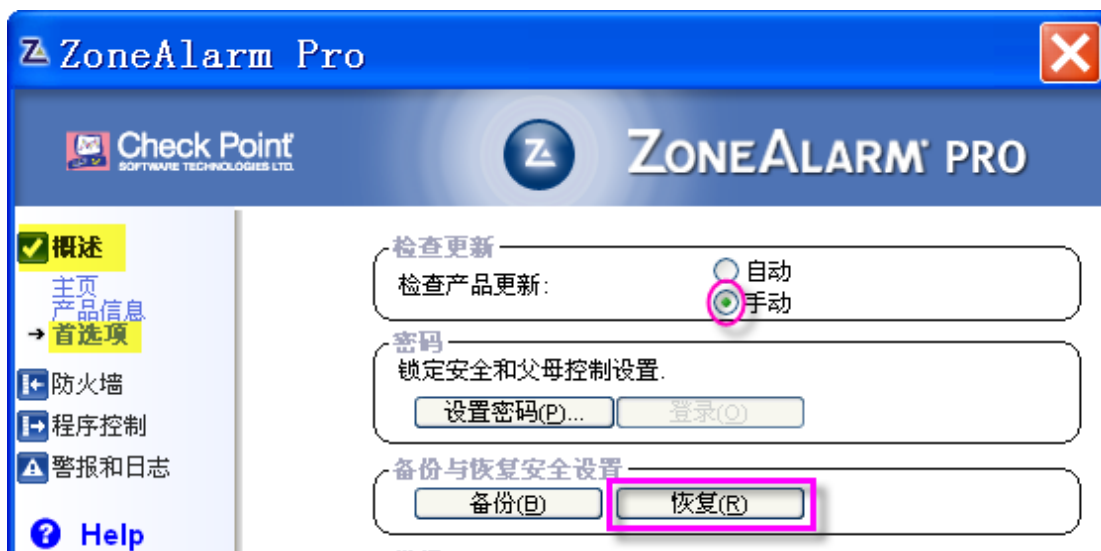
说明：1. WIN7 可选用 ZoneAlarm 9.3.014，导入规则依然使用 ZA8\_ZHUJI\_X.xml；技术论坛推荐版本 Comodo 3.14 不适用于 WIN7 64 位，但可用于 WIN7 32 位。

### ➤ ZoneAlarm的设置（如果是COMODO请看后续部份）

说明：请将ZA8\_ZHUJI\_X.xml按以下图示导入；如需修改请参考[《防火墙设置方法》](#)；以上X指不同的版本，用从本站下载的压缩包FHQ\_Daoru.rar解压即可。

#### A. 导入规则

1. 在概述 → 首选项，先将检查产品更新改为手动，然后点恢复：



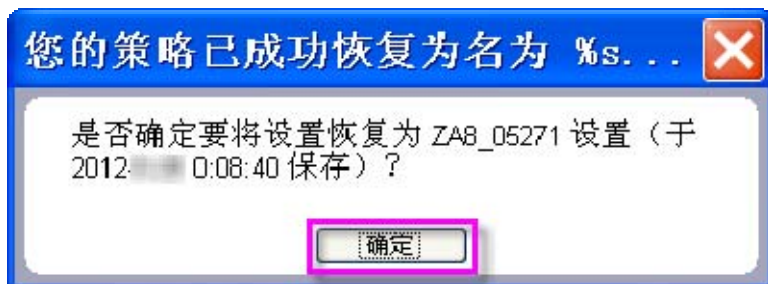
2. 找到下载并解压的文件，点打开：



3. 点确定:



4. 点确定。



([返回虚拟机第三方防火墙的设置](#))

### ➤ 第三方防火墙Comodo的设置 ([如果是ZA请看前面部份](#))

说明: 请将COMODO314\_ZHUJI\_X按以下图示导入; 如需更改请参考 [《防火墙设置方法》](#); 以上X指不同的版本, 用从本站下载的压缩包FHQ\_Daoru.rar解压即可。

1. **注意:** WIN7 首先退出 COMODO, 再右键点击“以管理员身份运行”。在其它, 点管理我的配置:



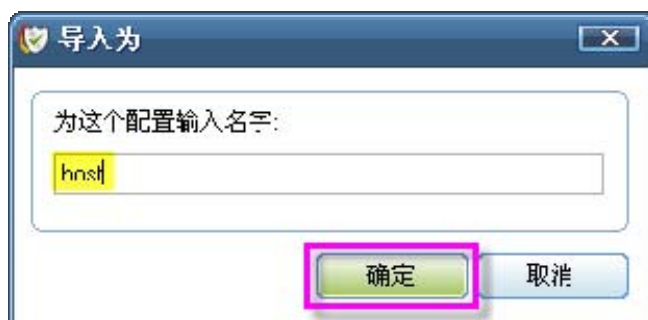
## 2. 点导入：



## 3. 找到下载的 COMODO314\_ZHUJI\_X, 点打开：



## 4. 导入时会自动带入名称，也可自行修改（可仿制原列表中配置名称稍做修改使其较隐蔽），点确定：



## 5. 导入成功提示：

6. **关键步骤：一定要激活才起作用：**选中导入的配置名称，点**激活**，出现提示点**确定**：





7. 激活后该配置右侧有“活动”标识，点关闭：



([返回虚拟机第三方防火墙的设置](#))

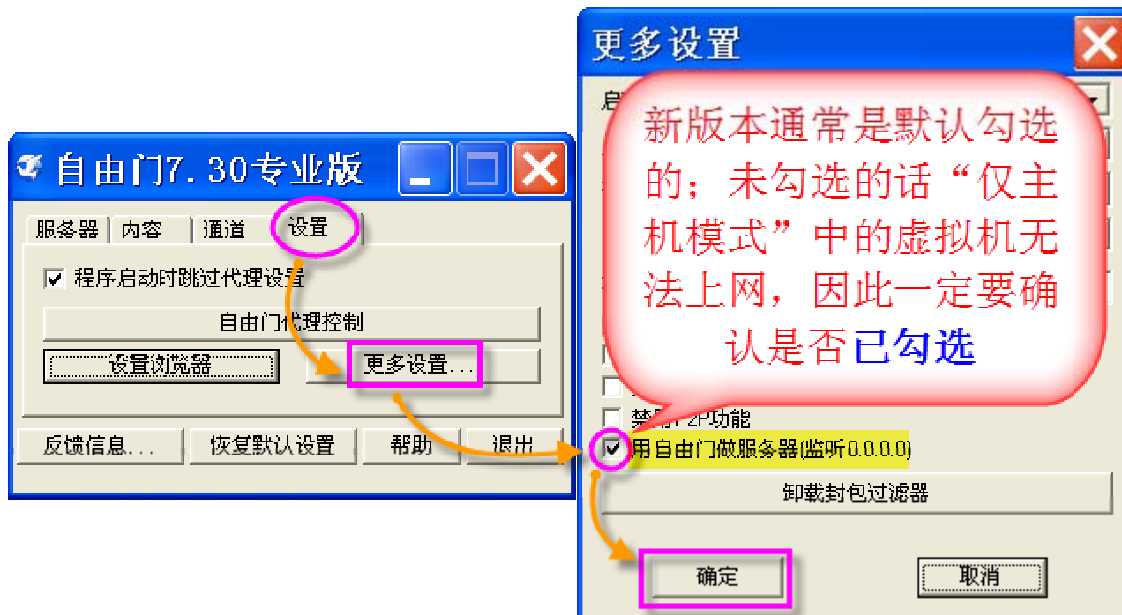
#### （四）主机破网软件需开启监听 0.0.0.0 或无界分享

可用于本方案的主要破网软件有：自由门/逍遥游/无界浏览/TorManager2.7 等。

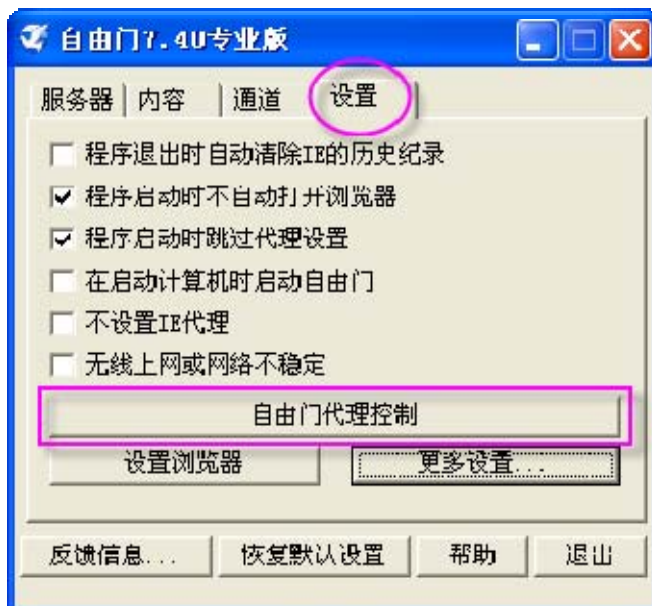
提示：可先学习这部份内容，实际操作可在联网测试时设置。

##### ➤ 自由门/逍遥游 端口：8580/8581

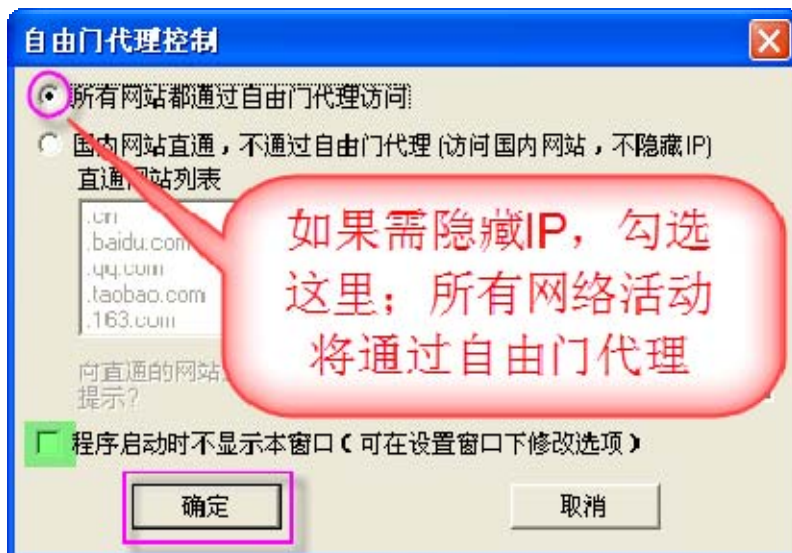
1. 自由门/逍遥游的设置方法相似。在设置 → 更多设置 → 勾选用自由门（逍遥游）做服务器（监听 0.0.0.0）→ 确定。



2. 提示：以下设置涉及安全问题，请一定要确认设置正确。在初次使用自由门时会弹出设置，或在设置—自由门代理控制（如果逍遥游代理控制可用，设置方法相同）：



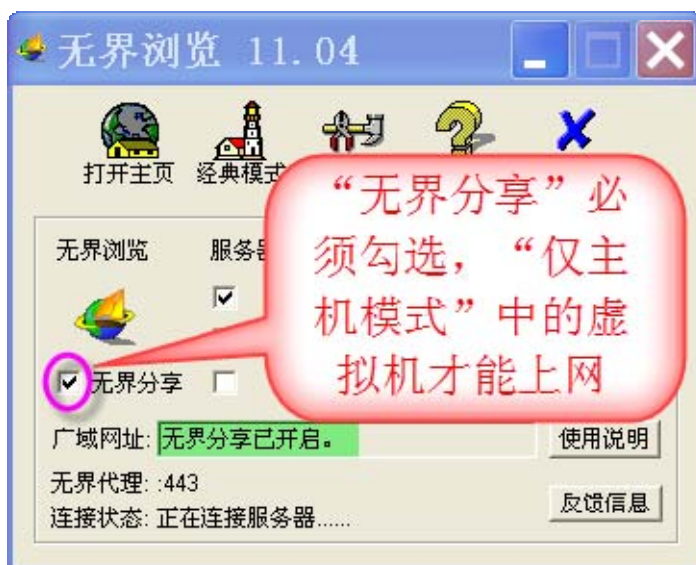
3. 勾选所有网站都通过自由门代理访问。**重要提示：**如果勾选了国内网站直通，不通过自由门代理（访问国内网站，不隐藏 IP）的功能后，登陆直通网站列表中的网站时是以真实 IP 登陆的；为了不出现暴露真实 IP 的情况，启动自由门后要在自由门代理控制的设置中勾选所有网站都通过自由门代理访问；为了避免无意中使用了“国内网站直通”功能，不要勾选下方的程序启动时不显示本窗口，这样每次上网前确认一下。最后点确定。



4. 那么在整机隔离方案下如何短时间上普通网站、或运行非安全软件呢？请参考：[附加功能：不隐藏IP登陆国内网站](#)

### ➤ 无界浏览 端口：443

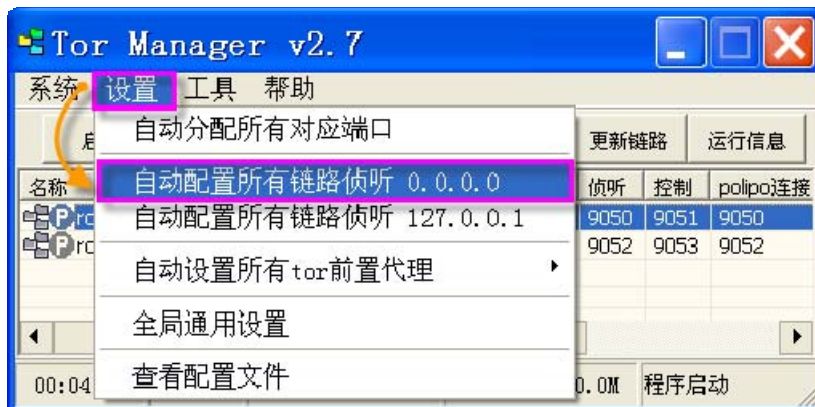
设置方法：勾选无界分享（只有高版本才有此功能，请选择 11.03 以上版本），无界代理变成以 443 为端口的代理；此时可以侦听 0.0.0.0：



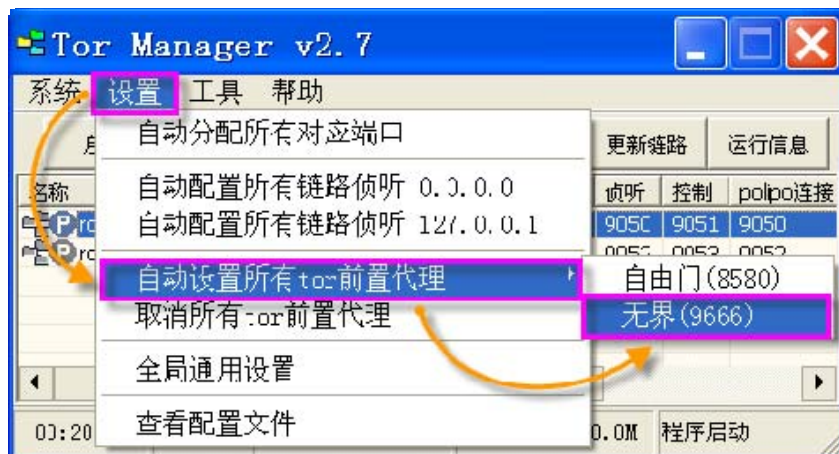
### ➤ TorManager2.7 两类端口：http(https)：8118； Socks5： 9050

注意：Tor 来源于第三方，安全度未知，请酌情使用。Tormanager2.7 是技术高手推出的应用 Tor 的一款软件，尚未发表，请到禁书网查询。

1. 步骤：启动 tormanager.exe 后，在设置选自动配置所有链路侦听 0.0.0.0：

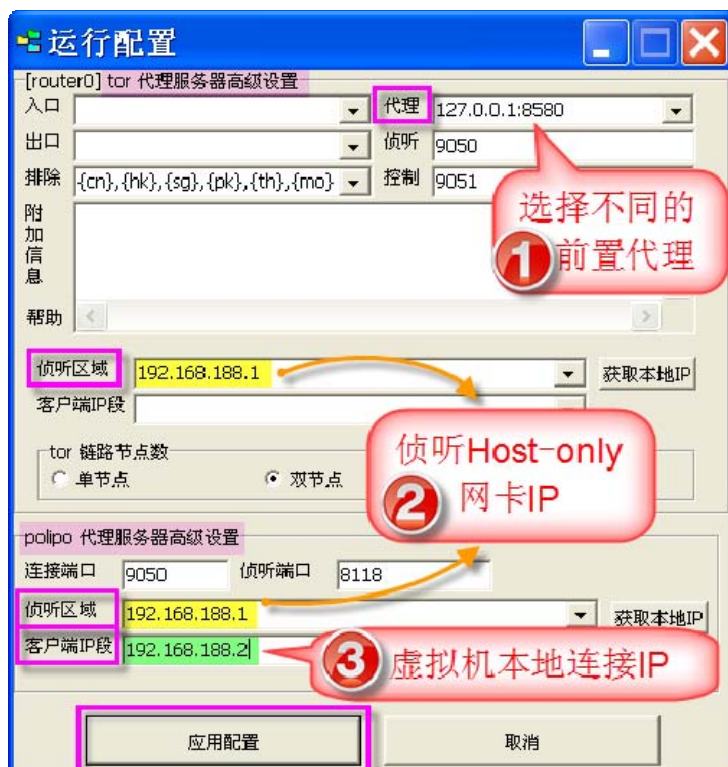


2. 在设置，选自动设置所有 Tor 前置代理，根据实际选择自由门（8580）或无界（9666）；  
注意：无界只用于 Tor 的前置代理不要勾选“无界浏览”；或前置代理更改端口为 443。



3. 以上两项也可以通过双击链路单独设置，这样只设置了本条链路。

- (1) 两个侦听区域均选择 Host-only 网卡 IP（192.168.188.1）；或（0.0.0.0）监听所有；
- (2) 客户端 IP 段填写虚拟机本地连接网卡的 IP（192.168.188.2）。如果同时代理主机本地网络，可加上 127.0.0.1 并用半角逗号隔开，如：192.168.188.2,127.0.0.1；



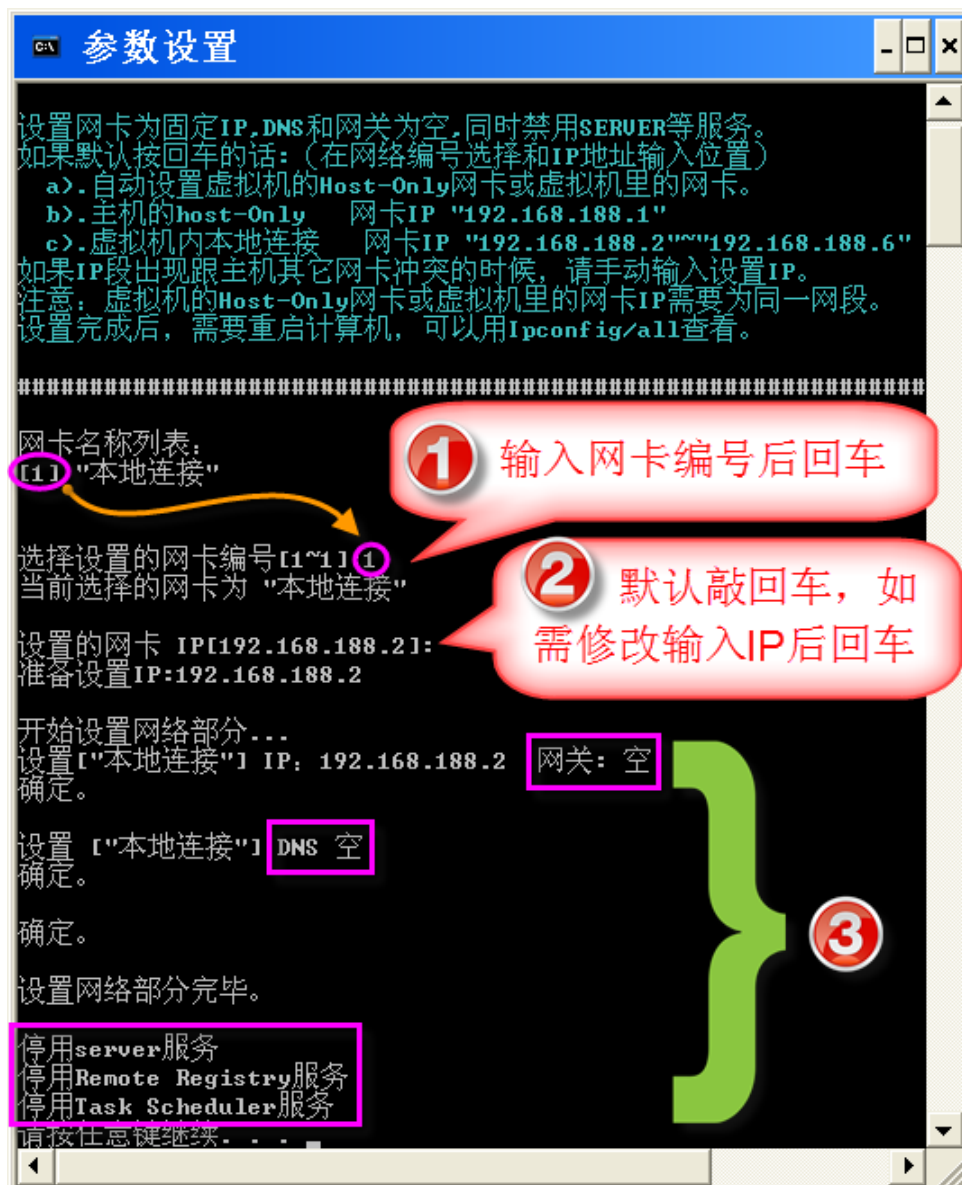


## 二、在虚拟机中的设置

### （一）运行“设置.bat”

说明：VirtualBox 和 VMware 虚拟机里设置方法相同：

- 虚拟机系统为 WINXP，直接在虚拟机里运行**设置.bat**（shezhi\_X.bat）即可。
- 虚拟机系统为 WIN7，请选中**设置.bat**，点右键选择以管理员身份运行；如果运行后界面一晃而过，需要将**设置.bat**拷贝到虚拟机本地 C 盘下，再次按以上方法运行。
- 无论主机是 WINXP 或 WIN7，虚拟机使用 WINXP 或 WIN7 均可，无对应关系。
- 运行**设置.bat**后，请参考浅兰色字体说明；设置不要做任何更改按默认回车即可。
- 如需更改请参考[整机隔离完整版教程](#)。如果无影无踪使用时有问题，需手动打开SERVER服务；WIN7 中Task Schedule自动启用、且无法手动修改，就按默认即可。



## （二）虚拟机内防火墙设置

### A. 虚拟机 IPSEC（必设置）

与[主机IPSEC](#)的设置方法相同，导入"IPSEC\_XUNJI\_X.ipsec"(FHQ\_Daoru.rar解压)。

### B. 第三方防火墙的设置（必选 ZA 或 COMODO 之一）

1. ZoneAlarm: 请将ZA8\_XUNJI\_X.xml，按照[主机防火墙ZoneAlarm的设置](#)方法导入；

**注意：**WIN7 适用的 ZA 版本与 XP 的不同，但是可用同一导入规则。

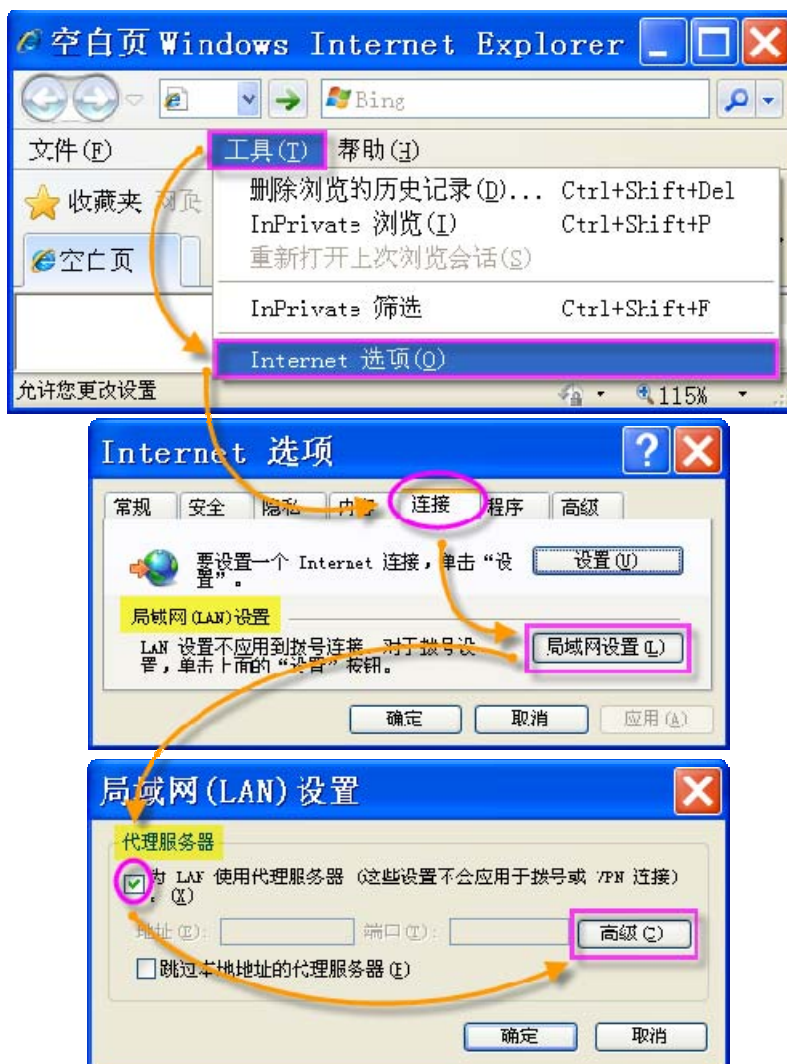
2. Comodo: 请将COMODO314\_XUNJI\_X，按[主机防火墙Comodo的设置](#)方法导入；如需修改请参考[《防火墙设置方法》](#)。

## （三）虚拟机里上网软件设置代理

本教程以比较常用的 IE 浏览器和 Firefox（火狐）为例介绍设置方法。

### ➤ IE 浏览器

1. IE → 工具 → Internet 选项 → 连接页签 → 局域网设置 → 代理服务器下勾选为 LAN 使用代理服务器 → 高级：

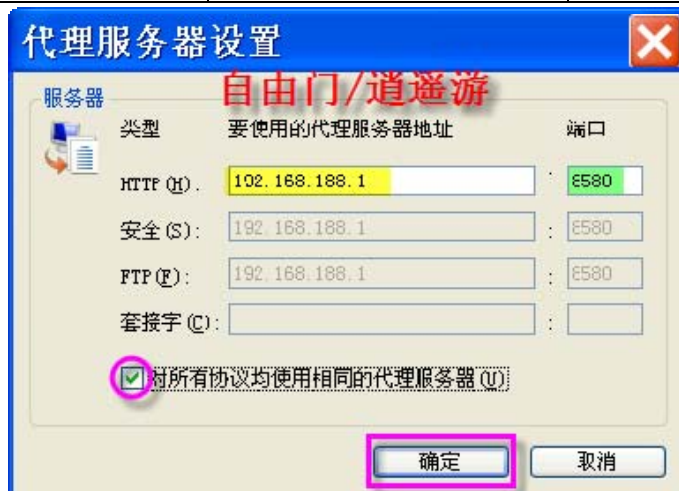




2. 由上继续，点**高级**：根据不同破网软件（如自由门/逍遥游/无界/Tor 等）设置。

以主机的虚拟网卡（Host-Only）IP 是 192.168.188.1 为例；如果端口相同可勾选“对所有协议均使用相同的代理服务器”，否则不要勾选：

破网软件	Host-only 网卡 IP	端口
自由门/逍遥游	192.168.188.1	8580/8581
无界分享	192.168.188.1	443
Tormanager2.7	192.168.188.1	http(s)：8118/8119/8120/8121/8122
		Socks：9050/9052/9054/9056/9058

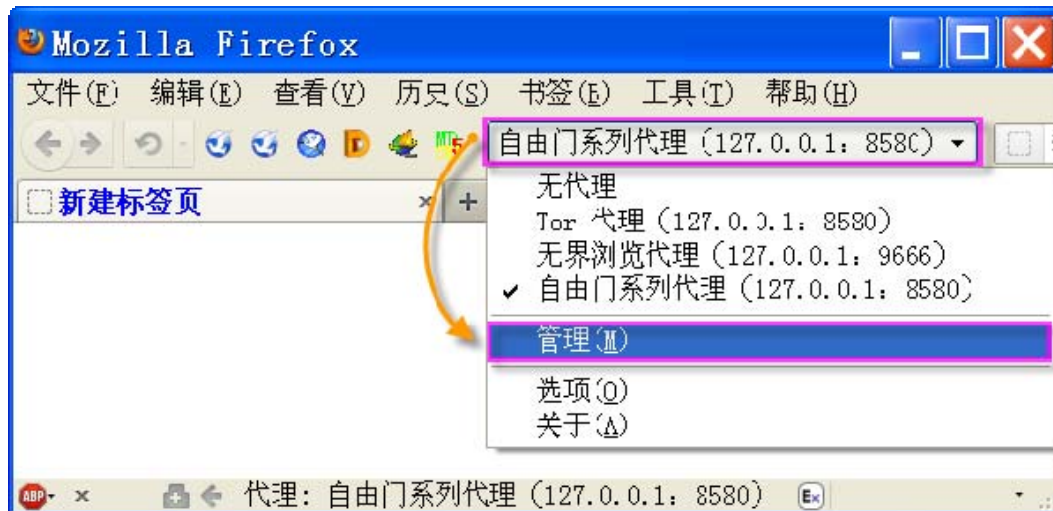


注：以上图示中标识“套接字”的在有些 IE 版本中标识为“Socks”，两者的设置方法相同的。

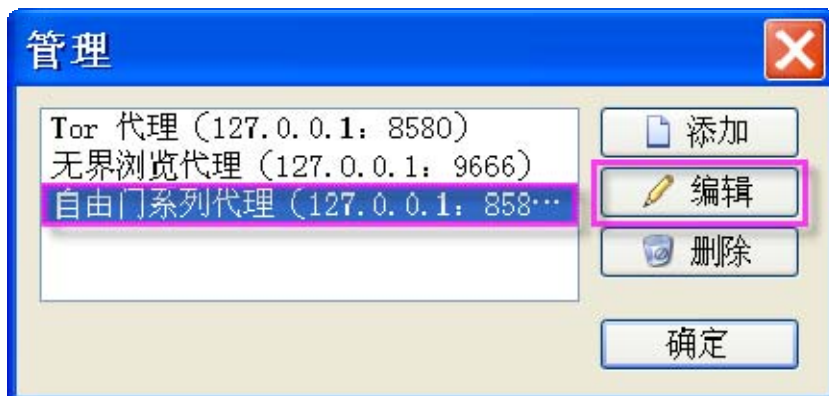
## ➤ Firefox(火狐)

以 FirefoxPortableESR10.0.4\_G 为例：

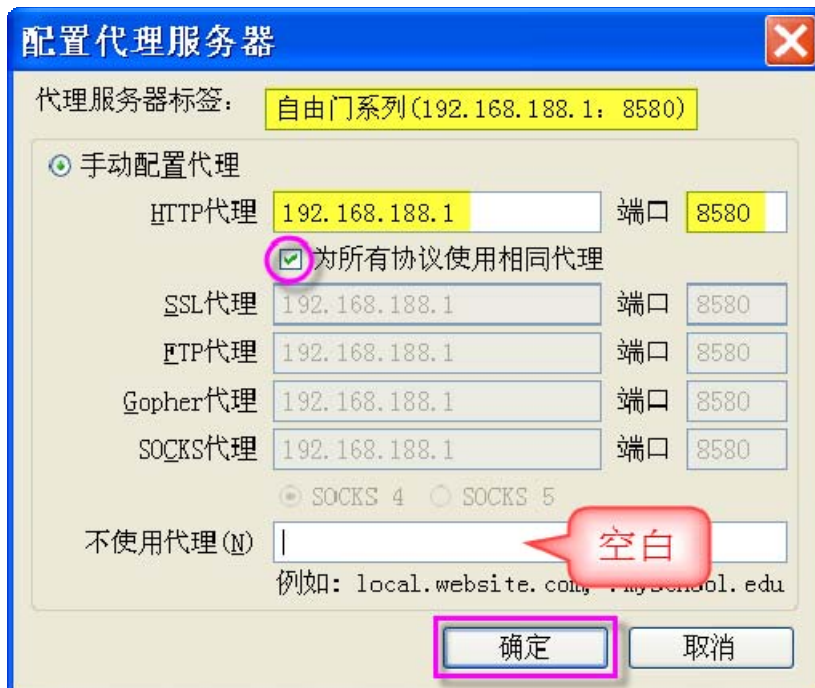
1. 因虚拟机浏览器的代理 IP 要用主机虚拟网卡 Host-only 的 IP，因此原程序自带的代理服务器设置不能直接用，需从新设置。点击自由门系列代理，选择管理：



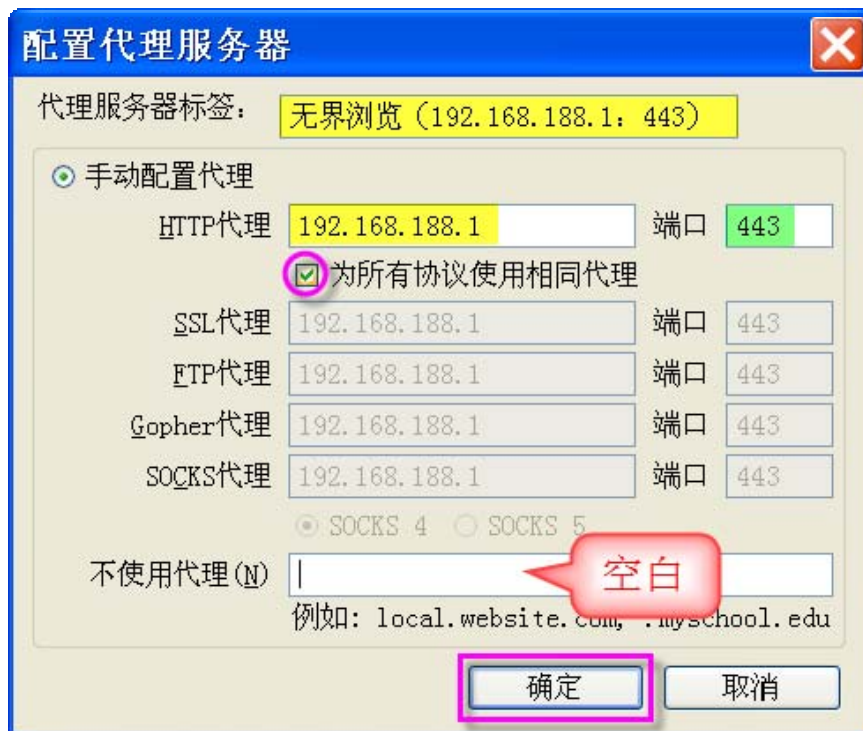
2. 顺序选中以下三个代理，点编辑（或点添加）：



3. 自由门系列代理（127.0.0.1：8580），更改代理服务器标签，按图示修改后点确定：



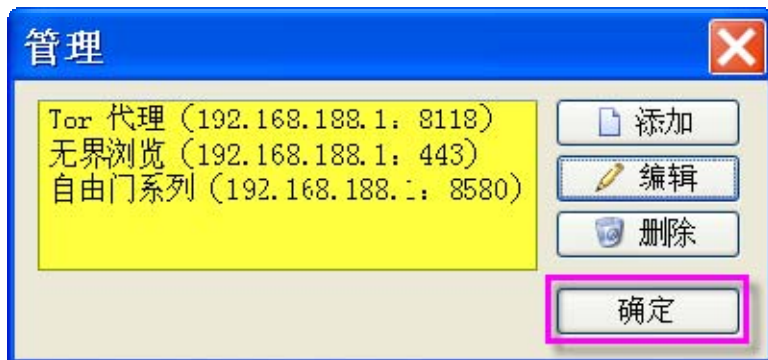
4. 无界浏览代理 (127.0.0.1: 9666)，更改代理服务器标签，按图示修改后点确定：



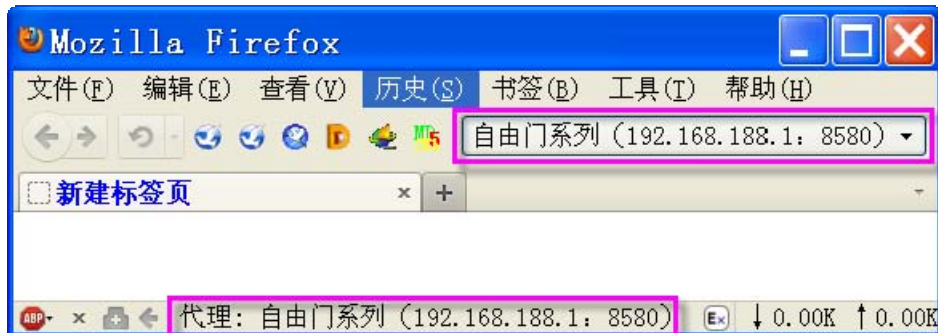
5. Tor 代理 (127.0.0.1: 8580)：因为 Tor 可以有許多链路，不同的链路需设立不同的代理，以下可更改 Tor 为 Tor0，更多 Tor 代理设置方法类似。所有代理均设置目前所用的 Host-only 网卡 IP (192.168.188.1)；不勾选为所有协议使用相同代理；前四项端口设置 Tor 的 polipo 侦听端口 8118（建立更多 Tor 代理顺排 8119/8120/8121/8122）；Socks 端口 9050（建立更多 Tor 代理顺排 9052/9054/9056/9058）；勾选 Socks5，不使用代理处清空；点确定：



6. 设置完成后如图，点**确定**：



7. 使用哪个破网软件，就选择对应的代理；启用后在浏览器下方状态栏可看到已启用的代理；之后输入网址回车即可通过代理上网；下次启动火狐后会默认是上一次使用的代理：



### 三、联网测试

**注意：**主机正常联网（主机联网方式不限，宽带、3G、ADSL 等均可），主机启动破网软件，主机破网软件开启监听 0.0.0.0、无界分享或 Tor 的侦听区域，虚拟机浏览器或软件设置相应代理（例 192.168.188.1:443），此时虚拟机中浏览器输入网址应该可以上网了。

国内网站可能有“回墙现象”无法登陆，因此测试时需用国外网站。本方案可保证不会误联正义网站（即未开启破网软件时联网行为出不了虚拟机），因此在本方案中虚拟机中可联正义网站测试虚拟机是否正常上网。

如果不能上网请查看以上注意事项的每一部份及防火墙日志，如不能解决可到禁书网反馈。

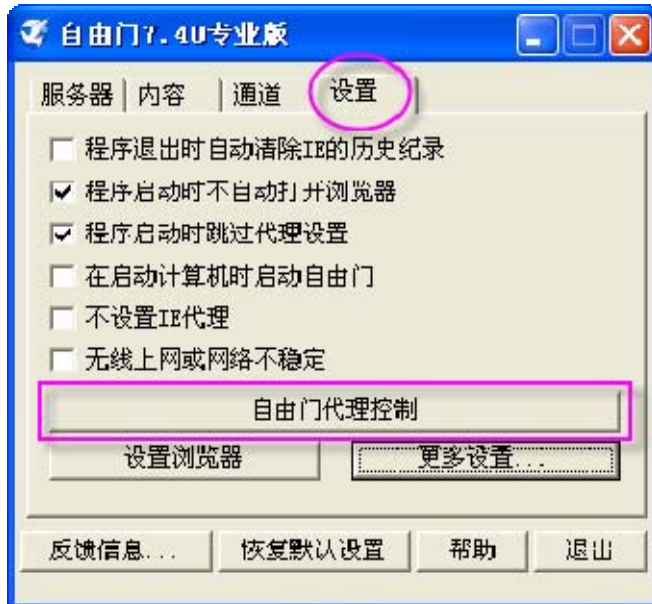
### 四、附加功能：不隐藏 IP 登陆国内网站

**说明：**整机隔离方案的安全基础是主机安全，因此主机不能使用国内软件及其它不安全软



件、不直接登陆网站等。同时由于整机隔离方案设定的特殊的联网方式，虚拟机不通过代理是无法上网的。那么在整机隔离方案下如何短时间上常人网站、或运行非安全软件呢？这里有解决方案：建立一个全新的虚拟机，设置完备后建立快照，每次使用后关闭虚拟机时点**控制一退出一强制退出**（勾选**恢复到当前备份 XX**）；此虚拟机的网络代理设置方法、浏览器代理设置与整机隔离相同，但是破网软件目前只能使用自由门（如果逍遥游的**逍遥游代理控制**可用的话，亦可用逍遥游代理上网），具体方法如下：

### 1. 在自由门软件的设置点自由门代理控制：



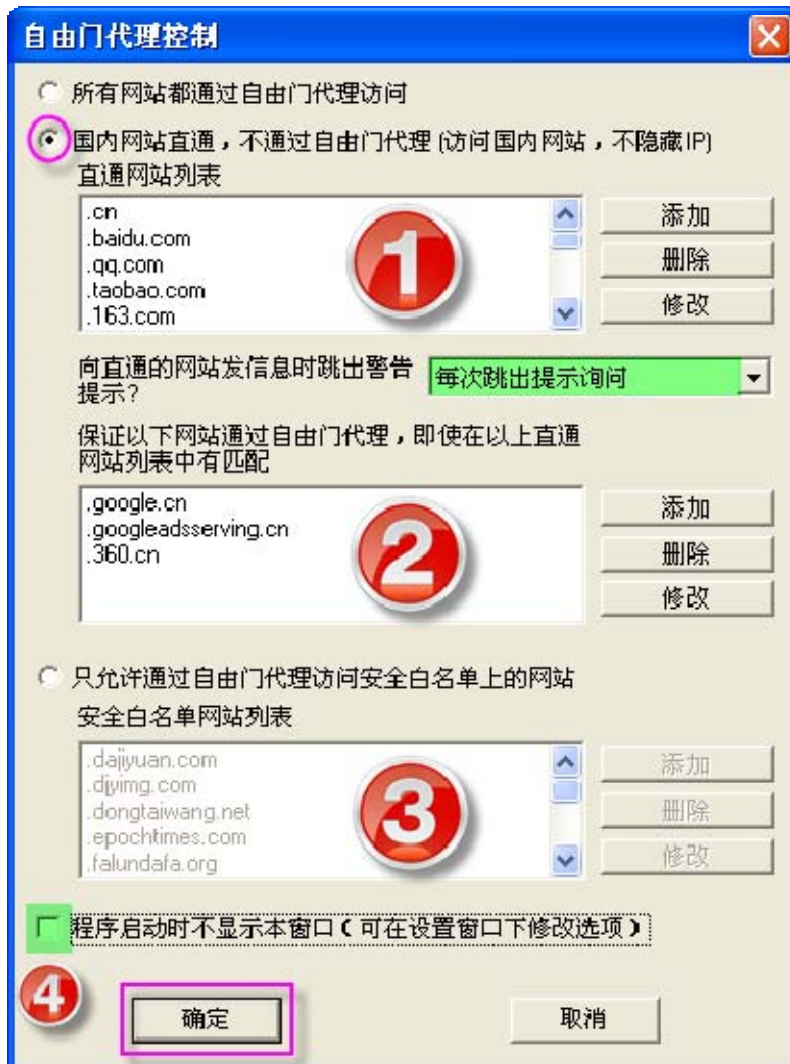
2. 勾选**国内网站直通**，不通过自由门代理（访问国内网站，不隐藏 IP）。向直通的网站发信息时跳出警告提示？选择**每次跳出提示询问**。这样设置是为了避免未经代理误连国内网站；如果确认是要连接国内网站，可在出现的提示询问上点**不再显示本窗口**（下一步有具体说明）；

①可**添加、删除、修改**“直通网站列表”；添加的关键字仿照自带列表，或在软件主界面点**帮助查看**；

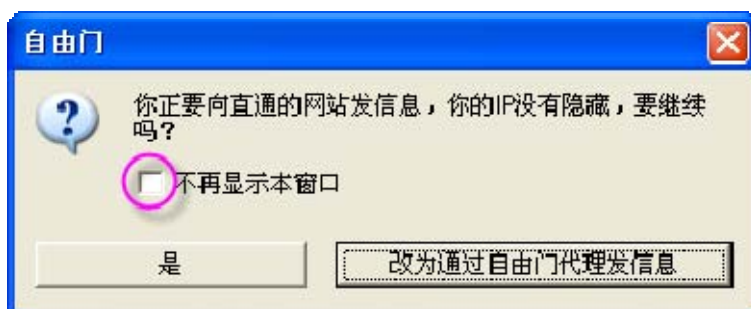
②与以上**直通网站列表**关键字相同、但又想通过自由门代理上网，可**添加**到这里，亦可**删除、修改**；

③如果只想通过代理访问白名单上的网站，可勾选**只允许通过自由门代理访问安全白名单上的网站**。可**添加、删除、修改**“安全白名单网站列表”；

④不要勾选**程序启时不显示本窗口**（通过代理和未经代理直通国内网站的两种上网方式同时存在，为了保证正确设置，每次开自由门时需从新确认），最后点**确定**：



3. 因为以上设置了向直通网站发信息时每次跳出提示询问，在每一步需发信息给网站都会跳出提示；如果你确认目前是在不隐藏 IP 登陆国内网站，点是；如果这段时间都不隐藏 IP 登陆国内网站，可临时勾选不再显示本窗口，再点是；如果需要经代理上网，可点改为通过自由门代理发信息。**注意：国内网站往往在使用自由门等代理时是无法登陆的。**



## 结 语

新手通过本教程能够上网后就可以开始使用与测试了；等到有一定基础后可参考[教程完整版本](#)的相关说明；使用后如果有什么问题与心得，欢迎到禁书网分享。

将来可能会推出基于整机隔离方案的一些软件的应用，希望大家能很快掌握此方案，对于更自如、安全的突破封锁将大有助益。



## [大陆直连看禁书禁闻禁文禁网禁片禁歌禁曲](#)

---

[禁书网](#) 提供禁书下载阅读，禁书目录，禁书网 <http://www.bannedbook.org/> 是最大最全的禁书下载基地，中国禁书，大陆禁书应有尽有。禁书禁闻禁片大陆直连：<https://goo.gl/C6xxGf>