

ESET 安全套装防火墙如何添加黑白名单？

ESET NOD32 安全套装的个人防火墙提供了可以对本机创建许可 web 站点的功能（即常说的白名单功能），要创建网页黑白名单，可以根据下列步骤操作：

添加许可站点：


1. 通过双击 windows 公告栏的  图标或者单击 开始 → 程序 → ESET → ESET Smart Security 打开 ESET NOD32 安全套装主界面
2. 按 CTRL + M 组合键切换到高级模式；
3. 单击 设置 → 个人防火墙，在右边界面 切换到交互过滤模式 → 配置规则和区域...



Fig. 1-1



Fig.1-2

4. 在 配置规则或区域窗口，点击切换到所有规则的详细视图，然后点击新建 按钮；

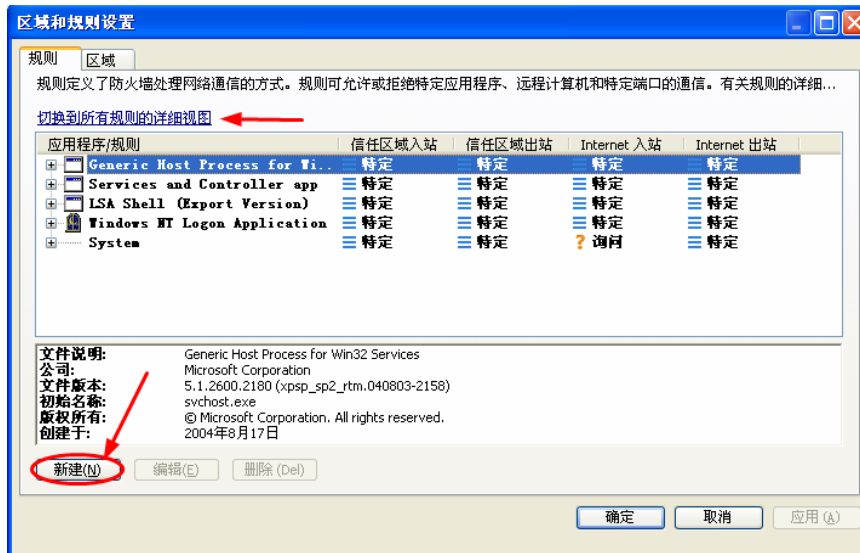


Fig. 1-3

5. 输入一个规则名称比如：许可站点，. 从 方向:下列菜单中选择出站 以及从操作下拉菜单中选择允许；

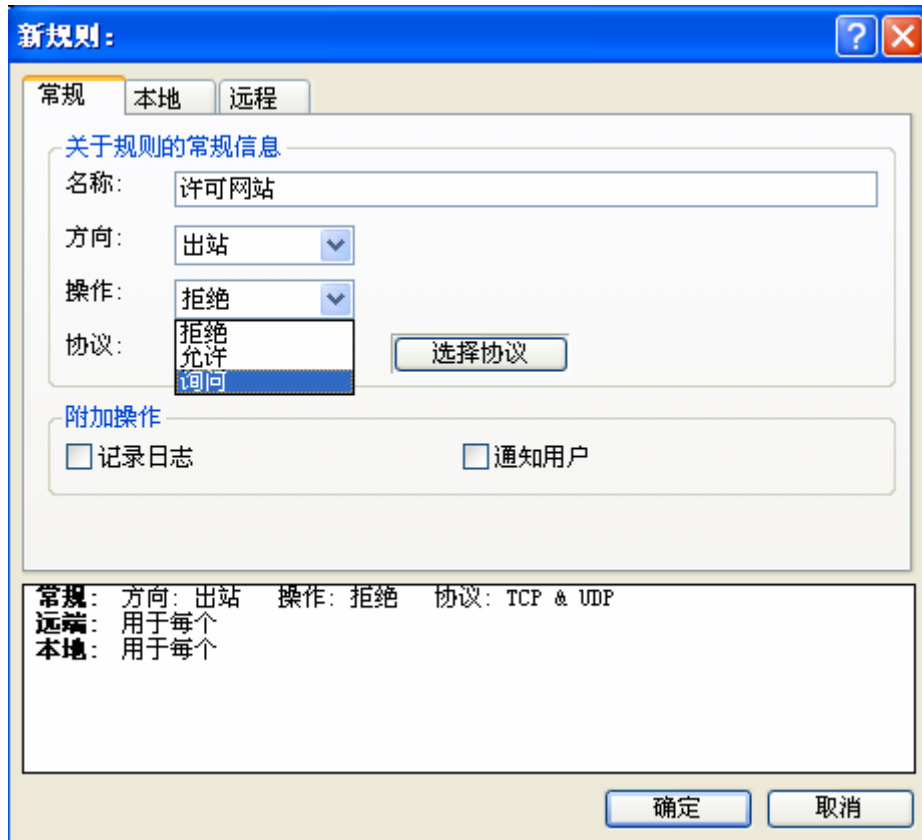


Fig. 1-3

6. 点击远程标签，并单击添加端口按钮，在添加端口窗口，通过名称下拉框选择 HTTP，然后点击确定，返回到新规则窗口；
7. 点击添加地址 按钮输入允许访问的网站地址，然后点击确定。如下图 Figure 1-4 : 图中的 IP 地址只是一个例子，完成 IP 地址添加后，点击 OK 返回到规则与区域窗口。

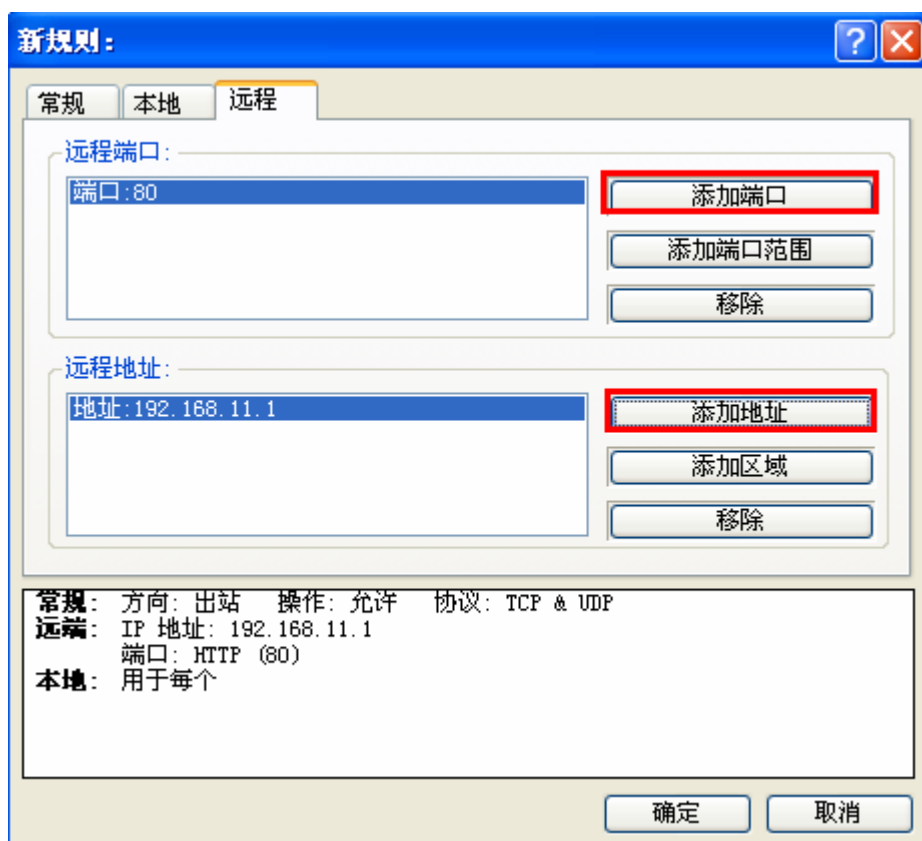


Fig. 1-4

阻止网站的出入站

如果要阻止某些网站的出入，则可以根据上面图 Fig.1-3 中，在**操作**下拉框中选择‘**拒绝**’即可。其他步骤同上。

安装完 ESET 安全套装后不能收发邮件

如果你在安装完 ESET NOD32 安全套装后，发现收发邮件困难甚至无法收发邮件，请先关闭 ESET NOD32 安全套装的防火墙后检查一下你的电脑与邮件服务器的连接，请参考以下步骤：


1. 通过双击 windows 公告栏的  图标或者单击 开始 → 程序 → ESET → ESET Smart Security 打开 ESET NOD32 安全套装主界面
2. 按 CTRL + M 组合键切换到高级模式；
3. 单击 设置 → 个人防火墙， 在右边界面 点击 ‘禁用’ ；



Fig. 1-1

个人防火墙关闭后，检查邮件是否能正常接收/发送。如果仍然没有解决，请卸载 ESET NOD32 安全套装再检查邮件的收发状态，如果问题依旧，请按下列步骤依次检查你的系统：

- Internet 网络连接正常；
- 通过网页方式进入邮箱，（比如：mail.163.com)能够正常收发邮件；
- Microsoft Outlook 或其他邮件客户端配置正确；
- 计算机没有安装其他防火墙。

修改个人防火墙设置

如果卸载 ESET NOD32 安全套装后或者禁用防火墙之后，能够解决邮件不能收发的问题，那么我们就需要调整个人防火墙的规则或者把规则置为默认值。请参照以下步骤：

1. 打开 ESET NOD32 安全套装主界面；
2. 在高级模式下，点击**设置** → **个人防火墙**，然后在右边界面的下方，找到**高级防火墙设置...用鼠标单击**(如下图 Fig. 1-2)。



Fig. 1-2

3. 从**过滤模式**的下拉框中选择**交互模式**；
4. 在左边目录树的**个人防火墙**下面选择**规则和区域**；
5. 在**区域和规则编辑器**界面，点击**设置按钮**(如下图 Fig. 1-4).



Fig. 1-3

6. 在区域和规则配置区域界面，在规则标签窗口中，使用编辑和删除按钮来进行规则的修改。(如图 Fig. 1-4).



Fig. 1-4

关于个人防火墙规则的更多设置,可参考 ESET NOD32 安全套装本身自带的帮助文档。如果修改规则后还是不能解决邮件收发问题,那么可以尝试将防火墙的配置还原到默认状态,具体步骤如下:

1. 在 ESET NOD32 安全套装的高级设置界面,在左边的目录树中选择**个人防火墙**后,点击右侧页面下方的**‘默认’**按钮;
2. 在弹出的默认设置对话框中,选择**只将“个人防火墙”设置恢复为默认(R)**,然后点击**是**,再点击确定返回到 ESET NOD32 安全套装主界面。

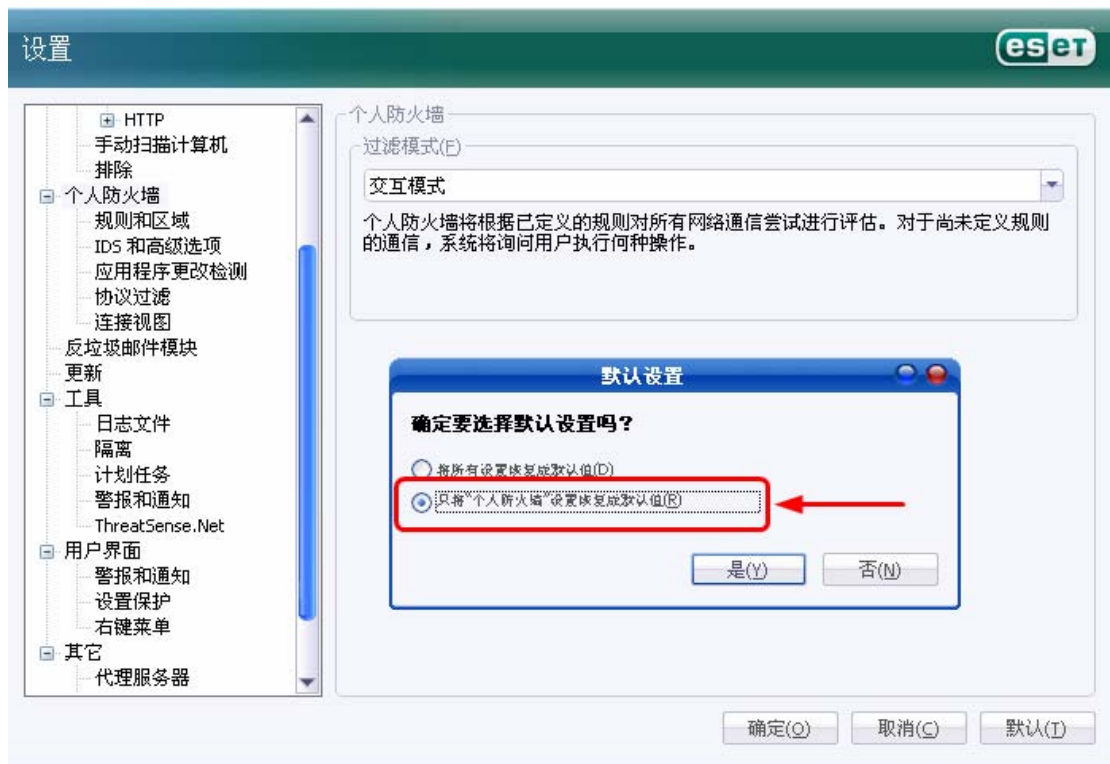



Fig. 1-5

安装完 ESET 安全套装后，局域网或网络共享无法正常运行？

如果您在安装完 ESET NOD32 安全套装后，局域网或者外部网络设备不能正常运行时（比如：网络共享文件夹无法访问等），这时您需要更改个人防火墙的过滤模式。ESET NOD32 安全套装个人防火墙的过滤模式。请参照以下步骤操作：

1. 通过双击 windows 公告栏的  图标或者单击 开始 → 程序 → ESET → ESET Smart Security 打开 ESET NOD32 安全套装主界面，按 **F5** 快捷键进入高级设置界面；
2. 从高级设置左边的目录树中，找到**个人防火墙**，并选中，在右边的过滤模式下拉框中，选择‘交互模式’，如下图：

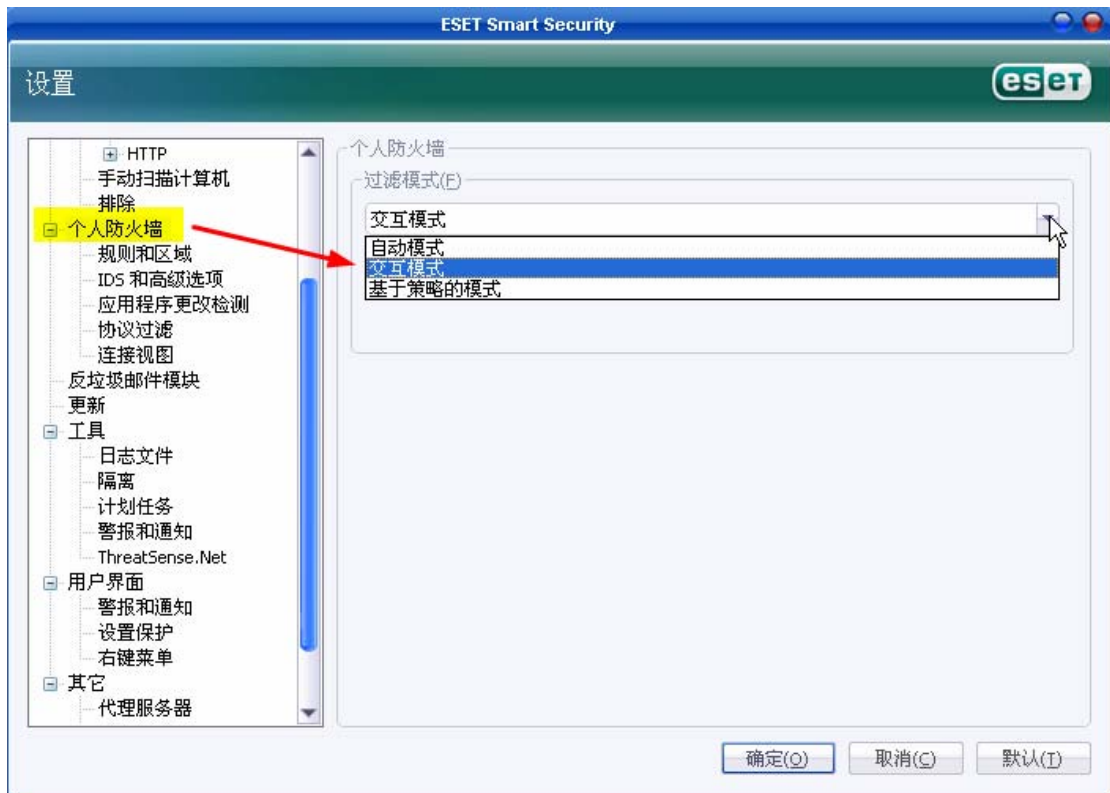


Fig. 1-1

3. 在左边目录树，展开**个人防火墙**→**规则和区域**，在**信任区域**点击**设置...**按钮，然后选择**允许共享**后点击确定。

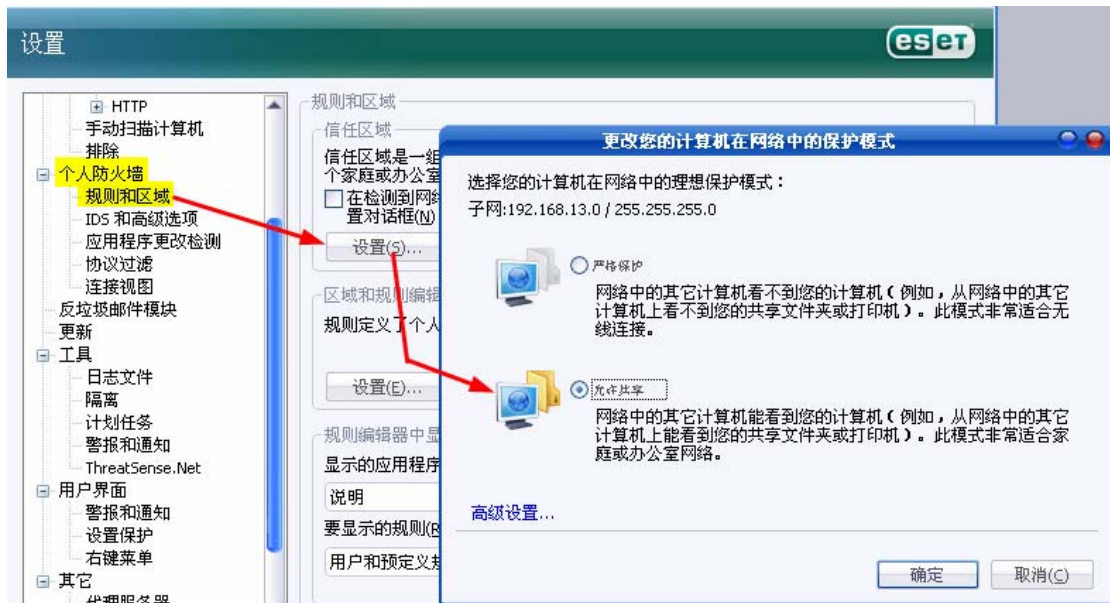
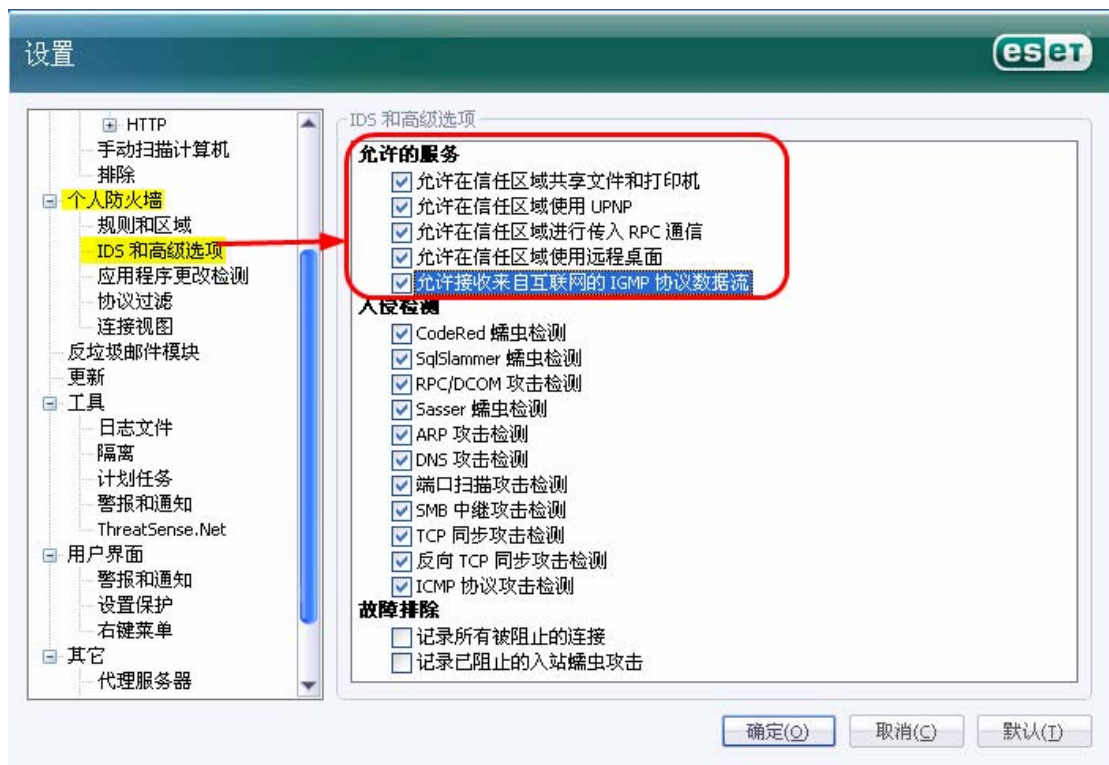


Fig. 1-2

4. 点击个人防火墙 → IDS 和高级选项，在允许的服务区域，确保所有的服务都被勾选。



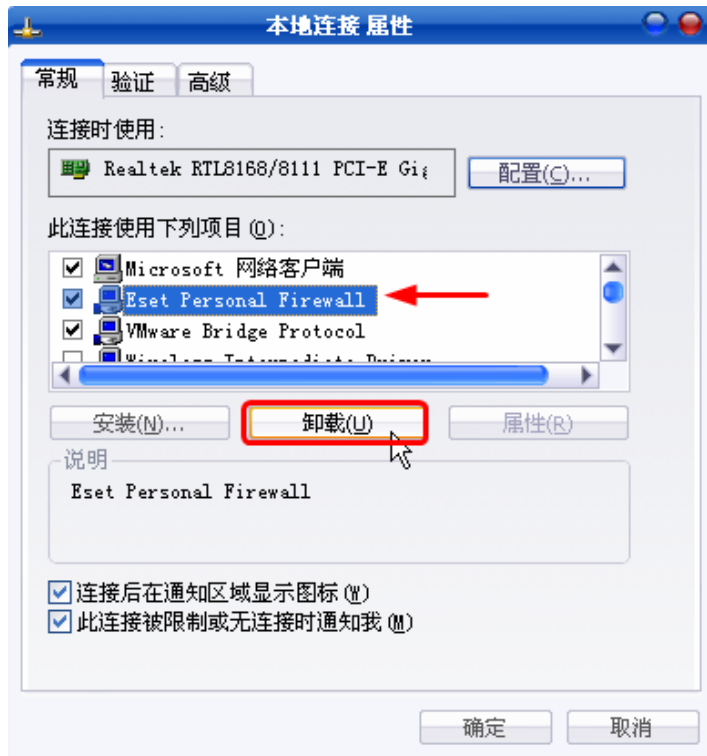
如何解决"ESET 个人防火墙初始化失败"?

当安装完 ESET NOD32 安全套装启动时，提示“ESET 个人防火墙初始化失败”的信息，那么导致这个错误提示的原因是因为 ESET NOD32 安全套装安装不正确或不完全。要修复这个错误，先需要使用 windows 清理工具来卸载 ESET NOD32 安全套装，并重新安装 ESET NOD32 安全套装。请参照以下步骤准备：

1. 从微软网站 <http://support.microsoft.com/kb/290301> 下载 windows 清理工具，或者通过 google、百度网站搜索并下载该工具；
2. 运行 windows 清理工具卸载计算机中的 ESET NOD32 安全套装；
3. 从 ESET 官方网站重新下载 ESET NOD32 安全套装安装程序（建议下载时不要使用下载工具）；

确保 ESET NOD32 安全套装的个人防火墙服务在本地连接中已经被删除：

1. 鼠标右键桌面的**网上邻居**，选择**属性**，在出现的窗口中右键**本地连接**，选择属性；或者通过**开始→设置→控制面板→网络连接**，双击打开。
2. 选择 **Eset Personal Firewall** 然后点击**卸载**；



3. 卸载完成后，重起电脑，然后重新安装 ESET NOD32 安全套装。

为什么安装 ESET 安全套装防火墙后，应用程序无法运行？

If a third party application on your computer is not working properly when the ESET Smart Security Personal firewall is in Automatic mode, or if an application works only while in Interactive mode, please review the information below.

Rules created in Interactive mode do not apply in Automatic mode. Automatic filtering mode (default mode) allows:

-all outgoing communication

-all incoming communications which were initiated by an application already communicating outwards.

Automatic mode may not be suitable for use with applications (e.g., Bit Torrent) which initiate multiple outgoing connections (only one is allowed), or applications which rely on non-initiated incoming communication.

If Automatic mode is preventing an application from working properly, you can switch the Personal firewall to Policy-based mode and enable two pre-defined rules which simulate the behavior of Automatic mode. Please see the steps below for detailed instructions:

1. From the ESET Smart Security main program window, press the F5 key. The Advanced Setup window will appear.
2. Click **Personal firewall** from the setup tree on the left. Select **Policy-based mode** from the **Filtering mode** drop-down menu and click **OK**.

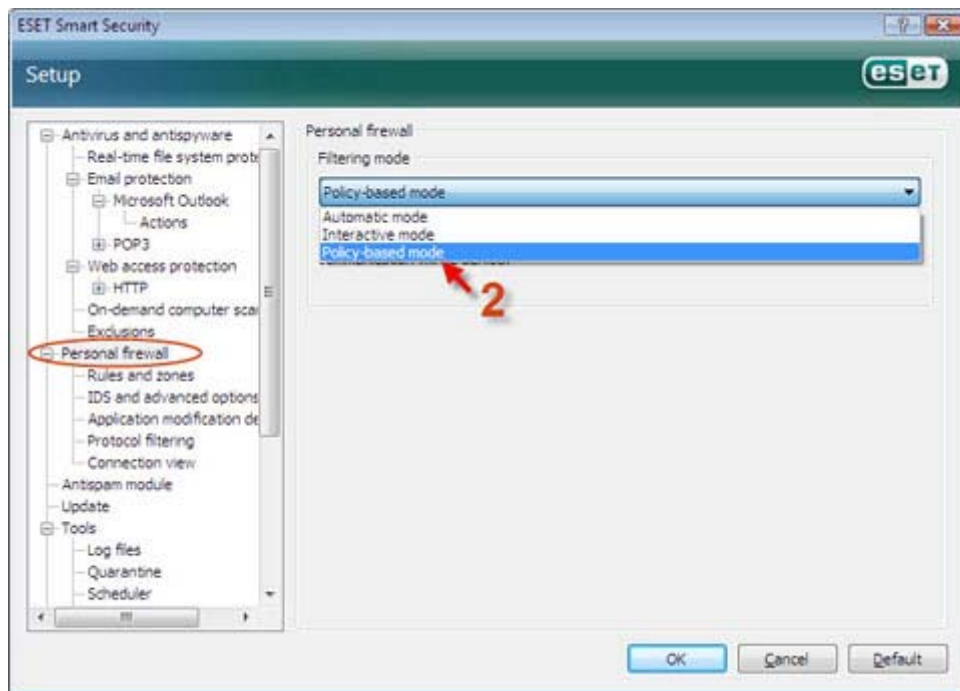


Fig. 1-1

3. Press the F5 key to display the Advanced Setup window. From the setup tree, click **Rules and zones**, and then click the **Setup...** button in the **Zone and rule editor** section.

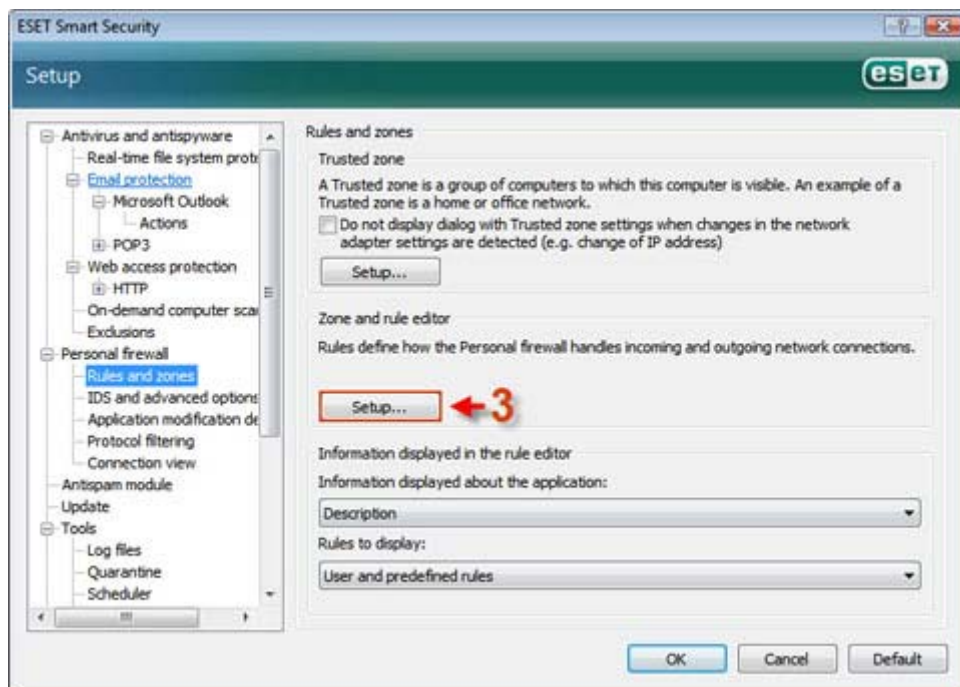


Fig. 1-2

4. Select the **Allow all outbound traffic** and **Allow initiated inbound traffic** check boxes and then click **OK** twice to return to the main program window. (Click **Toggle application tree view** if you don't see individual firewall rules as shown in Fig. 1-3).

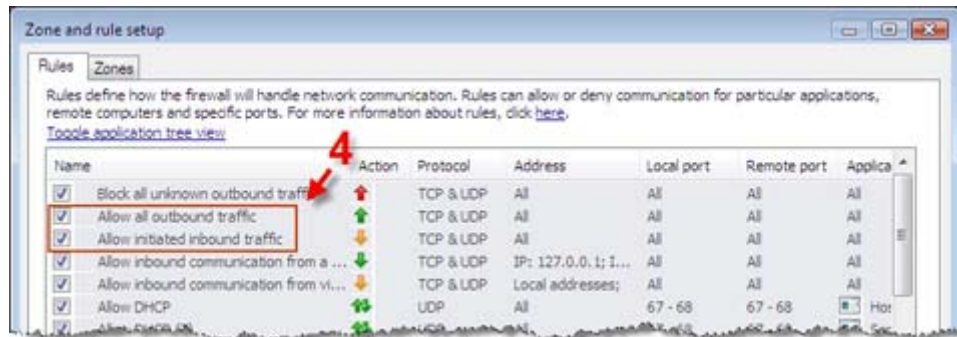


Fig. 1-3

The Personal firewall will now function as it would in Automatic mode, while still allowing you to define specific exceptions (rules) for problematic applications.

在防火墙里解决网络连接堵塞的问题

In some instances, you may need to enable a special logging mode to help troubleshoot problems with blocked connections in the Personal firewall module, such as conflicts with other NDIS filtering device drivers. This mode allows the Personal firewall to log additional information about the computer's network connection(s) which can be used by ESET's support specialists to help resolve issues.

The Personal firewall special logging mode should only be used if:

- No entries are written to **Tools** → **Log files** → **ESET Personal firewall log** when the **Personal firewall** → **IDS and advanced options** → **Log all blocked connections** option is enabled in the Advanced Setup window.
- Problems continue to occur after the Personal firewall module has been disabled.

Follow the steps below to activate special logging:

1. Click **Start** → **Run**. The **Run** window will be displayed. Type **regedit** and click **OK** (Windows Vista users: Click **Start**, type **regedit** and press ENTER)
2. Navigate to the following key: HKLM/SOFTWARE/Eset/ESET Security/CurrentVersion/Plugins 01000200/Profiles/@My profile
3. Create a new DWORD value titled **WriteBlockedToPcap** and set its value to 1. Restart your computer.
4. All blocked packets will now be saved to C:/Document and Settings/All Users/Application Data/Eset/Eset Smart Security/EpfwLog.pcap
5. Replicate the problematic situation.
6. Disable special logging (set the **WriteBlockedToPcap** value to 0 and restart your computer).
7. Send the file EpfwLog.pcap file (and all other files in the same folder beginning with 'Epwf') for analysis to ESET's support specialists. The contact email address is support@eset.com

NOTE: Please replicate the problem as soon as possible after step 3 and then disable special logging mode (step 6). This will prevent the logging of extraneous or misleading network communications. However, simulating the problem several times in a row before disabling debug mode will provide additional relevant data for analysis.