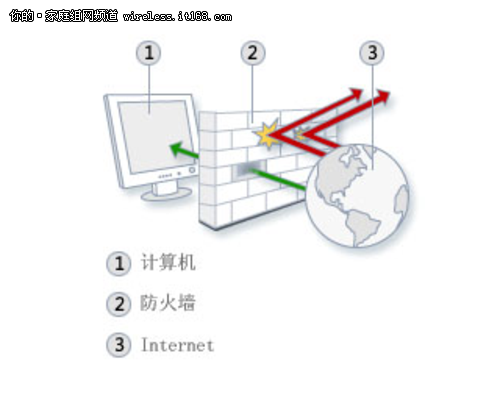
**网络安全巧设置 Win2008 R2 防火墙详解**

参考：<http://safe.it168.com/a2012/0503/1344/000001344554.shtml>

【IT168 技术】针对一般中小型企业来说，如果希望对企业网络进行安全管理，不一定非得花高价钱购买专业的防火墙设置，直接借助操作系统本身自带的防火墙功能即可以满足一般企业的应用，今天我们就一起来探究一下Windows Server 2008 R2系统防火墙的强大功能。熟练的应用Windows 内置防火墙，首先需要了解网络位置。



**网络位置**

　　第一次连接到网络时，必须选择网络位置（家庭组、工作组；专有网络和公共网络）。这将为所连接网络的类型自动设置适当的防火墙和安全设置。如果用户在不同的位置(例如，家庭、本地咖啡店或办公室)连接到网络，则选择一个网络位置可帮助确保始终将用户的计算机设置为适当的安全级别。

　　在Windows Server 2008中，有四种网络位置：

　　家庭网络：

　　对于家庭网络或在用户认识并信任网络上的个人和设备时，请选择“家庭网络”。家庭网络中的计算机可以属于某个家庭组。对于家庭网络，“网络发现”处于启用状态，它允许用户查看网络上的其他计算机和设备并允许其他网络用户查看用户的计算机。

　　工作网络：

　　对于小型办公网络或其他工作区网络，请选择“工作网络”。默认情况下，“网络发现”处于启用状态，它允许用户查看网络上的其他计算机和设备并允许其他网络用户查看用户的计算机，但是，用户无法创建或加入家庭组。

　　公用网络：

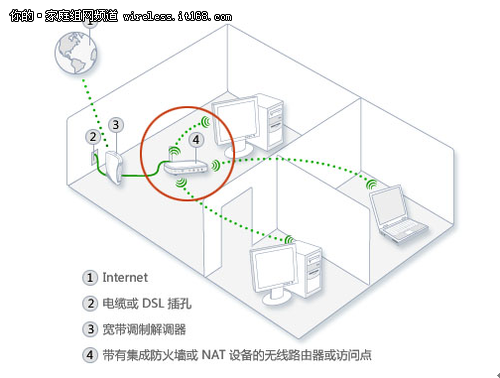
　　为公共场所(例如，咖啡店或机场)中的网络选择“公用网络”。此位置旨在使用户的计算机对周围的计算机不可见，并且帮助保护计算机免受来自 Internet 的任何恶意软件的攻击。家庭组在公用网络中不可用，并且网络发现也是禁用的。如果用户没有使用路由器直接连接到 Internet，或者具有移动宽带连接，也应该选择此选项。

　　域网络：

　　“域”网络位置用于域网络(如在企业工作区的网络)。这种类型的网络位置由网络管理员控制，因此无法选择或更改。

**Windows 防火墙如何影响网络位置**

　　在公共场所连接网络时，“公用网络”位置会阻止某些程序和服务运行，这样有助于保护计算机免受未经授权的访问。如果连接到“公用网络”并且 Windows 防火墙处于打开状态，则某些程序或服务可能会要求用户允许它们通过防火墙进行通信，以便让这些程序或服务可以正常工作。



　　在用户允许某个程序通过防火墙进行通信后，对于具有的位置与当前所连接到的位置相同的每个网络，也会允许该程序进行通信。例如，如果用户在咖啡店连接到某个网络并选择“公用网络”作为位置，然后解除了对一个即时消息程序的阻止，则对于所连接到的所有公用网络，对该程序的阻止都将解除。

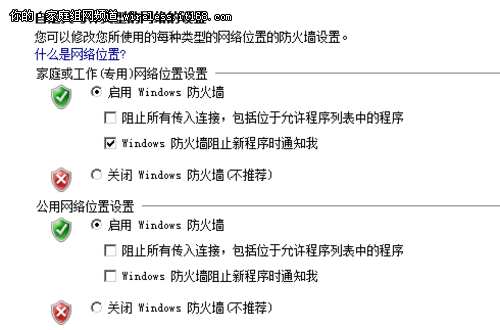
　　如果在连接到公用网络时计划解除对多个程序的阻止，请考虑将网络位置更改为“家庭”网络或“工作”网络。从这点而言，相对于影响用户所连接到的每个公用网络，这一更改操作可能会更安全。但请记住，如果进行了此更改，用户的计算机将对网络上的其他人可见，这样存在安全风险。

**Windows防火域基本设置**

　　当我们安装好系统后，默认就已经启用了防火墙功能，此时，只要设置好网络位置，就会阻止其他计算机与此计算机的通信。查看防火墙工作状态的方法是，在控制面板中点击系统和安全，从中打开Windows防火墙即可，然后就可以看到下图所示的状态：



　　如果希望打开或关闭Windows防火墙的话，只需要点击左侧的“打开或关闭防火墙”即可，然后看到如下图所示的界面：



　　从此图可以看到针对专用网中的家庭网络和工作网络已经开启了防火墙功能，此时就会封锁所有的传入连接。

　　但在实际应用中，不能把所有的传入连接都给封锁，在此用户可以根据需要设置相应的“白名单”来放开某些连接，方法是点击防火墙工作状态界面左侧中的“允许程序或功能通过Windows防火墙”，出现下图所示的界面：



　　将某个程序添加到防火墙中允许的程序列表或打开一个防火墙端口时，则允许特定程序通过防火墙与您的计算机之间发送或接收信息。允许程序通过防火墙进行通信(有时称为“解除阻止”)就像是在防火墙中打开了一个孔。

　　每次打开一个端口或允许某个程序通过防火墙进行通信时，计算机的安全性也在随之降低。您的防火墙拥有允许的程序或打开的端口越多，黑客或恶意软件使用这些通道传播蠕虫、访问文件或使用计算机将恶意软件传播到其他计算机的机会也就越大。

**防火墙的高级安全设置**

　　刚才的基本设置操作比较简单，但功能也单一，如果需要进一步设置Windows 防火墙规则，就需要通过“高级安全Windows 防火墙”功能。打开方法如下：管理工具中点击高级安全Windows防火墙，或者是在刚才的防火墙状态中点击高级设置。如下图所示，然后，可以看到右侧所示的界面。



　　什么是高级安全Windows防火墙：

　　使用高级安全 Windows 防火墙可以帮助用户保护网络上的计算机。通过该防火墙您可以确定允许在计算机和网络之间传输的网络流量。它还包括使用 Internet 协议安全性 (IPsec) 保护在网络间传送的流量的连接安全规则。

　　高级安全 Windows 防火墙是一种有状态的防火墙，它检查并筛选 IP 版本 4 (IPv4) 和 IP 版本 6 (IPv6) 流量的所有数据包。在此上下文中，筛选意味着通过管理员定义的规则对网络流量进行处理，进而允许或阻止网络流量。默认情况下阻止传入流量，除非是对主机请求(请求的流量)的响应，或者得到特别允许(即创建了允许该流量的防火墙规则)。可以通过指定端口号、应用程序名称、服务名称或其他标准将高级安全 Windows 防火墙配置为显式允许流量。

　　创建防火墙规则：

　　可以创建防火墙规则以允许此计算机向程序、系统服务、计算机或用户发送流量，或者从程序、系统服务、计算机或用户接收流量。当用户的连接匹配该规则标准的所有连接执行以下三个操作之一：允许连接、只允许通过使用 Internet 协议安全 (IPSec) 保护的连接、阻止连接。

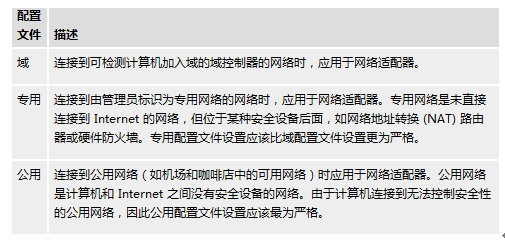
　　可以为入站通信或出站通信创建规则。可配置规则以指定计算机或用户、程序、服务或者端口和协议。可以指定要应用规则的网络适配器类型：局域网 (LAN)、无线、远程访问，例如虚拟专用网络 (VPN) 连接或者所有类型。还可以将规则配置为使用任意配置文件或仅使用指定配置文件时应用，当 IT 环境更改时，可能必须更改、创建、禁用或删除规则。

　　连接安全的实现：

　　连接安全包括在两台计算机开始通信之前对它们进行身份验证，并确保在两台计算机之间发送的信息的安全性。高级安全 Windows 防火墙使用 Internet 协议安全 (IPsec) 实现连接安全，方法是使用密钥交换、身份验证、数据完整性和数据加密(可选)。连接安全规则使用 IPsec 确保其通过网络时的流量安全。使用连接安全规则指定必须对两台计算机之间的连接进行身份验证或加密。可能还要必须创建防火墙规则以允许由连接安全规则保护的网络流量。

　　什么是防火墙配置文件：

　　防火墙配置文件是一种分组设置的方法，如防火墙规则和连接安全规则，根据计算机连接到的位置将其应用于该计算机。在运行此版本 Windows 的计算机上，高级安全 Windows 防火墙有三个配置文件：



　　每个网络适配器也就是网卡，分配匹配所检测网络类型的防火墙配置文件。例如，如果将网络适配器连接到公用网络，则到达或来自该网络的所有流量会由与公用配置文件关联的防火墙规则筛选。

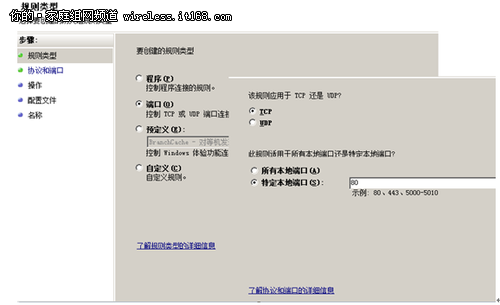
　　Windows Server 2008 R2 和 Windows 7 为每个活动网络适配器配置文件提供支持。在 Windows Vista 和 Windows Server 2008 中，每次计算机上只能有一个配置文件处于活动状态。如果存在多个连接到不同网络的网络适配器，则具有最严格配置文件设置的配置文件应用于计算机上的所有适配器。公用配置文件被认为是最为严格的，然后是专用配置文件;域配置文件被认为是最不严格的。

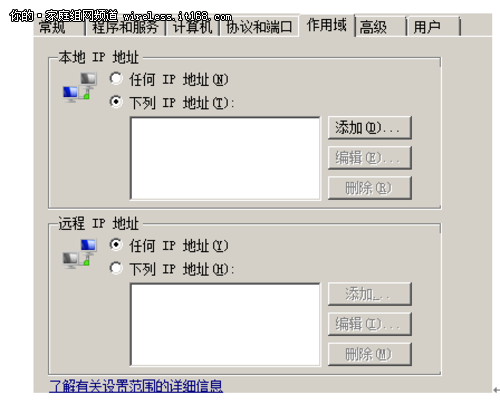
　　如果不更改配置文件的设置，则只要高级安全 Windows 防火墙使用配置文件，就应用其默认值。建议为所有三个配置文件启用高级安全 Windows 防火墙。

　　若要配置这些配置文件，请在高级安全 Windows 防火墙 MMC 管理单元中，右键单击“高级安全 Windows 防火墙”，然后单击“属性”。



　　如果需要使用的服务或应用程序在列表中没有出现的，用户可以通过新建规则的方式来创建，如现在操作的计算机是一台WEB服务器，而需要开放给其他用户连接此网站，可以通过新建规划来开放一个80端口的规则。





　　本地 IP 地址由本地计算机用于确定规则是否适用。规则仅适用于通过配置为使用一个指定本地 IP 地址的网络适配器的网络流量。任何 IP 地址，选择此选项可以指定匹配具有指定为本地 IP 地址的任意地址的网络数据包的规则。选中此选项时本地计算机始终匹配规则。下列 IP 地址，选择此选项可以指定规则匹配具有“本地 IP 地址”中指定的一个地址的网络流量。如果本地计算机没有使用一个指定 IP 地址配置的网络适配器，则规则不适用。在“IP 地址”对话框上，单击“添加”可以在列表中创建新条目，或单击“编辑”可以更改列表中的现有条目。还可以通过选择项目然后单击“删除”从列表中删除某个条目。

　　远程 IP 地址：指定应用规则的远程 IP 地址。如果目标 IP 地址是列表中的地址之一，则网络流量匹配规则。任何 IP 地址，此选项可以指定规则匹配发自(对于入站规则)或发往(对于出站规则)包含在列表中的任意 IP 地址的网络数据包。下列 IP 地址，选择此选项可以指定规则仅匹配具有“远程 IP 地址”中指定的一个地址的网络流量。在“IP 地址”对话

　　此外还需要将此防火墙规则应用到相应的配置文件和接口类型上，因此需要指定此规则所使用的配置文件，Windows 确定每个网络适配器的网络位置类型，然后对该网络适配器应用相应的配置文件。接口类型指的是单击“自定义”可以指定应用连接安全规则的接口类型。通过“自定义接口类型”对话框，可以选择“所有接口类型”或“局域网”、“远程访问”或“无线”类型的任意组合。最后一个需要介绍的就是边缘遍历。边缘遍历允许指的是计算机接受未经请求的入站数据包，这些数据包已通过诸如网络地址转换 (NAT) 路由器或防火墙之类的边缘设备。系统默认是阻止应用程序通过 NAT 边缘设备从 Internet 接收主动提供的流量。也可以设置为遵从用户或者是遵从应用程序，所谓遵从用户指的是让用户决定当应用程序请求通过 NAT 边缘设备从 Internet 接收主动提供的流量时是否允许该流量。遵从应用程序指的是让每个应用程序确定是否允许通过 NAT 边缘设备从 Internet 接收主动提供的流量。