

## 本文目录

- [什么是网络防火墙？](#)
- [什么是防火墙？它是如何确保网络安全的？](#)
- [什么是网络纵向防火墙？](#)
- [为什么其他国家不建防火墙？](#)
- [怎样关闭无线网络连接的防火墙？](#)
- [什么是防火墙，以及为什么要使用它的原因？](#)
- [怎么连接有防火墙的wifi？](#)
- [计算机防火墙是指？](#)

## 什么是网络防火墙？

网络防火墙是一种用来加强网络之间访问控制的特殊网络互联设备。计算机流入流出的所有网络通信均要经过此防火墙。

防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。

防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁木马。

最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

## 什么是防火墙？它是如何确保网络安全的？

防火墙，顾名思义，就是起到抵挡和防御外来侵犯的这样一个作用，相当于古时候的“盾牌”。大多数电脑用户都对电脑防火墙有一定的认识，但也只是一知半解，机友们都了解防火墙能够有效地保护我们电脑的安全，能够防止电脑黑客对于电脑的入侵，对于我们的电脑有着重要的保护作用，但是对于它的具体作用许多朋友并不是很了解，今天小编就重点来给大家说说防火墙的作用吧。

电脑防火墙作用：

一、首先自然是撑起网路的保护伞。防火墙都会制定自己的规则，凡是符合规则的一律放行，不符合规则的一律禁止，当然这些规则可以由网路管理员来自己制定，但是某些防火墙或许只能使用内置规则。

二、接下来就是强化网络安全策略，本来网络安全问题是由各个安全软件独立处理

，而防火墙可以有效的把所有安全软件配置在防火墙上，以防火墙为中心统一调用。防火墙的集中安全管理更经济，更安全。

三、防火墙还能有效地记录Internet上的活动，如果访问经过防火墙的话，它就能一五一十的记录下来，形成日志供用户查看。当有可疑情况发生的时候，防火墙会自动的发出适当的警报，并且提供详细的信息供用户查询。通过这些信息，我们可以有效的掌握目前的网络是否安全，是否需要进一步的配置确保万无一失。

四、防火墙可以限制暴露用户点。防火墙可以把网络隔成一个个网段，每个网段之间是相互独立互不干扰的，当一个网段出现问题的时候不会波及其他的网段，这样可以有效的防止因为一个网段问题波及整个网络的安全。

五、防火墙还有一个重要的功能就是防止信息外泄，隐私应该是每个上网用户最关心的问题，现在正是隐私泄露的敏感时期，因此更受到用户的关心，而防火墙可以阻塞有关内部网络中的DNS信息，使本机的域名和IP地址不会被外界所了解，能有效的阻止信息外泄。

六、当然防火墙的作用不止于安全范围，它还支持具有Internet服务特性的企业内部网络技术体系VPN(虚拟专用网络)。很多防火墙都含有VPN功能

相信大家看了介绍之后对防火墙一定有了一个全新的更加准确的认识了。目前我们处在网络信息的时代，电脑作为一种传媒工具当然是必不可少的了，但是也有很多不法分子制造病毒来危害我们的电脑，防火墙作为一个“电脑卫士”当然是非常重要的了，在了解防火墙相关作用之后，我们就可以更好地利用防火墙来保护我们的电脑了

## 什么是网络纵向防火墙？

网络纵向防火墙是一种网络安全技术，它可以控制网络中的数据流量，以防止未经授权的访问和攻击。

它可以检查网络中的数据包，并基于设定的规则来决定是否允许数据包通过。

网络纵向防火墙可以检查数据包的源地址、目的地址、端口号、协议类型等信息，以确定是否允许数据包通过。

它还可以检查数据包中的内容，以确定是否存在恶意代码或攻击行为。

## 为什么其他国家不建防火墙？

世界每个国家都有网络防火墙；因为网络防火墙是一种用来加强网络之间访问控制的特殊网络互联设备。计算机流入流出的所有网络通信均要经过此防火墙。

防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁木马。最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

## 怎样关闭无线网络连接的防火墙？

防火墙分2种:1.系统自带防火墙2.和你安装的防火墙一的一种关闭方法是:右键我的电脑点控制面板选着安全中心选着防火墙选着关闭二的一种关闭方法是:关闭防火墙进程或者直接右下角防火墙图标点关闭,如果你不希望它在电脑启动时候自动运行你可以在启动项里把它关闭.开始运行msconfig选择防火墙程序把前面的勾去点就OK了.希望对你有帮助.

## 什么是防火墙，以及为什么要使用它的原因？

先声明这里讨论的是计算机网络系统的防火墙，并非建筑内部的防火设备。中文歧义太多了。。。。

### 【什么是防火墙】

防火墙是一种集成软硬件为一体的计算机网络设备，一般位置处于不同性质网络之间（例如计算机局域网与广域网之间），用于网络数据通信的信息过滤。举个例子，下面图中的防火墙处于园区互联网出口，一端连接局域网的汇聚交换机，另一端连接ISP运营商的路由器或BRAS等网络设备。它能够根据企业的安全策略控制(比如允许、拒绝、检测等)出入网络的信息流，本身具有较强的抗攻击能力。

简单说，防火墙就是一种提供信息安全服务，实现网络和信息安全的基础设施。

数据来源：H3C官网，H3C SecPath F10x0 防火墙介绍

关于防火墙的详细规格参数，性能，选购配置，应用指南等信息，可以参考下面官网的产品介绍，类似的产品大同小异。

[http://www.h3c.com/cn/Products\\_\\_Technology/Products/IP\\_Security/FW\\_VPN/F1000/F10x0/](http://www.h3c.com/cn/Products__Technology/Products/IP_Security/FW_VPN/F1000/F10x0/)

### 【防火墙的内部架构简介】

例如Palo Alto防火墙，是一种包过滤防火墙，内部硬件由CPU、RAM、NVRAM、FLASH、ROM和一些相应的端口通过内部总线相连而构成，固件采用CISCO PIX OS操作系统。行业中常用处理器有Broadcom，Fortinet，Intel，NXP等。

数据来源：<https://www.staffeldt.net/palo-alto-networks-firewall-hardware-internals/>

### 【为什么使用防火墙】

一般的认为，局域网由于封闭性，其安全系数比较高，是低风险的，可信的；而互联网就充满未知和风险，是不可信的。例如蠕虫、木马、钓鱼网站等各种攻击方式对局域内网的安全产生严重威胁，有必要利用利用防火墙作为局域网的唯一出口，对数据进行防范。

另外，新一代的防火墙功能强大，还具有应用层状态包过滤功能，（如FTP、HTTP、SMTP、RTSP及其它基于TCP/UDP协议的应用层协议）。其他的如验证，授权，审计，NAT和VPN等功能也具实用价值。

"

### 怎么连接有防火墙的wifi？

- 1、点击右下角的网络访问，点开【打开网络和共享中心】；
- 2、点击左下角的【Windows 防火墙】，进入设置页面后，点击【打开或关闭Windows 防火墙】；
- 3、选定关闭Windows 防火墙，点击确定，再次连接无线网络。

### 计算机防火墙是指？

计算机防火墙是一种是一种计算机硬件或者软件或者软硬件结合的访问控制技术，根据预定的安全规则控制传入和传出内部网（可信网络）的网络流量。

防火墙 位于内部网和外部网之间的屏障，它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。换句话说，如果不通过防火墙，公司内部的人就无法访问Internet，Internet上的人也无法和公司内部的人进行通信。

防火墙是系统的第一道防线，其作用是防止非法用户的进入。由于防火墙不能阻止所有入侵行为，所以使用入侵检测系统作为第二道防线。

分类：

防火墙一般分为三大类：包过滤，应用代理和状态检测。