整机隔离之 **Host-Only** 虚拟机应用

防火墙设置方法

（二零一二年十月六日）

前　言

本教程是基于整机隔离方案的防火墙的设置，一般用户导入下载的规则即可；本文旨在展示规则的设置过程，对于希望深入探讨防火墙设置方法的会员能起到抛砖引玉的作用。

说明一：不同的防火墙设计不同，且主机、虚拟机要求不同，因此设置上有一定的差异；所以主机与虚拟机需导入相应不同的规则。IPSEC 为必设置内容，第三方防火墙可以自由选择一种；本文以 Comodo 与 ZoneAlarm 为例。

说明二：本文导入的规则相关 IP 如下：
主机 Host-only IP：　192.168.188.1
虚拟机内本地连接 IP：192.168.188.2 ~ 192.168.188.6
虚拟机代理设置：根据 Host-only 的 IP 与破网软件端口来设置

说明三：本文 WINXP 系统中以 Comodo 3.14 与 ZA 8.0.298 版本为例，WIN7 使用 WIN7 自带防火墙，或 ZoneAlarm 9.3.014（论坛推荐版本 Comodo 3.14 只适用于 WIN7 32 位）。所有 Comodo 均可使用导入规则，ZA 不论版本均可使用导入规则。

以下是下载地址：

◇ 科摩多防火墙 3.14 版本（Comodo 3.14）：
http://www.bannedbook.org/forum42/topic3156.html

◇ ZoneAlarm 8.0.298 防火墙下载、安装、汉化教程
http://www.bannedbook.org/forum42/topic3159.html

◇ ZoneAlarm 9.3.014 防火墙安装使用教程（建议在win7 下使用）
http://www.bannedbook.org/forum42/topic3164.html

说明四：主机定义三条规则（顺序很重要）：

- 允许虚拟机与 Host-only IP 基于破网端口访问
- 除以上规则外禁止虚拟机（Host-only）网段的其它访问
- 除以上规则外禁止访问破网端口

说明五：虚拟机定义两条规则：

- 允许虚拟机与 Host-only IP 基于破网端口的访问
- 阻止其它一切通讯

一、 主机 IPSEC 设置方法（必选）

IPSEC 是 Windows 自带的安全策略。为了防止第三方防火墙因故未启动，IPSEC 将是最后一道防线；因此 IPSEC 为必设选项。

导入 IPSEC_ZHUJI_X（注意导入有 ZHUJI 标识的相关防火墙）

说明一：以上 X 是序列号，代表不同的版本，用户只要下载本站的当前附件即可。导入的规则为最基本的对主机、Host-Only、虚拟机的安全防护，其余一些细节，比如一些软件适用的规则等还需要在使用中慢慢添加。

说明二：

(1). 本文以同时开启 5 台虚拟机上网为例，如果需要更多虚拟机同时上网，请相应调整 Host-only 与虚拟机内本地连接的掩码，同时调整防火墙规则中的 IP 范围；如果不是同时上网，每台虚拟机 IP 可以设置相同，比如都是：192.168.188.2；

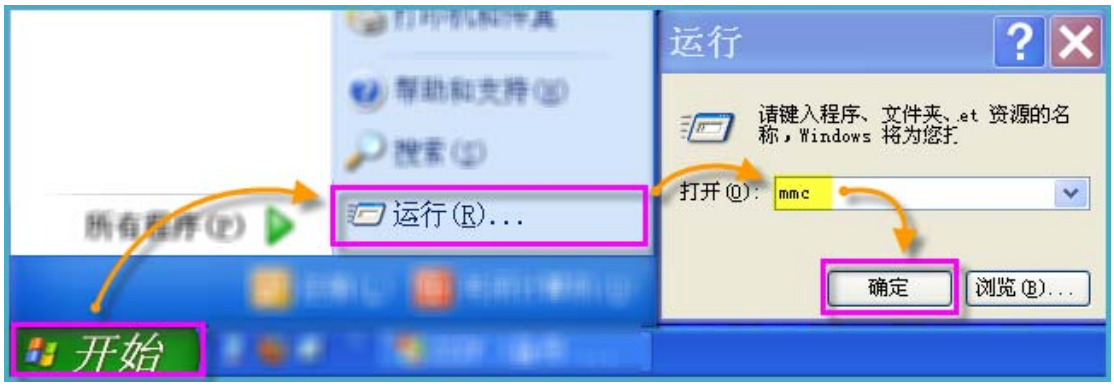
(2). Tor 以开启 2 个链路为例，如需更多链路请相应增加防火墙设置；

(3). 自由门有时端口为 8581，为避免这种情况无法上网，增加了此端口。

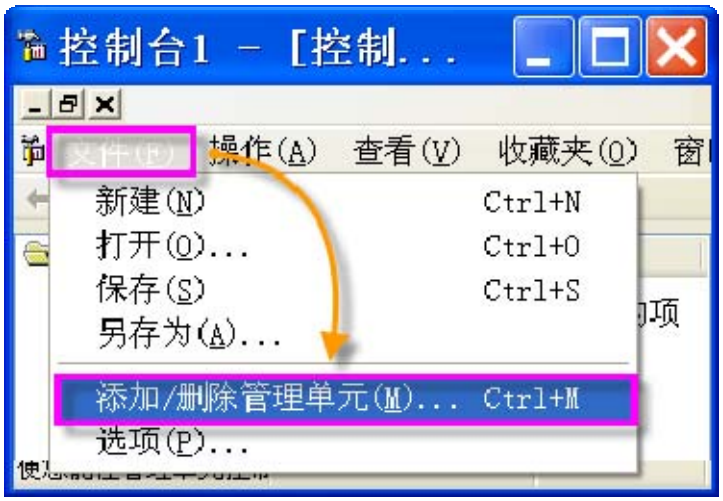
虚拟机内 IP	主机上 Host-only IP	无界端口：443
		自由门/逍遥游端口： 8580/8581
192.168.188.2~ 192.168.188.6	192.168.188.1	Tormanager 端口： http,https 端口：8118/8119 Sock5 端口：9050/9052

1. 建立控制台并导入策略

1. 在**开始** → **运行**输入 **mmc** 点**确定**；创建控制台，是为了观察 IPSEC 的策略表达与实施：



2. 在**文件**，点**添加/删除管理单元**：



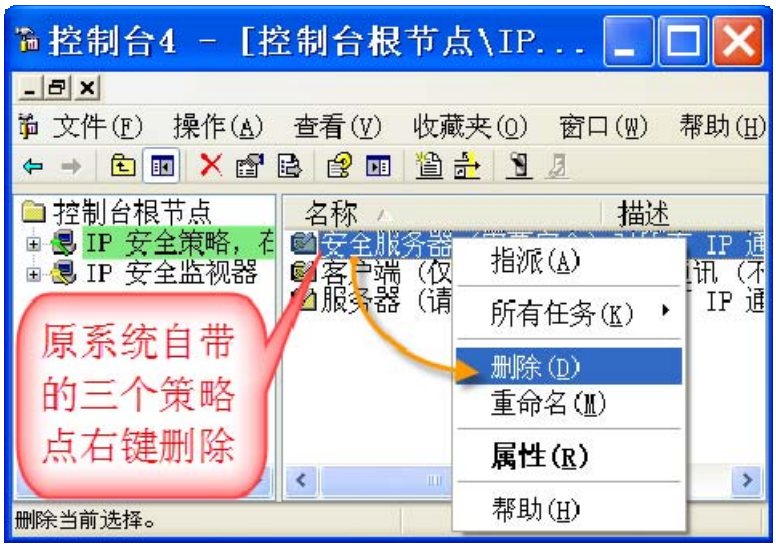
3. 点**添加**：

4. 分别**添加**“IP 安全策略管理”与“IP 安全监视器”，两项均添加完成后点**关闭**：

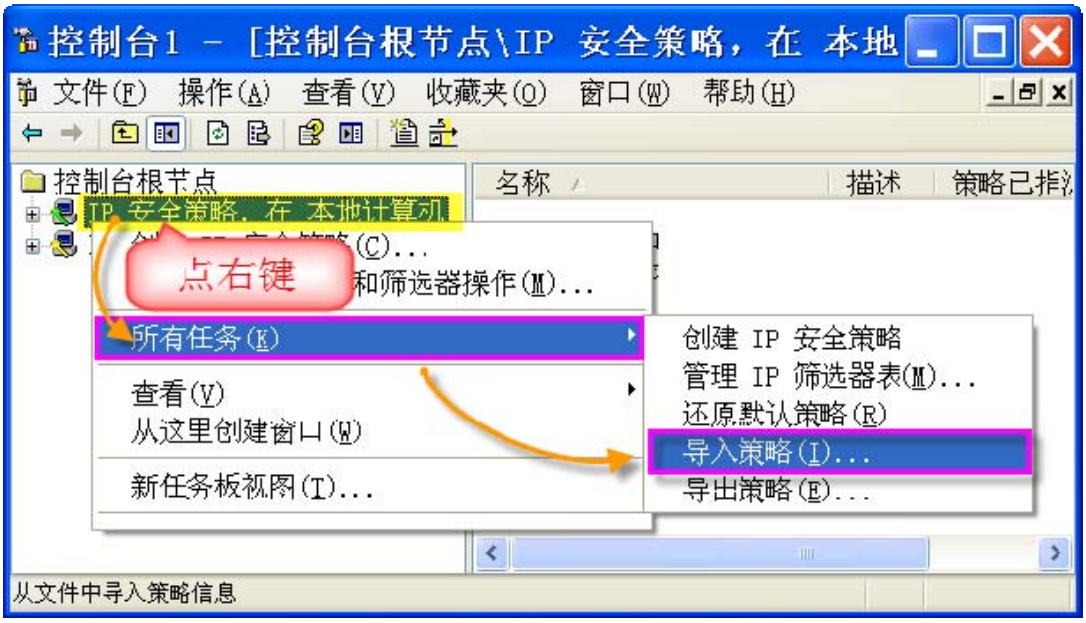
5. 下一步如图默认是**本地计算机**，点**完成**：

6. 添加完成后点**确定**：

7. 删除系统自带的三个策略；这是为了后续删除一些无关的规则（避免无意中使用错误规则带来隐患）。



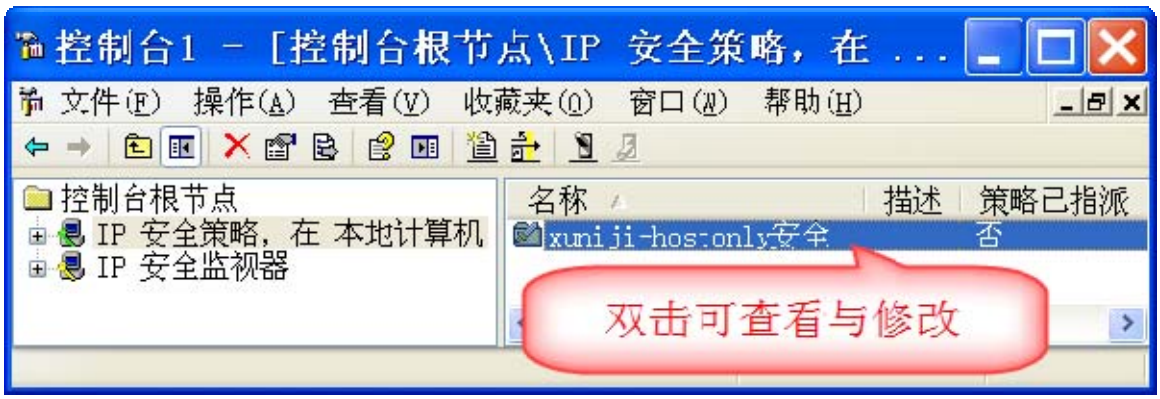
8. 在 **IP 安全策略、在本地计算机**点右键 → **所有任务** → **导入策略**：



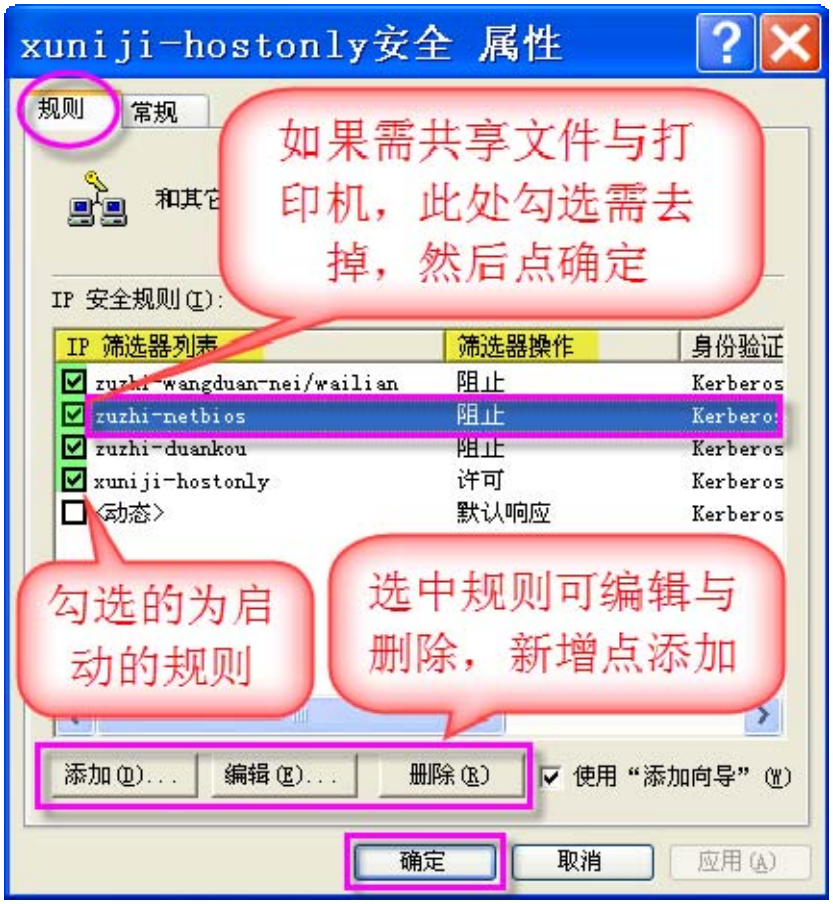
9. 找到最新下载的 IPSEC_ZHUJI_X.ipsec，点**打开**；X 代表不同的更新版本：

2. 策略查看与修改

1. 导入后，双击可查看与修改：

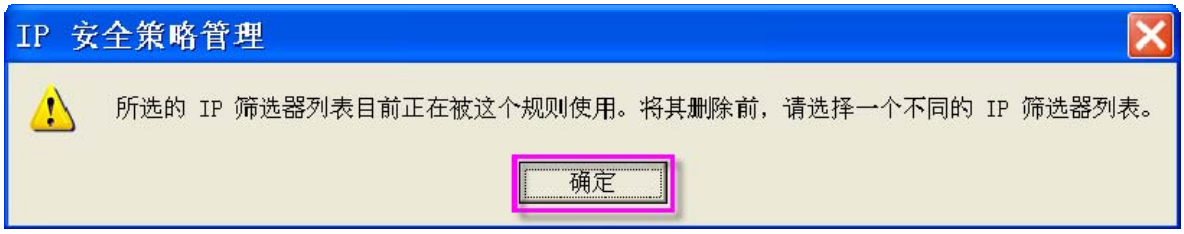


2. 如果需添加新规则可点**添加**；不需要的规则可点**删除**；双击可查看与修改；**只对 IP 筛选器进行修改，其它的规则定义和 IP 筛选操作不要修改。**

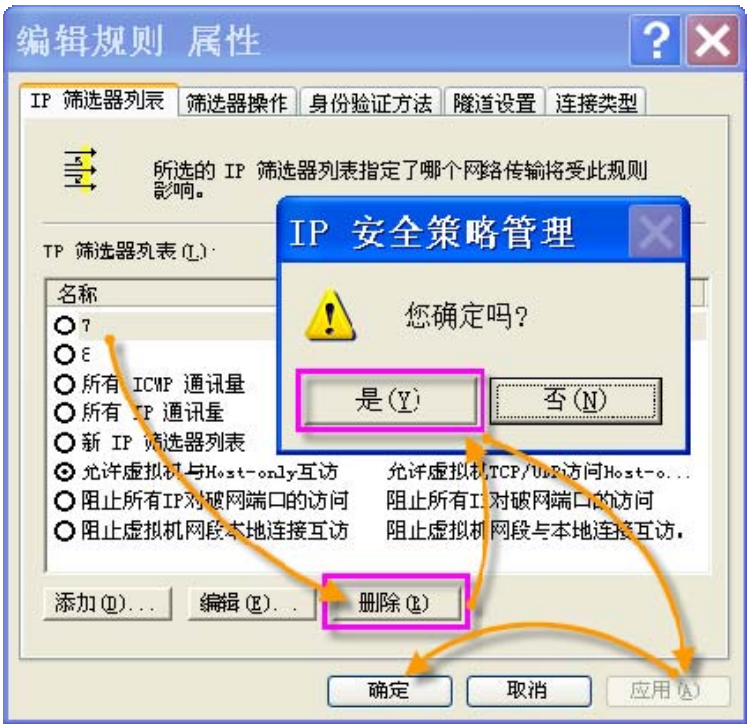


3. 除这四条绿色的规则外其余所有规则均删除（粉色框中内容以自己当前电脑为准，不一定是图示的样子）；这就是上面所说：如果系统自带策略不删除，相关的规则是不允许删除的。

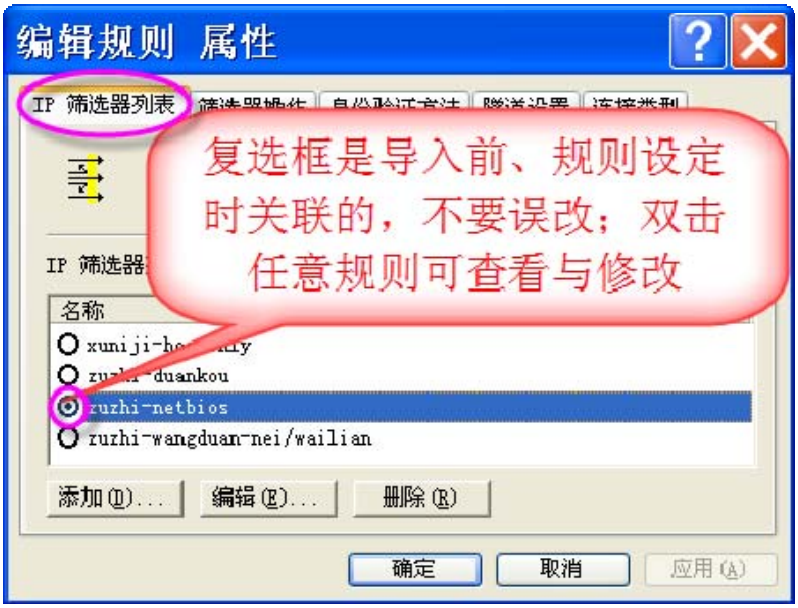
4. 不用担心误删除我们所用的规则，会自动出现以下提示、说明不可删除。



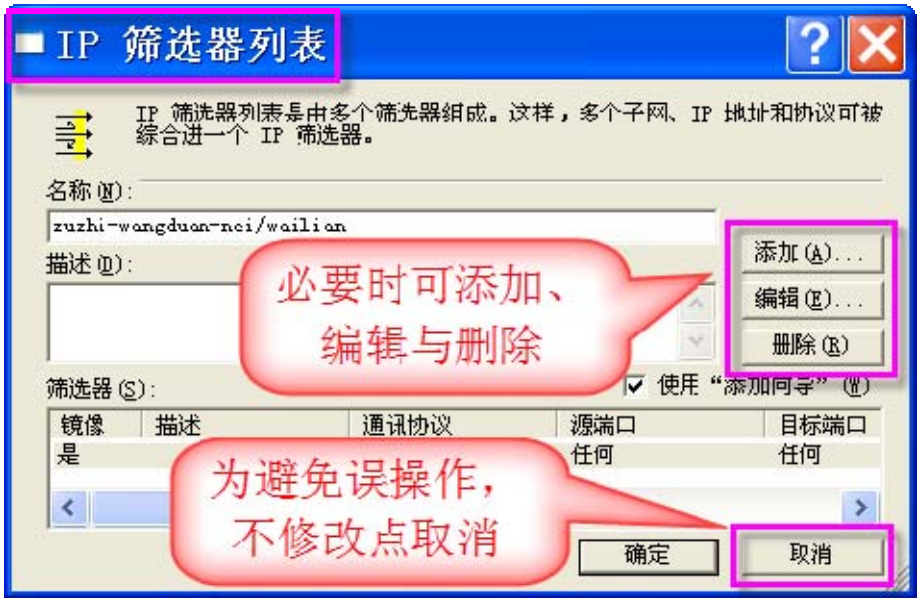
5. 删除时先选中该行，点**删除 → 是(Y) → 应用 → 确定**：



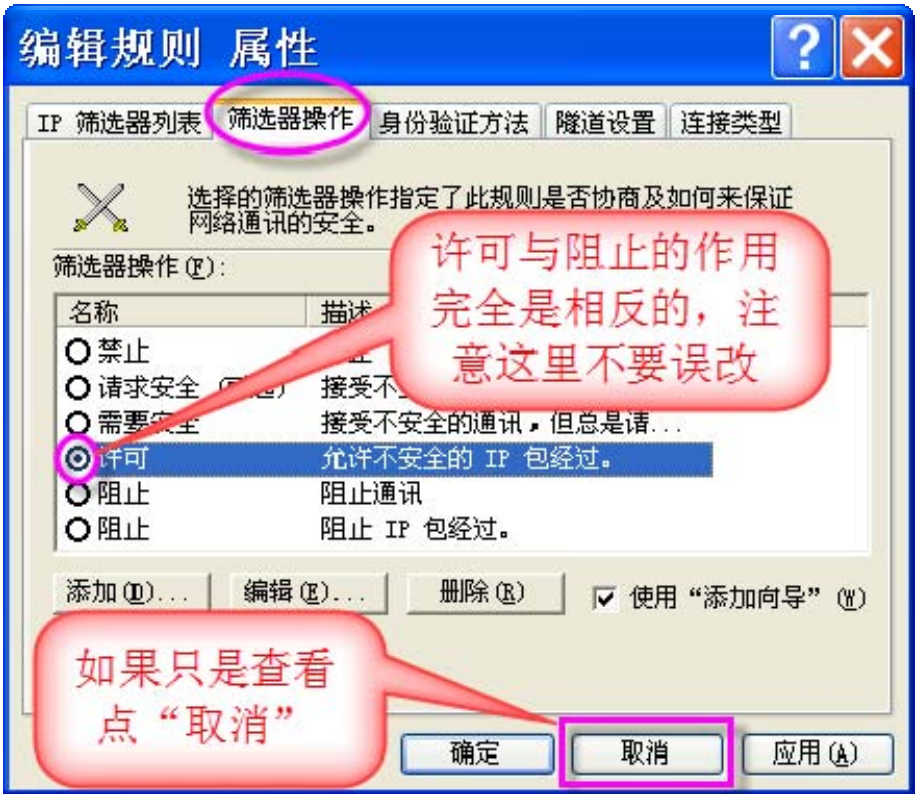
6. 所有规则均显示在这里，相关的选项的复选框是选中的，不要改动。双击该行可查看与修改。



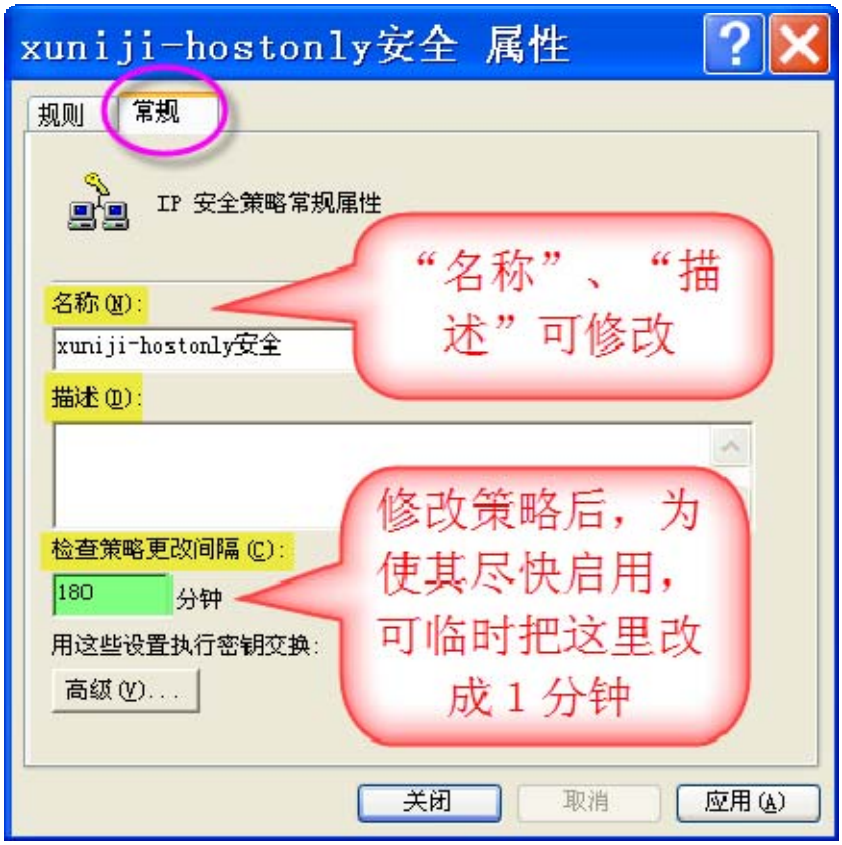
7. 可**添加**、**编辑**与**删除**筛选器；修改完点**确定**，如未修改、点**取消**（避免无意中的修改）：



8. **筛选器操作**也非常关键，**IP 筛选器列表**中的规则最终是**允许**还是**阻止**效果是相反的。不修改的话用**取消**退出当前画面：



9. 在**常规**，如果修改了策略又希望尽快实施的话，可修改**检查策略更改间隔**；
注意：IPSEC 的实施与停止会有时间延迟。如果更改后测试结果有问题，可从启电脑后再试。为了避免有敏感信息，用了较简易的名称，描述空白；可自行添加与修改。



10. 修改后点**应用**、**确定**，未修改点**取消**退出画面：

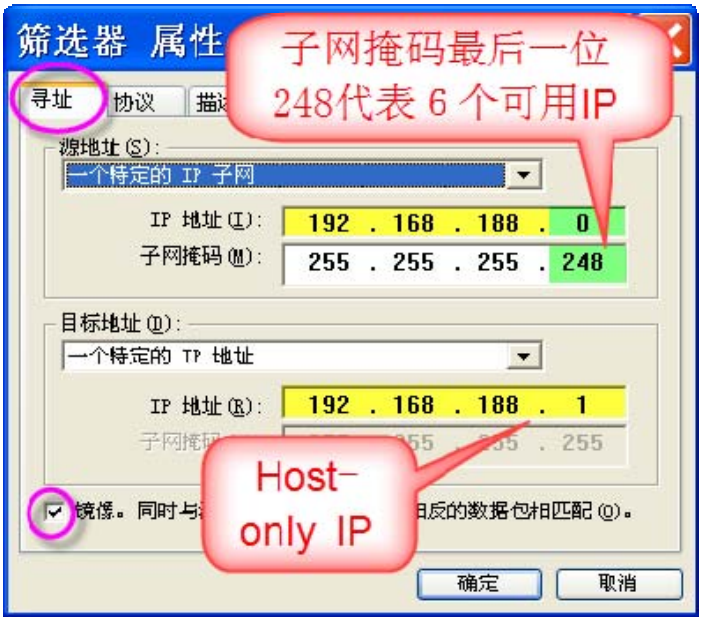
3. 四条规则

1. 许可虚拟机与 Host-only 基于破网端口的互访（xuniji-hostonly）

（1） **源地址**与**目标地址**均可以通过修改子网掩码增加可用 IP 数，请参考（2）的说明；目标端口可根据实际情况增加：

源地址/IP 掩码	192.168.188.0/255.255.255.248
目标地址/IP 掩码	192.168.188.1
源端口	任何
目标端口	8580/8581/8118/8119/9050/9052/443
通讯协议	TCP
镜像	是
操作	许可

（2）在**寻址**，IP 范围用**一个特定的 IP 子网**来实现。勾选**镜像**，反方向亦适用。

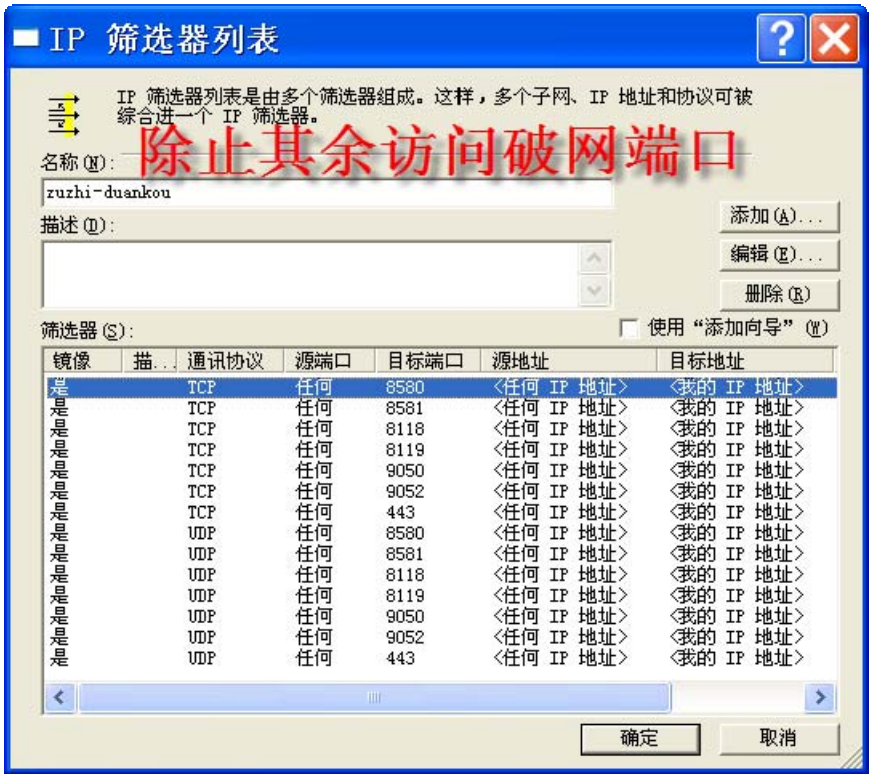


（3）在**协议**，在**到此端口**修改对应的端口；每个**协议**与**端口**要逐项添加：

2. 阻止除以上规则外对破网端口的访问（zuzhi-duankou）

（1）目标端口可根据实际情况添加：

源地址	任何 IP 地址
目标地址	我的 IP 地址
源端口	任何
目标端口	8580/8581/8118/8119/9050/9052/443
协议	TCP/UDP
镜像	是
操作	阻止



（2）勾选**镜像**：

（3）**协议**与**端口**逐项添加：

3. 阻止除以上规则外与虚拟机网段的通讯（zuzhi-wangduan-nei/wailian）

（1）除规则允许的访问，阻止与 192.168.188.x 网段的通讯：

源地址	192.168.188.x
目标地址	任何 IP 地址
源端口	任何
目标端口	任何
协议	任何
镜像	是
操作	阻止

（2）注意这里掩码与 IP 地址最后一位均为 0：

4. 阻止网络共享端口（zuzhi-netbios）

注意：如果开启文件与打印机共享，必须将导入规则中的 zuzhi-netbios 去除勾选（不起作用），否则共享无法实现。

源地址	任何 IP 地址
目标地址	我的 IP 地址
源端口	任何
目标端口	135/137/138/139/445
协议	TCP/UDP
镜像	是
操作	阻止

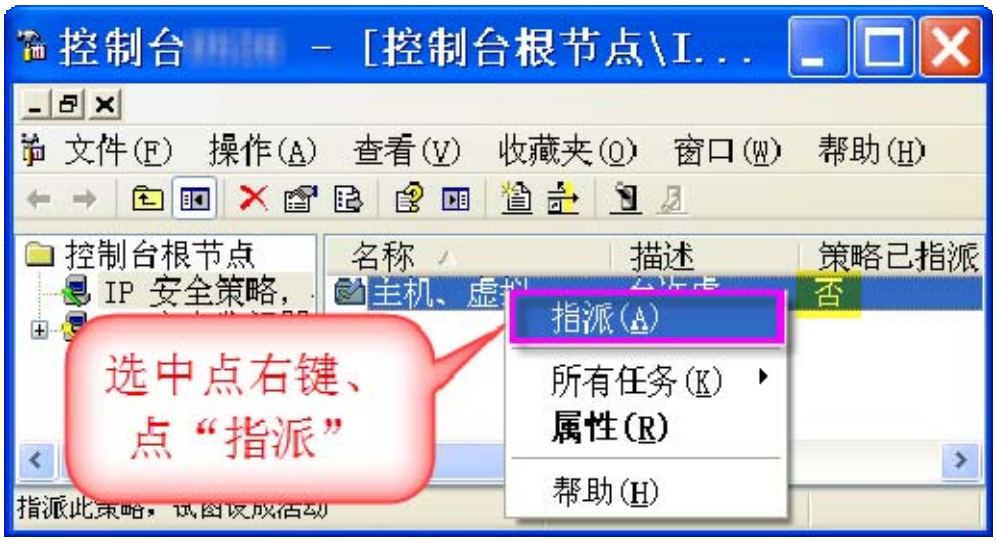

筛选器 属性
寻址
协议
描述
源地址(S):
任何 IP 地址
目标地址(D):
我的 IP 地址
镜像。同时与源地址和目标地址正好相反的数据包相匹配(O)。
确定
取消


筛选器 属性
寻址
协议
描述
选择协议类型(P):
TCP
6
设置 IP 协议端口:
从任意端口(F)
从此端口(R):
到任意端口(T)
到此端口(O):
135
确定
取消

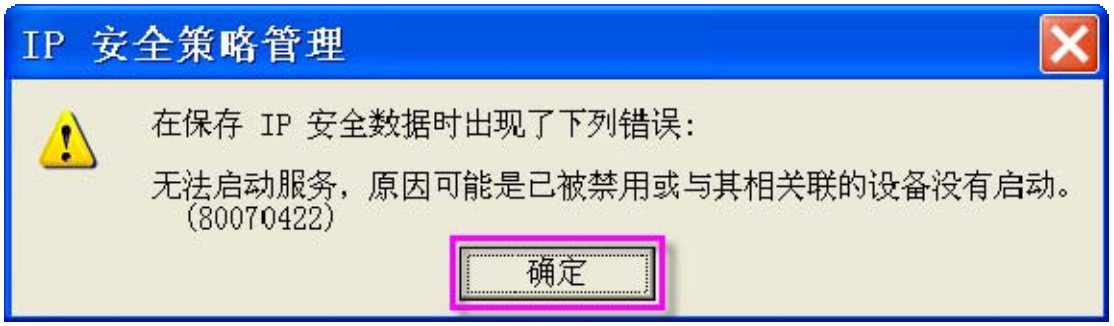

筛选器 属性
寻址
协议
描述
选择协议类型(P):
UDP
17
设置 IP 协议端口:
从任意端口(F)
从此端口(R):
到任意端口(T)
到此端口(O):
135
确定
取消

4. 指派主机策略

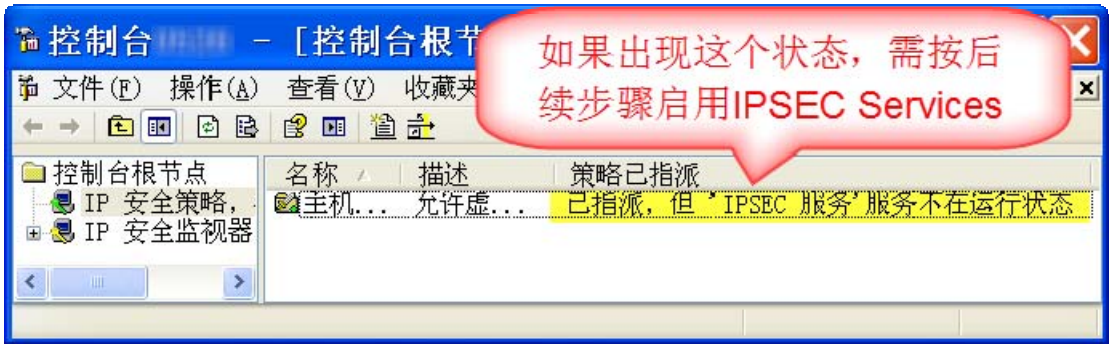
1. 选中导入的策略，点右键、点**指派**：



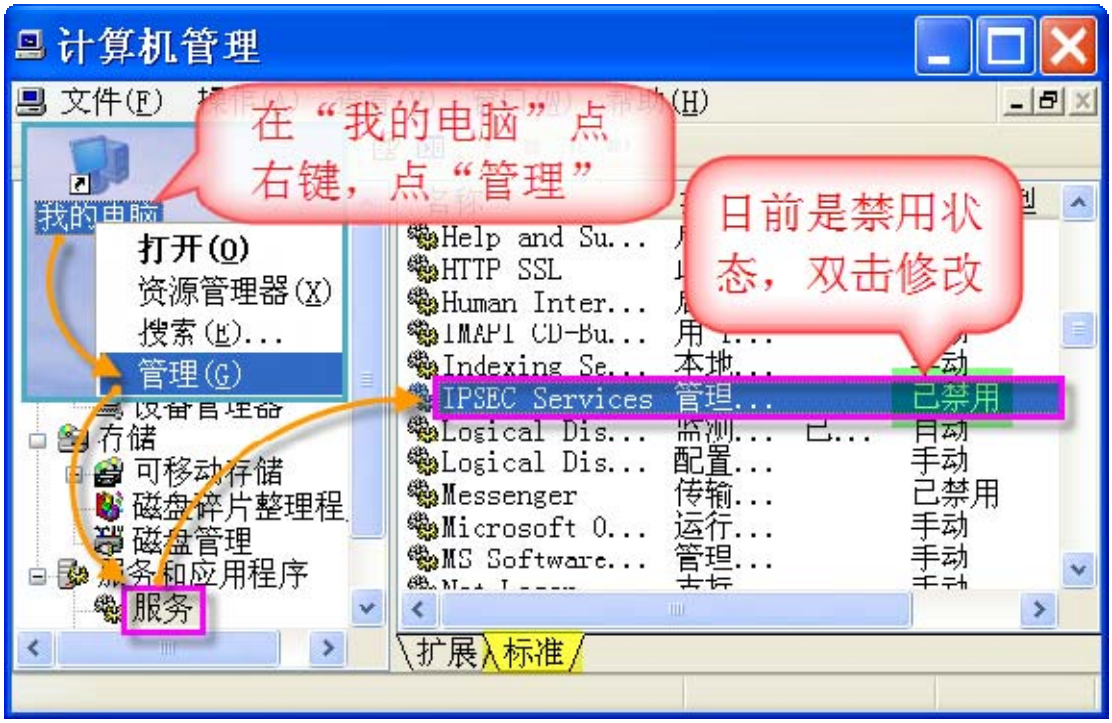
2. 错误提示：



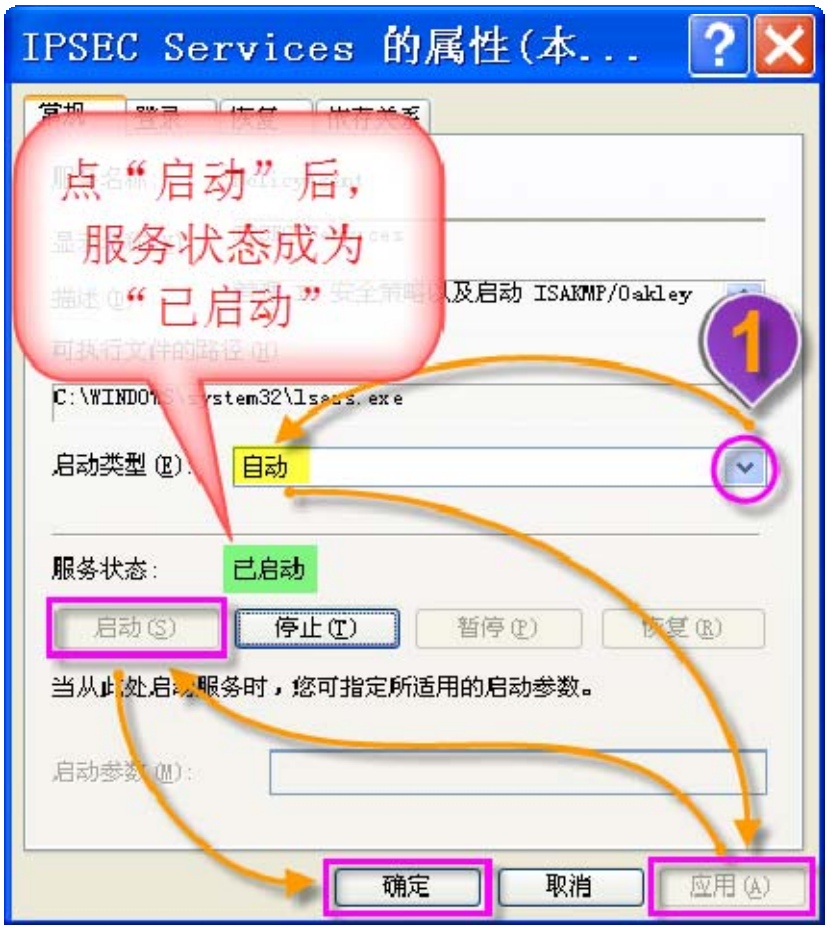
3. 如果出现以上提示，策略已指派的状态如下，请按后续方法解决：



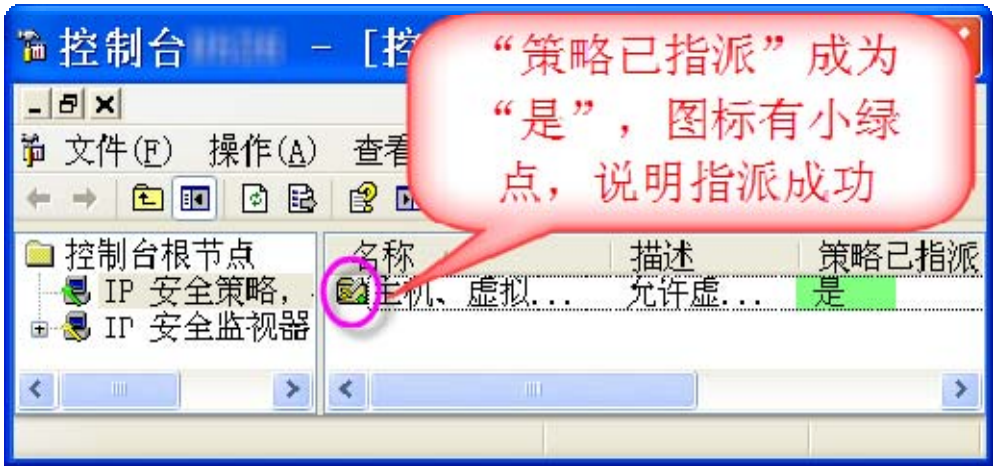
4. 在**我的电脑**点右键 → **管理** → **服务和应用程序** → **服务**，双击 **IPSEC Services**：



5. 在图示 1 的小箭头找到**自动**，然后按图示顺序操作直至**确定**：



6. 正常后**策略已指派**会显示**是**，图标有绿色小点：



二、 主机 COMODO 的设置（任选一）

1. 导入与查看设置

1. 在**其它**，点**管理我的配置**：

2. 点**导入**：

3. 找到下载的 COMODO314_ZHUJI_X（X 代表不同的版本，只要下载网站的附件即可），点**打开**：

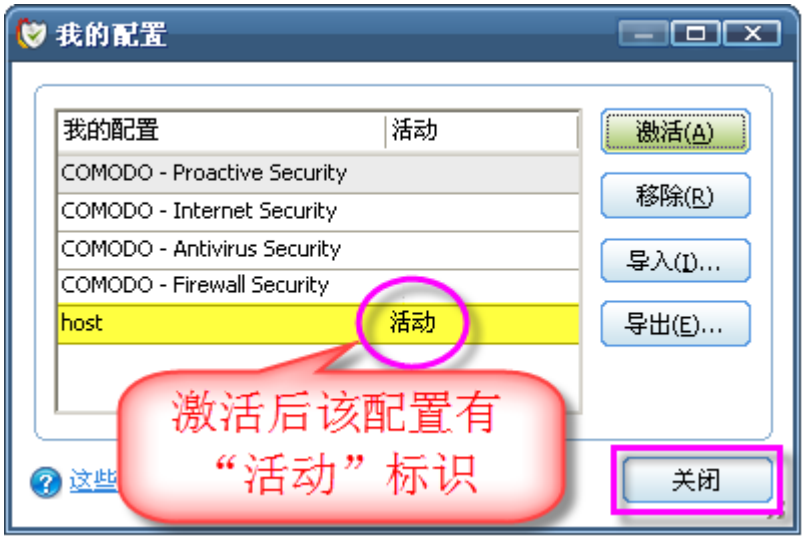
4. 导入时会自动带入名称，也可自行修改，点**确定**：

5. 导入成功提示：

6. 选中导入的配置名称，点**激活**，出现提示点**确定**：

注意：一定要激活才起作用；另外，对于高级用户如果临时不用 Host-only 方案，而又想让虚拟机上网，可暂时激活其它普通策略（单纯关闭 Comodo 不行）。但是如果正式使用时忘了激活本方案的导入策略将非常危险，因此一般用户不要尝试，一定要保证导入策略是激活状态。

7. 激活后该配置右侧有“**活动**”标识：



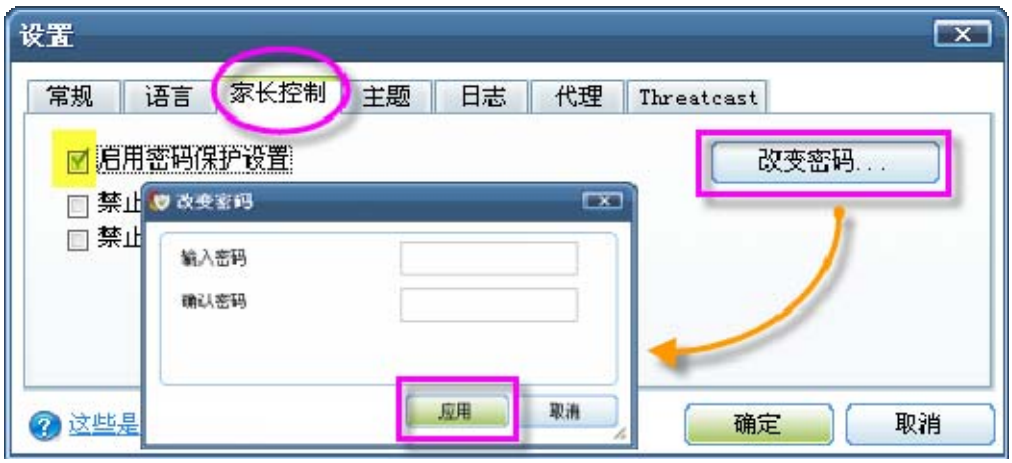
注意：导入规则后请第一时间设置密码，以避免规则等被查看与修改，保证安全。详细请参考下一页密码的设置与修改。

8. 在**其它**，点**设置**：

9. 在**常规**，去掉**自动检测程序升级**的勾选。不升级不影响功能实施。

重要提示：不可升级，升级后有不安全软件商成为防火墙信任软件商，会有安全隐患。

10. 在**家长控制**，勾选**启用密码保护设置**，**输入密码**并**确认密码**后，点**应用**：



（返回导入规则）

11. 在**日志，日志文件大小超过**改成 1MB，注意禁用日志的两个选项不要勾选，以便今后有问题时查看。为了保护隐私，要及时或定期清除日志：

12. 在 **DEFENSE+ → 高级设置 → Defense+设置**：

13. 在**一般设置**，（1）把 **Defense+安全级别**调到**疯狂模式**，（2）去掉**信任被信任软件商数字签名的应用程序**的勾选；（3）勾选**如果本程序关闭，阻止所有未知请求**（注意勾选此项后，如果有时软件运行不正常，有可能是 COMODO 本身运行不正常，这时可把 COMODO 关闭再从启）：

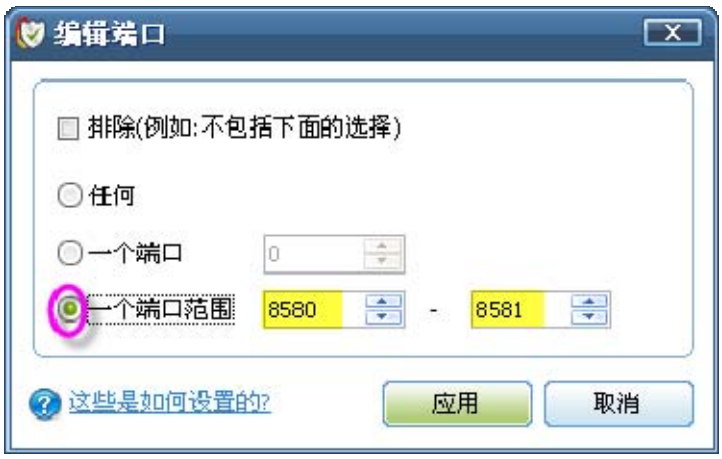
14. 在**监视设置**，勾选所有项。

说明：刚开始会有许多不了解的提示，要多注意观察与尝试，有些不敏感的问题可勾选记忆，敏感的软件出现请求时，建议点选**程序信任为 → 可信程序**，但不要勾选**记住我的选择**，因为记忆后会在安全规则中显示（或每次下网后手动在**应用程序规则/计算机安全规则**中选中相关行、点**移除**）。

15. 在**防火墙 → 常规设置 → 我的端口管理**：

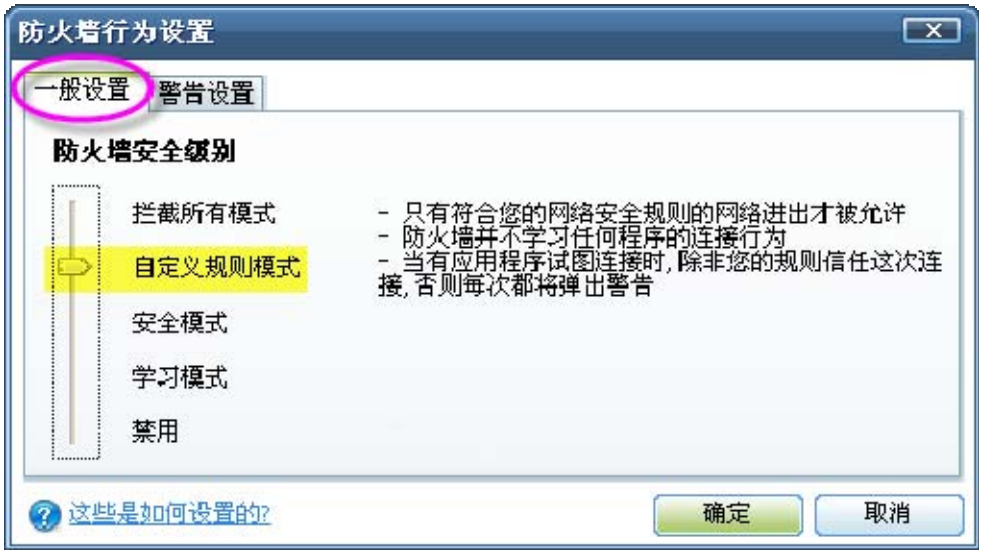
16. 已设置好“安全端口”（破网端口的集合），双击可查看与编辑，新增端口可点**添加**：

17. 可修改端口范围等：



18. 在**防火墙 → 高级设置 → 防火墙行为设置**：

19. 在**一般设置，防火墙安全级别**已设置为**自定义规则模式**：



20. 在**警告设置，警告频率级别**设到很高，并勾选所有项：

21. 在**防火墙 → 高级设置 → 网络安全规则**：

22. 在**应用程序规则**，已有三条规则，允许 Windows 升级；其中注意 Comodo 要禁止联网（避免升级）；System 当内网共享时才需要上网，因此这里也禁止联网。

注意：如果开启文件与打印机共享，需移除阻止 System 这一项。

23. 在**全局规则**，已有如下规则，以下将详述这四条规则：

2. 规则说明

1. 允许虚拟机基于破网端口访问 Host-only（xuniji-hostonly-ru）：

行为	允许
协议	TCP
方向	入
源地址 IP 范围	192.168.188.2~192.168.188.6
目的地址 IP	192.168.188.1
源端口	任何
目的端口	安全端口(8580/8581/8118/8119/9050/9052/443)

（1）COMODO 与有些防火墙不同，就是方向本身已包含了双向通讯。比如允许方向是**出**，它同时允许由其发起的回应的**入**；当然，并不包含由其它因素引起的**入**。而 ZA 与 IPSEC 均是单向，要想要双向通讯成功，需双方向均设置。

说明：为了不使日志过于繁杂，允许的规则一般不勾选“**如果触发了规则，将在防火墙日志中记录**”。

（2）如需增加可用 IP 数量，可修改**单个 IP** 到 **IP 范围**；如果想修改 IP 地址，可修改**网络地址**最后一位；如果网段不同，可修改**网络地址**相应位置：

（3）**说明**：无论方向如何（**出/入**），**源端口**一定对应的是源端口，而不会出现选“出”时是源端口，选“入”时是目的端口：

（4）修改后点**应用**，如果只是查看，为避免误改，可点**取消**：

2. 除以上规则外，阻止虚拟机、Host-only 网段的外连(zuzhi-wangduan-wailian)

行为	阻止
协议	IP
方向	出/入
源地址/IP 掩码	192.168.188. 0/255.255.255.0
IP 细节	任何

（1）同上，IP 地址可根据实际情况修改；但规则不要修改。以下举例说明方向选择出/入的含义：比如，阻止 Host-only IP 出站连接主机的本地连接；阻止虚拟机 IP 连入到主机本地连接等。以上两个例子中的源地址均属于 192.168.188.x 网段的。

（2）其实也同时阻止了虚拟机与 Host-only 基于非破网端口的互访：

（3）**IP 协议**“任何”包括了 TCP/UDP/ICMP/IGMP 等：

3. 除以上规则外，阻止内连虚拟机、Host-only 网段(zuzhi-neilian-wangduan)

阻止除允许规则外的一切 IP 内连到虚拟机或 Host-only 网卡，保证两个主要部份的安全：

行为	阻止
协议	IP
方向	出/入
源地址	任何
目的地址/IP 掩码	192.168.188.0/255.255.255.0
IP 细节	任何


过滤控制规则
常规
行为:
阻止
如果触发了规则,将在防火墙日志中记录
协议:
IP
方向:
出/入
描述:
zuzhi-neilian-wangduan
源地址
目的地址
IP 细节
排除(例如:不包括下面的选择)
任何
单个IP
这些是如何设置的?
应用
取消


过滤控制规则
常规
行为:
阻止
如果触发了规则,将在防火墙日志中记录
协议:
IP
方向:
出/入
描述:
zuzhi-neilian-wangduan
源地址
目的地址
IP 细节
排除(例如:不包括下面的选择)
任何
单个IP
IP 范围
IP 掩码
区域
网络地址:
192 . 168 . 188 . 0
掩码:
255 . 255 . 255 . 0
这些是如何设置的?
应用
取消

4. 除以上规则外，阻止连接本机端口（zuzhi-duankou）

行为	阻止
协议	IP
方向	入
源地址	任何
目的地址	任何
IP 细节	任何

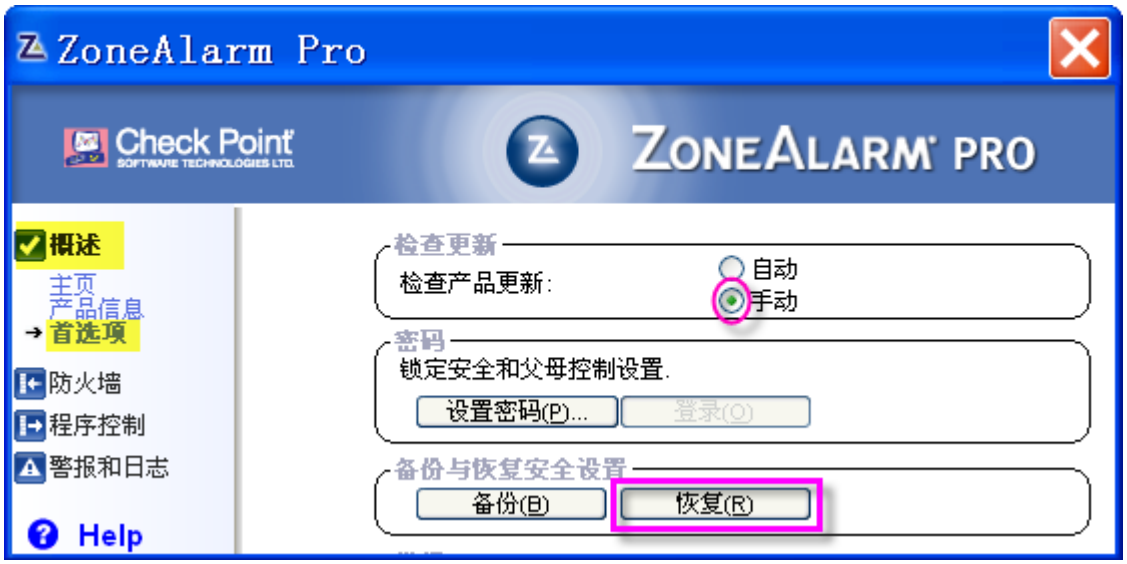
说明：由于如上所述，Comodo 的方向是（基于发出方）双向的，因此这里可以设置阻止一切 IP 的入（指发起方非本机），因此不会影响由本机发起的正常通讯；而且这样设置涵盖更广、更严密。ZA 与 IPSEC 不能这样设置，需具体设置相应的端口。

三、 主机 ZoneAlarm Pro 的设置（任选一）

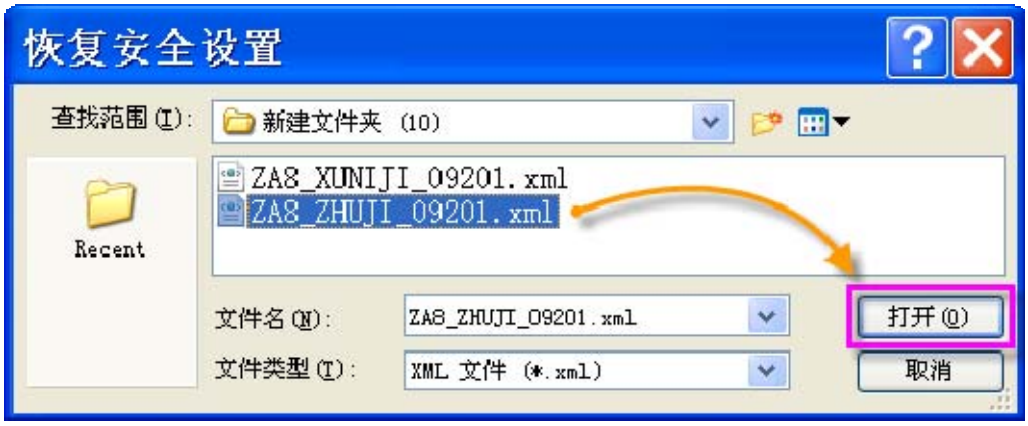
导入规则，ZA8_ZHUJI_X（X 代表不同的版本，只要下载网站附件即可）

1. 导入与查看设置

1. 在**概述** → **首选项**，把**检查产品更新**改为**手动**，再点**恢复**：

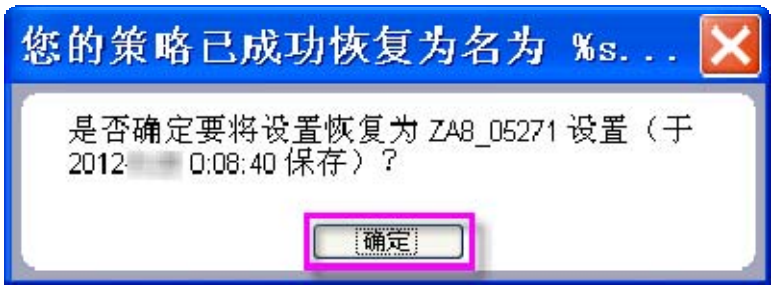


2. 找到最新下载文件 ZA8_ZHUJI_X.xml，X 为不同的版本系列，点**打开**。
说明：主机导入的文件有 ZHUJI 字样，虚拟机导入的文件有 XUNIJI 字样：



3. 点**确定**：

4. 点**确定**：



5. 注意：导入后在第一时间设置密码。在**概述 → 首选项**，点**设置密码**；如果出现**旧密码**，说明已设置密码；如果没出现**旧密码**直接输入两次新密码，点**确定**；**允许他人无密码使用程序**不要勾选；为保证防火墙不被任意修改，可点**注销**：

6. 导入后的规则在**防火墙 → 专家级**可以看到。以下是组的相关说明。

注意： ZA9 的**组**由于程序本身的原因不可用，因此实际导入规则中未用组的方法，此处作为**组**的介绍保留，以便其它版本可用，并且有助于理解后续内容。

7. 在**组管理器 → 位置**，选择一条**位置组**，点**编辑**（可点击**添加**增加多个位置组）：

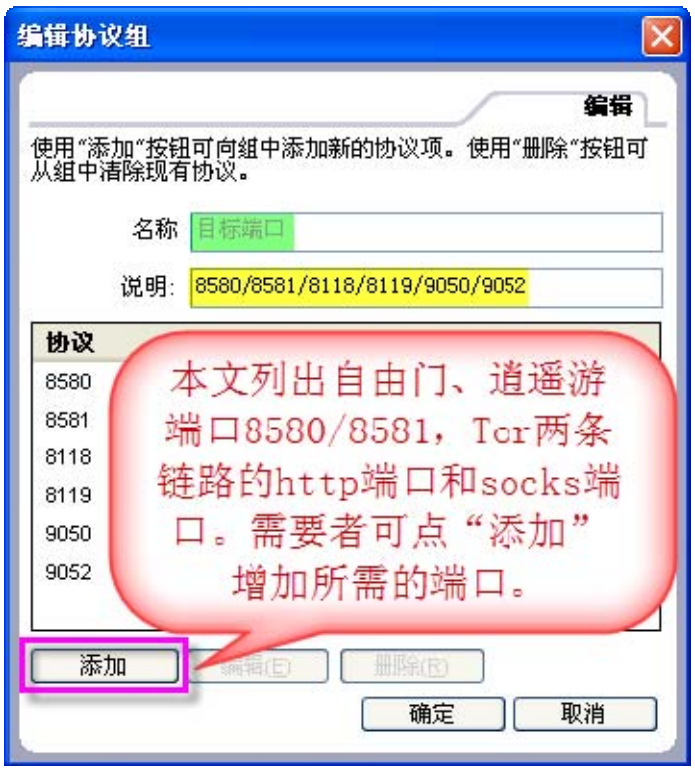
8. 选择一条**位置**点**编辑**（可点击**添加**来增加多条位置）：

9. 本文 Host-only IP 以 192.168.188.1 为例：

10. 本文虚拟机 IP 范围以 192.168.188.2~192.168.188.6 为例：

11. 在**组管理器 → 协议**，设置相关的协议与端口。点**编辑**查看或修改：

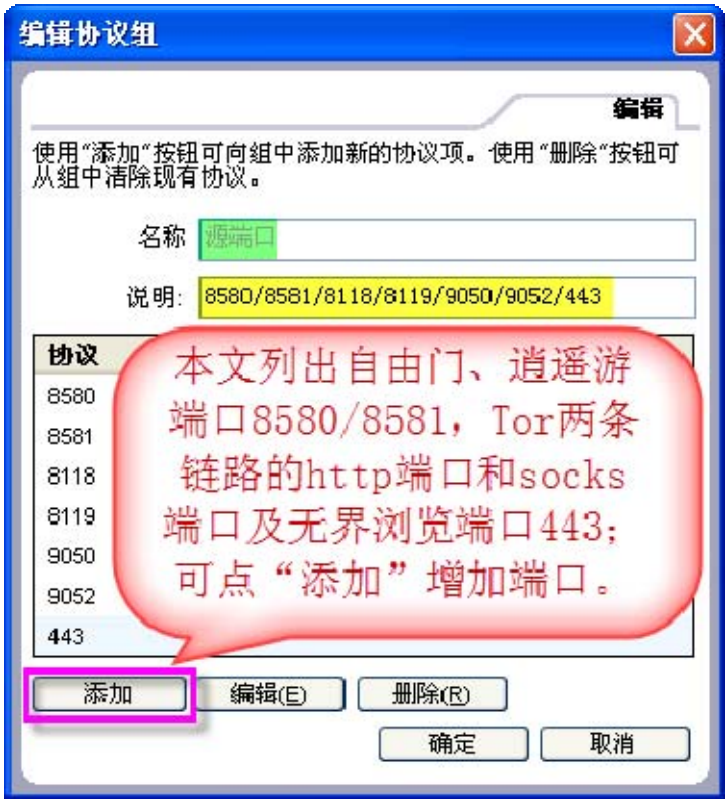
12. 在**编辑协议组**，选中一条协议点**编辑**查看或修改；如需更多端口可点**添加**：



13. 在**编辑协议**，可修改**协议**或**目标端口**：

说明：目标端口输入“443”，左侧会自动变为“HTTPS”；输入 8580 等，左侧会自动变为“其它”。

14. 在**编辑协议组**，选中**源端口**一条协议、点**编辑**可以查看或修改，如需更多端口可点**添加**：



15. 由上继续，在**编辑协议**，可修改**协议**与**源端口**：

2. 规则说明

1. 以上是**组**的建立与修改。**组**建立好以后，就可以建立或修改规则了。规则的排列是有优先顺序的，排列在前的优先级高（即**次序**越小的优先级越高）；在**防火墙 → 专家级**，双击任一条规则查看或修改。

注：为了不带有敏感信息，规则中的注释为空白，需要时可查看教程中的解释。另外由于没有用**组**的方法，实际看到**协议**处是 8580/8581/8118/8119/9050/9052/443 字样。

2. 说明：

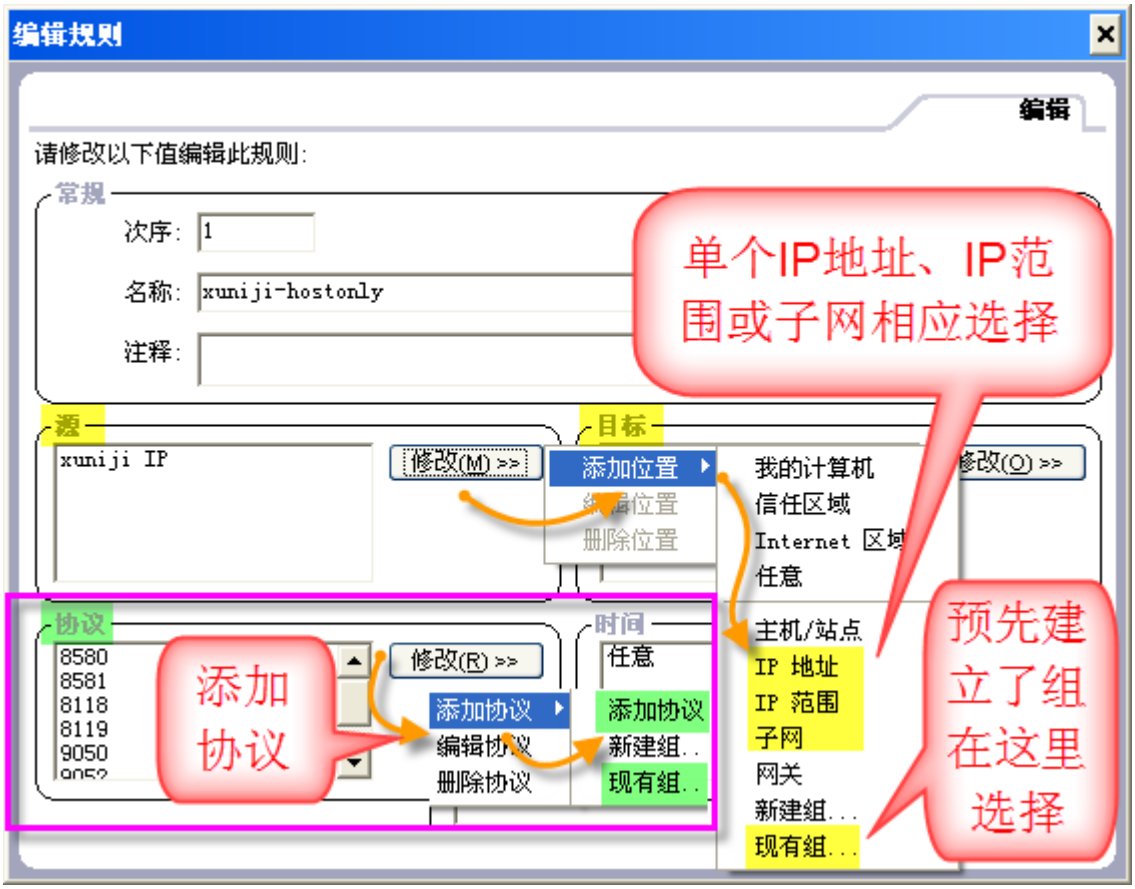
（1） 通常所有规则的**状态**均是“启用”状态，如果是测试，可临时禁用、再启用。**真正使用时注意启用**；

（2） **操作**的**允许**与**拦截**作用完全相反，一定要注意，不要误改；

（3） **操作**选**拦截**的最好选择**跟踪**（警告与日志），这样有触犯规则的会反映到日志，便于查看；**如果不能正常上网，也要到日志去查看哪里有问题**；

（4） 点击**源**、**目标**、**协议**的**修改**来查看与修改；**时间**无需修改，因为我们需要规则时时防范：

3. **源**、**目标**点**修改** → **添加位置**，然后选择相应内容，如果是单个 IP 可选 **IP 地址**，如果是一个 IP 范围可选 **IP 范围**，子网可选**子网**等；如果预先建立了组，可选**现有组**；**协议**点**修改** → **添加协议**，如果预先建立了组可选**现有组**，或直接选**添加协议**，如果涉及多个端口或协议需多次添加：

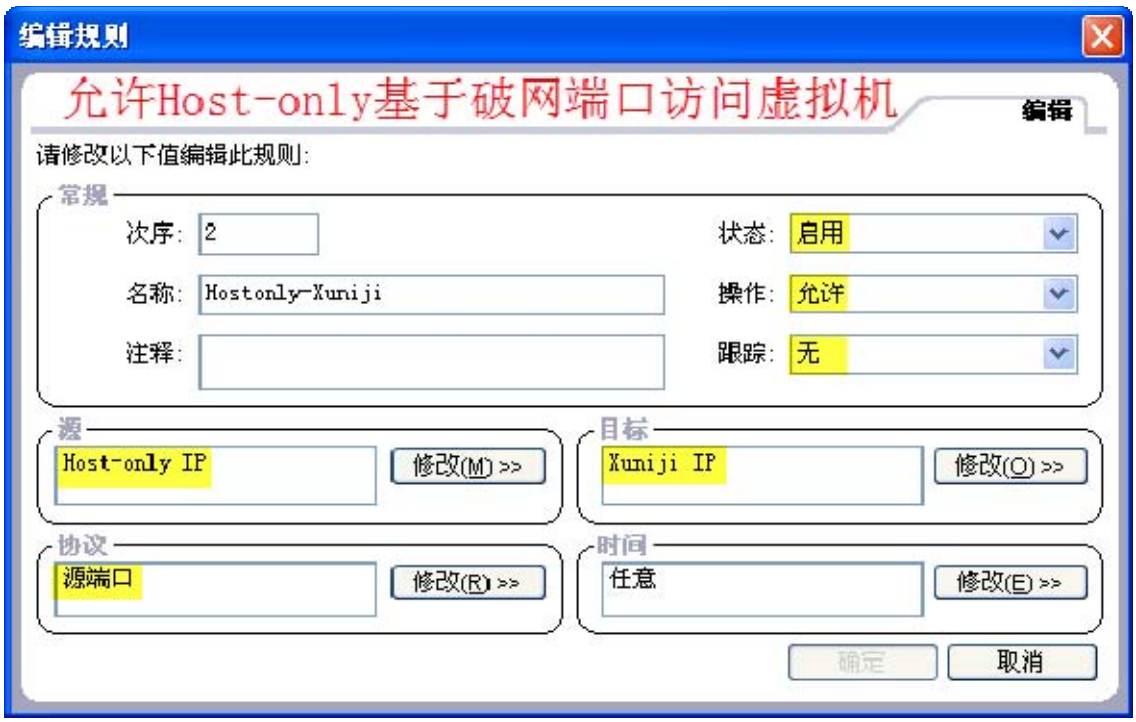


4. 允许虚拟机基于破网端口访问 Host-only(xuniji-hostonly)

状态	启用
操作	允许
跟踪	无
源	虚拟机 IP 范围(组：Xuniji IP)　　192.168.188.2~192.168.188.6
目标	Host-only　IP(组：Host-only IP)　　192.168.188.1
协议	目标端口（组：目标端口）8580/8581/8118/8119/9050/9052/443
时间	任意

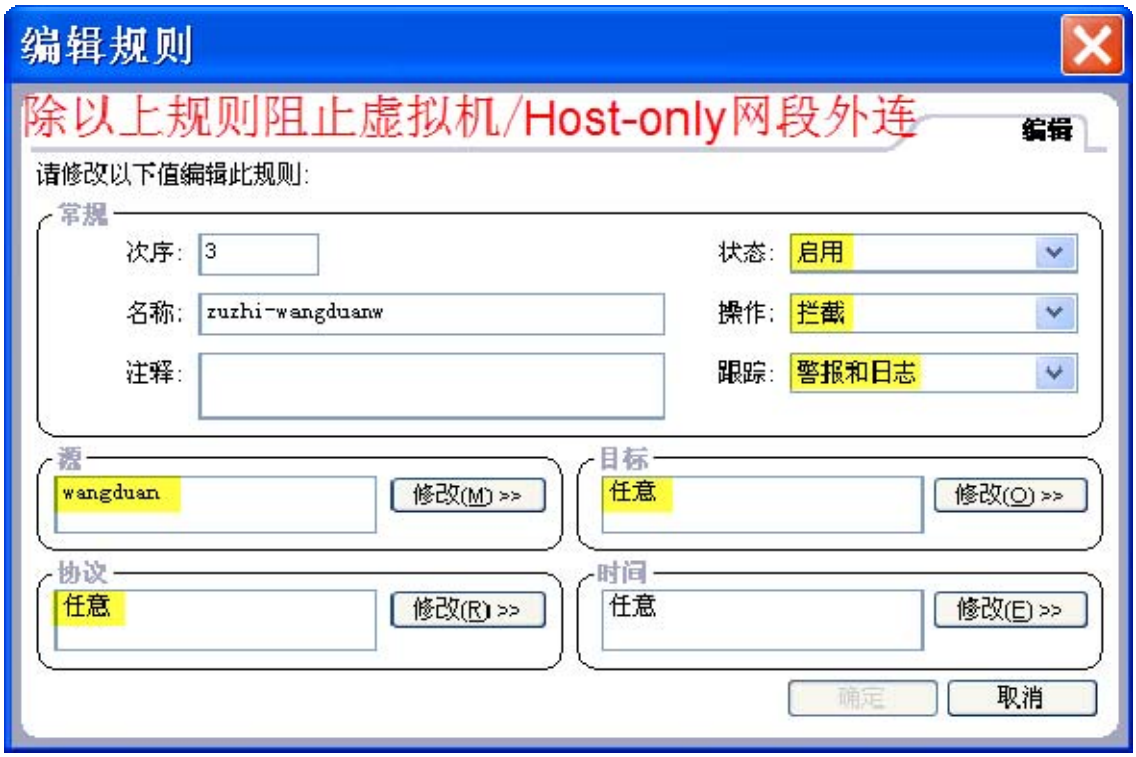
5. 允许 Host-only 基于破网端口访问虚拟机(hostonly-xuniji)

状态	启用
操作	允许
跟踪	无
源	Host-only IP（组：Host-only IP） 192.168.188.1
目标	虚拟机 IP 范围(组：Xuniji IP) 192.168.188.2~192.168.188.6
协议	源端口 8580/8581/8118/8119/9050/9052/443
时间	任意



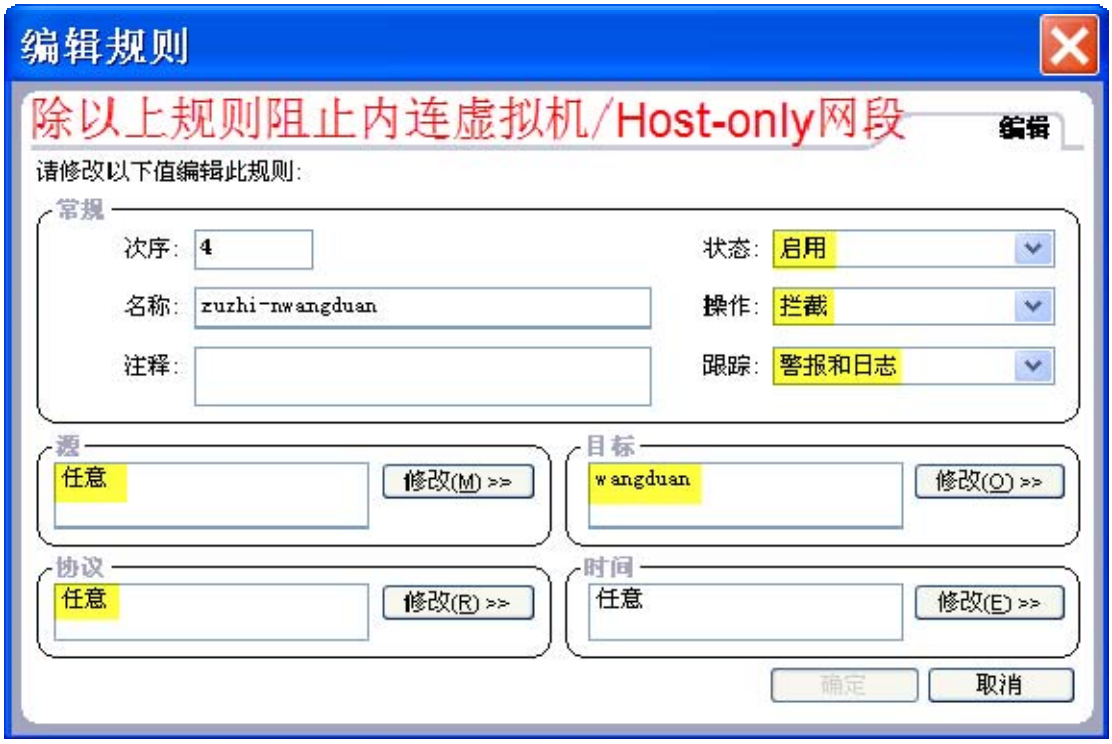
6. 阻止虚拟机/Host-only 网段外连(zuzhi-wangduanw)

状态	启用
操作	拦截
跟踪	警告和日志
源	虚拟机与 Host-only 网段 192.168.188.0/255.255.255.0 （组：wangduan）
目标	任意
协议	任意
时间	任意



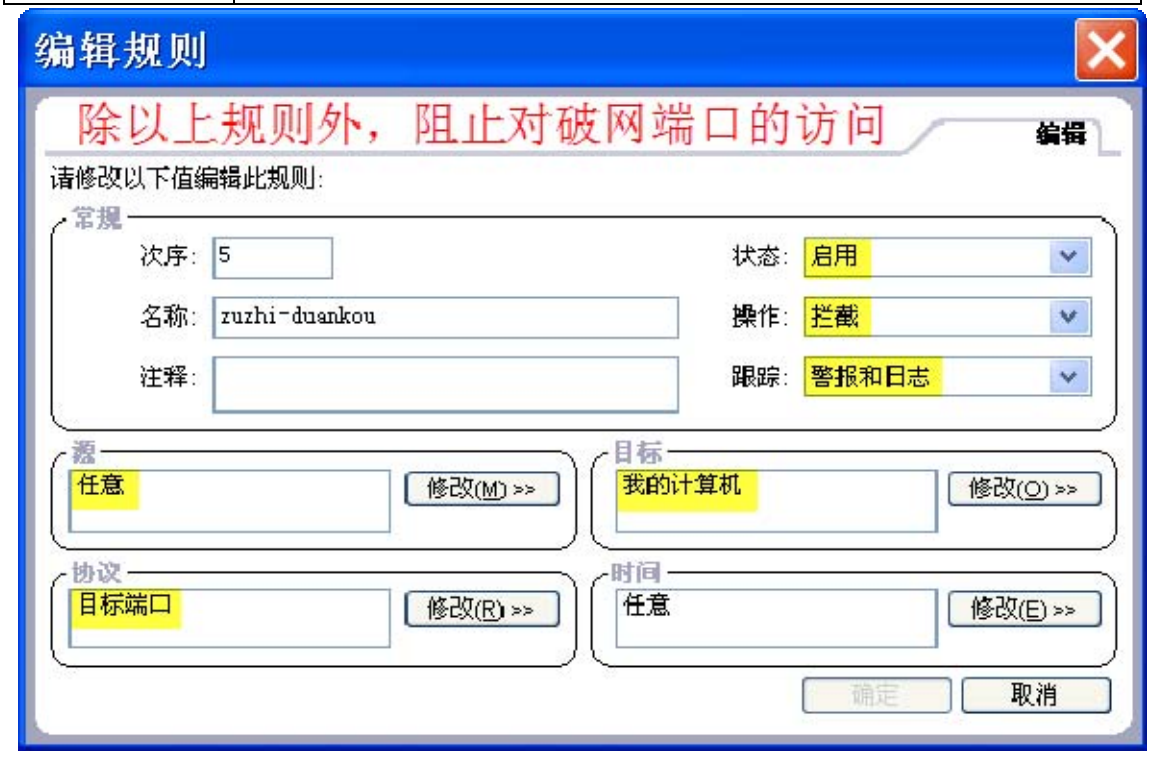
7. 阻止内连虚拟机/Host-only 网段 (zuzhi-nwangduan)

状态	启用
操作	拦截
跟踪	警告和日志
源	任意
目标	虚拟机与 Host-only 网段 192.168.188.0/255.255.255.0 （组：wangduan）
协议	任意
时间	任意



8. 除以上规则外拦截对破网端口的访问 (zuzhi-duankou)

状态	启用
操作	拦截
跟踪	警告和日志
源	任意
目标	我的计算机
协议	目标端口 8580/8581/8118/8119/9050/9052/443
时间	任意



四、 虚拟机防火墙的设置

虚拟机的防火墙规则：

(1). 允许与 Host-only 基于破网端口的通讯；
(2). 阻止其它一切通讯

1. IPSEC（xuniji 安全）

导入 IPSEC_XUNIJI_X（注意导入有 XUNIJI 标识的相关防火墙）

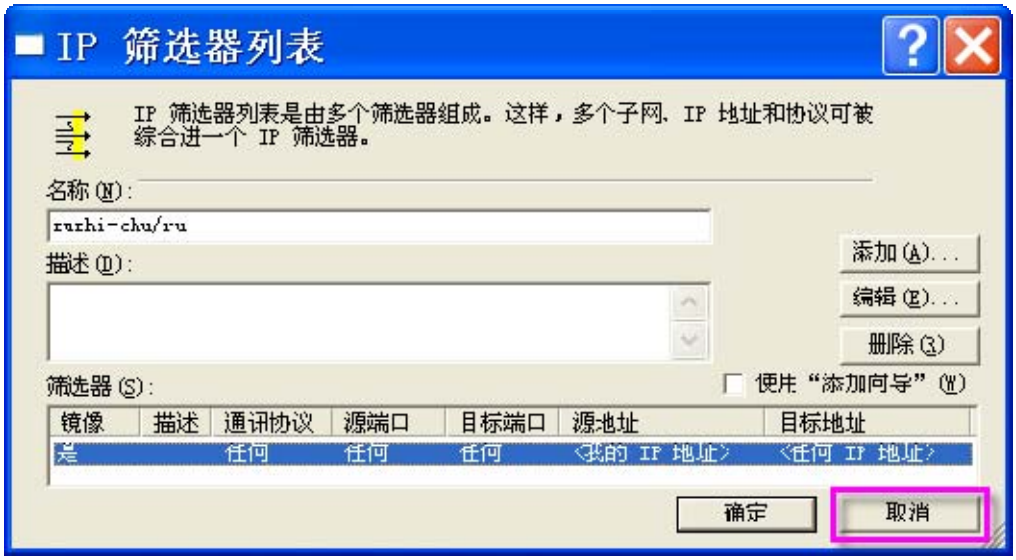
1. 阻止除“许可”规则外一切通讯（zuzhi-chu/ru）

源地址	我的 IP 地址
目标地址	任何 IP 地址
源端口	任何
目标端口	任何
通讯协议	任何
镜像	是
操作	阻止

2. “许可”规则同主机相同，请参考主机相关部份：

3. 选中 **IP 筛选器列表**中 zuzhi-chu/ru 规则双击查看：

4. 不修改的话点**取消**：



2. COMODO

导入 COMODO314_XUNIJI_X（注意导入有 XUNIJI 标识的相关防火墙）

1. 两条规则：

2. 允许虚拟机基于破网端口对 Host-only 的访问（xuniji-hostonly-chu）：

说明：通讯是双向的，COMODO 允许的**出**已同时允许了由虚拟机引发的双向通讯。

行为	允许
协议	TCP 或 UDP
方向	出
源地址/IP 范围	192.168.188.2~192.168.188.6
目的地址/单个 IP	192.168.188.1
源端口	任何
目的端口	安全端口(8580/8581/8118/8119/9050/9052/443)

（1）**源地址**是虚拟机 IP 范围：

（2）**目的地址**是 Host-only IP 地址：

（3）**源端口** → 任何：

（4）**目的端口**选择已经设置好的“**安全端口**”，即破网端口。不修改的话，为避免无意中的修改，点**取消**退出：

3. 阻止其它一切通讯（zhuzhi-chu/ru）

行为	阻止
协议	IP
方向	出/入
源地址	任何
目的地址	任何
IP 细节	任何

（1）**源端口 → 任何**：

（2）目的端口 → 任何：

（3）IP 细节 → 任何：

3. ZoneAlarm Pro

导入 ZA8_XUNIJI_X（注意导入有 XUNIJI 标识的相关防火墙）

1. 两条允许规则（通讯双向），与主机相同请查看主机相关部份；一条阻止规则：

2. 阻止除“允许”规则外一切出站（zuzhi-chu/ru）：

状态	启用
操作	拦截
跟踪	警告和日志
源	任意
目标	任意
协议	任意
时间	任意

五、 联网测试步骤

1. 各网卡运行正常（首先关闭所有防火墙）

主机与虚拟机均运行“设置.bat”及完成手动设置，从启计算机后，查看本地连接、Host-only 网卡、虚拟机本地连接是否连接正常。

2. 破网软件运行正常

破网软件启用并联网，自由门软件需设置好侦听 0.0.0.0，无界浏览需开启“无界分享”，Tor 管理器需设置侦听相关 IP。

3. 虚拟机浏览器或软件代理设置正确

虚拟机浏览器或需上网的软件，代理应是 Host-only 的 IP，端口是正在使用的破网软件的端口。此时浏览器或软件如果能正常上网，请继续下一步。

4. 开启主机第三方防火墙

这时看虚拟机中浏览器或软件是否上网正常。不能上网的话看此防火墙的日志，根据日志排除问题。正常的话继续下一步。

5. 开启虚拟机第三方防火墙

这时看虚拟机中浏览器或软件是否上网正常。不能上网的话看此防火墙的日志，根据日志排除问题。正常的话继续下一步。

6. 指派主机 IPSEC

这时看虚拟机中浏览器或软件是否上网正常。正常的话继续下一步。

7. 指派虚拟机 IPSEC

这时看虚拟机中浏览器或软件是否上网正常。正常的话测试完毕。

结　语

本文仅涉及防火墙的一些基础设置，有些特殊的软件可能需要开放一些特殊的许可，这些都需要大家在使用中琢磨与总结。

大家在使用中有任何问题，请到禁书网讨论。