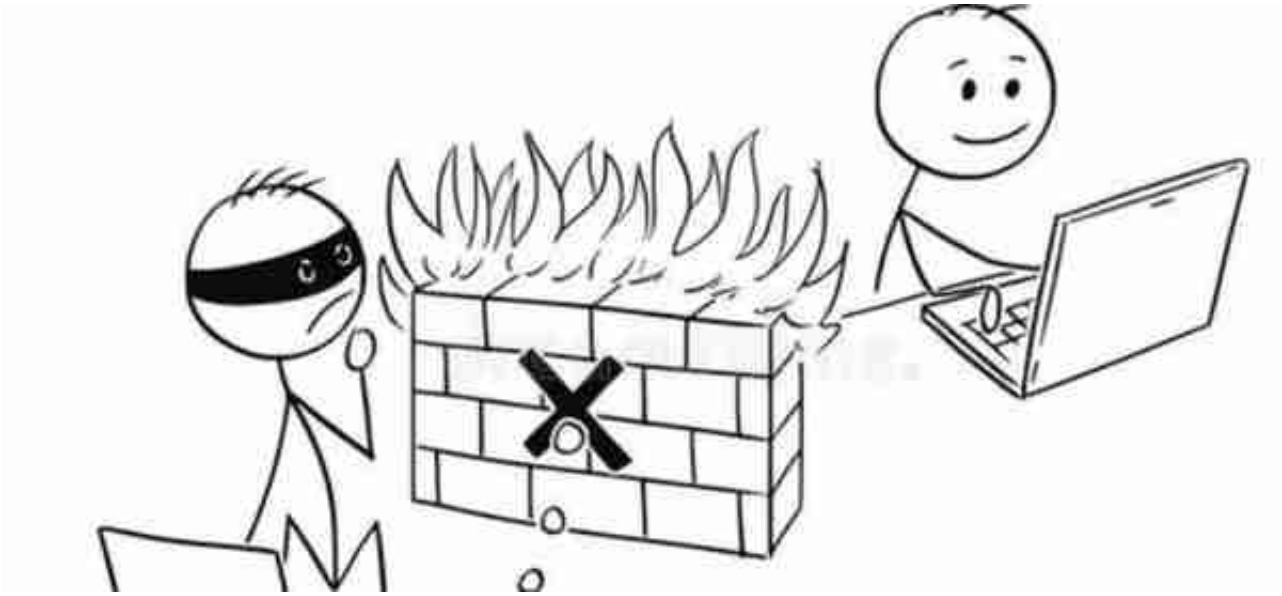
定义

所谓防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障.是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使Internet与Intranet之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关4个部分组成，防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件。该计算机流入流出的所有网络通信和数据包均要经过此防火墙。



应用层防火墙

应用层防火墙是在 TCP/IP
堆栈的“应用层”上运作，您使用浏览器时所产生的数据流或是使用 FTP 时的数据流都是属于这一层。应用层防火墙可以拦截进出某应用程序的所有封包，并且封锁其他的封包(通常是直接将封包丢弃)。理论上，这一类的防火墙可以完全阻绝外部的数据流进到受保护的机器里。

防火墙借由监测所有的封包并找出不符规则的内容，可以防范电脑蠕虫或是木马程序的快速蔓延。不过就实现而言，这个方法既烦且杂(软件有千千百百种啊)，所以大部分的防火墙都不会考虑以这种方法设计。

XML 防火墙是一种新型态的应用层防火墙。

根据侧重不同，可分为：包过滤型防火墙、应用层网关型防火墙、服务器型防火墙。

基本特性

（一）内部网络和外部网络之间的所有网络数据流都必须经过防火墙

这是防火墙所处网络位置特性，同时也是一个前提。因为只有当防火墙是内、外部网络之间通信的唯一通道，才可以全面、有效地保护企业网内部网络不受侵害。

根据美国国家安全局制定的《信息保障技术框架》，防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。所谓网络边界即是采用不同安全策略的两个网络连接处，比如用户网络和互联网之间连接、和其它业务往来单位的网络连接、用户内部网络不同部门之间的连接等。防火墙的目的就是在网络连接之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。

典型的防火墙体系网络结构如下图所示。从图中可以看出，防火墙的一端连接企事业单位内部的局域网，而另一端则连接着互联网。所有的内、外部网络之间的通信都要经过防火墙。

计算机信息攻击。混合媒体

发展史

第一代防火墙

第一代防火墙技术几乎与路由器同时出现，采用了包过滤（Packet filter）技术。下图表示了防火墙技术的简单发展历史。

第二、三代防火墙

1989年，贝尔实验室的Dave Presotto和Howard Trickey推出了第二代防火墙，即电路层防火墙，同时提出了第三代防火墙——应用层防火墙（代理防火墙）的初步结构。

第四代防火墙

1992年，USC信息科学院的BobBraden开发出了基于动态包过滤（Dynamic packet filter）技术的第四代防火墙，后来演变为目前所说的状态监视（Stateful inspection）技术。1994年，以色列的CheckPoint公司开发出了第一个采用这种技术的商业化的产品。

第五代防火墙

1998年，NAI公司推出了一种自适应代理（Adaptive proxy）技术，并在其产品Gauntlet Firewall for NT中得以实现，给代理类型的防火墙赋予了全新的意义，可以称之为第五代防火墙。

一体化安全网关UTM

UTM统一威胁管理，在防火墙基础上发展起来的，具备防火墙、IPS、防病毒、防垃圾邮件等综合功能的设备。由于同时开启多项功能会大大降低UTM的处理性能，因此主要用于对性能要求不高的中低端领域。在中低端领域，UTM已经出现了代替防火墙的趋势，因为在不开启附加功能的情况下，UTM本身就是一个防火墙，而附加功能又为用户的应用提供了更多选择。在高端应用领域，比如电信、金融等行业，仍然以专用的高性能防火墙、IPS为主流。

文章与图片皆来源于网络，仅供学习交流，希望对大家有帮助。

想要在程序员生涯内有更高的成就的话，最最重要的是尽可能的提升自己的编程能力，并且，与其想着怎么去提升，不如从现在开始动手动脑，如果对于C/C++感兴趣的话，可以关注+私信小编【C/C++编程】有一些视频希望可以帮助到你，学习不怕从零开始，就怕从不开始。