探讨防火墙维护与管理、技术发展趋势 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/287/2021_2022__E6_8E_A2_E8_AE_A8_E9_98_B2_E7_c97_287606.htm 本文从介绍防火墙的基本概念、分类以及特点入手，探讨防火墙维护与管理的方法、技术的发展趋势。 1、引言 网络安全是一个不容忽视的问题，当人们在享受网络带来的方便与快捷的同时，也要时时面对网络开放带来的数据安全方面的新挑战和新危险。为了保障网络安全，当园区网与外部网连接时，可以在中间加入一个或多个中介系统，防止非法入侵者通过网络进行攻击，非法访问，并提供数据可靠性、完整性以及保密性等方面的安全和审查控制，这些中间系统就是防火墙(Firewall)技术。它通过监测、限制、修改跨越防火墙的数据流，尽可能地对外屏蔽网络内部的结构、信息和运行情况、阻止外部网络中非法用户的攻击、访问以及阻挡病毒的入侵，以此来实现内部网络的安全运行。 2、防火墙的概述及其分类 网络安全的重要性越来越引起网民们的注意，大大小小的单位纷纷为自己的内部网络“ 筑墙 ”、防病毒与防黑客成为确保单位信息系统安全的基本手段。防火墙是目前最重要的一种网络防护设备，是处于不同网络(如可信任的局域内部网和不可信的公共网)或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的惟一出入口，能根据企业的安全策略控制(允许、拒绝、监测)出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。 2.1 概述 在逻辑上，防火墙其实是一个分析器，是一个分离器，同时也是一个限制器，它有效地

监控了内部网间或Internet之间的任何活动，保证了局域网内部的安全。 1)什么是防火墙 古时候，人们常在寓所之间砌起一道砖墙，一旦火灾发生，它能够防止火势蔓延到别的寓所。现在，如果一个网络接到了Internet上面，它的用户就可以访问外部世界并与之通信。但同时，外部世界也同样可以访问该网络并与之交互。为安全起见，可以在该网络和Internet之间插入一个中介系统，竖起一道安全屏障。这道屏障的作用是阻断来自外部通过网络对本网络的威胁和入侵，提供扼守本网络的安全和审计的关卡，它的作用与古时候的防火砖墙有类似之处，因此就把这个屏障叫做“ 防火墙 ”。 防火墙可以是硬件型的，所有数据都首先通过硬件芯片监测.也可以是软件型的，软件在计算机上运行并监控。其实硬件型也就是芯片里固化了UNIX系统软件，只是它不占用计算机CPU的处理时间，但价格非常高，对于个人用户来说软件型更加方便实在。 2)防火墙的功能 防火墙只是一个保护装置，它是一个或一组网络设备装置。它的目的就是保护内部网络的访问安全。它的主要任务是允许特别的连接通过，也可以阻止其它不允许的连接。其主体功能可以归纳为如下几点： 根据应用程序访问规则可对应用程序联网动作进行过滤. 对应用程序访问规则具有学习功能. 可实时监控，监视网络活动. 具有日志，以记录网络访问动作的详细信息. 被拦阻时能通过声音或闪烁图标给用户报警提示。 3)防火墙的使用 由于防火墙的目的是保护一个网络不受来自另一个网络的攻击。因此，防火墙通常使用在一个被认为是安全和可信的园区网与一个被认为是不安全与不可信的网络之间，阻止别人通过不安全与不可信的网络对本网络的攻击，破坏网络安全，限制非法用户

访问本网络，最大限度地减少损失。 2.2 防火墙的分类 市场上的硬件防火墙产品非常之多，分类的标准比较杂，从技术上通常将其分为“ 包过滤型 ”、“ 代理型 ”和“ 监测型 ”等类型。 1)包过滤型 包过滤型产品是防火墙的初级产品，其技术依据是网络中的分包传输技术。网络上的数据都是以“ 包 ”为单位进行传输的，数据被分割成为一定大小的数据包，每一个数据包中都会包含一些特定信息，如数据的源地址、目标地址、TCP/UDP(传输控制协议/用户数据报协议)源端口和目标端口等。防火墙通过读取数据包中的地址信息来判断这些“ 包 ”是否来自可信任的安全站点，一旦发现来自危险站点的数据包，防火墙便会将这些数据拒之门外。 2)代理型 代理型防火墙也可以被称为代理服务器，它的安全性要高于包过滤型产品，并已经开始向应用层发展。代理服务器位于客户机与服务器之间，完全阻挡了二者间的数据交流。从客户机来看，代理服务器相当于一台真正的服务器.而从服务器来看，代理服务器又是一台真正的客户机。当客户机需要使用服务器上的数据时，首先将数据请求发给代理服务器，代理服务器再根据这一请求向服务器索取数据，然后由代理服务器将数据传输给客户机。由于外部系统与内部服务器之间没有直接的数据通道，外部的恶意侵害也就很难伤害到企业内部网络系统。 3)监测型 监测型防火墙是新一代的产品，这一技术实际上已经超越了最初的防火墙定义。监测型防火墙能够对各层的数据进行主动的、实时的监测，在对这些数据加以分析的基础上，监测型防火墙能够有效地判断出各层中的非法侵入。同时，这种监测型防火墙产品一般还带有分布式探测器，这些探测器安置在各种应用服务器和其他网络的

节点之中，不仅能够检测来自网络外部的攻击，同时对来自内部的恶意破坏也有极强的防范作用。据权威机构统计，在针对网络系统的攻击中，有相当比例的攻击来自网络内部。因此，监测型防火墙不仅超越了传统防火墙的定义，而且在安全性上也超越了前两代产品。