电子商务安全技术：防火墙技术电子商务考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/582/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_582937.htm 一、防火墙的基本概念 防火墙（firewall）是网络安全的第一道屏障，保障网络安全的第一个措施往往是安装和应用防火墙。人们对防火墙的理解伴随着计算机技术的发展逐渐深入。防火墙最原始的含义是：设计一种建筑以防止发生火灾时，火势不至于从一个房间蔓延到另外一个房间。后来，这种称呼延伸到到计算机安全领域之中，特别是近年来飞速发展的Internet网络之中，所以，防火墙有时也被称为 Internet防火墙。 目前关于防火墙的定义有很多，其中最典型的是：防火墙是在两个网络之间强制实施访问控制策略的一个系统或一组系统。 从狭义上来讲，防火墙是指安装了防火墙软件的主机或路由器系统。防火墙被放在两个网络之间，并具有以下特性： ①所有的从内部到外部或从外部到内部的通信都必须经过它； ②只有有内部访问策略授权的通信才被允许通过； ③系统本身具有高可靠性。 简而言之，防火墙是保护可信网络，防止黑客通过非可信网络入侵的一种设备。这两种网络最典型的例子是企业内部网和Internet。 防火墙具有如下功能： ①过滤不安全的服务和非法用户。所有进出内部网络的信息都必须通过防火墙，防火墙成为一个检查点，禁止未授权的用户访问受保护的网络。 ②控制对特殊站点的访问。防火墙可以允许受保护网络中的一部分主机被外部网访问，而另一部分则被保护起来，例如：受保护网中的Mail、FTP、WWW服务器等可被外部网访问，而其他访问则被禁止。 ③作为网络安全的集中监视

点。防火墙可以记录所有通过它的访问，并提供统计数据，提供预警和审计等功能。 但防火墙也并非十全十美，不能说有了防火墙就可以万事大吉了，因为防火墙也有其不足之处，主要表现在：①防火墙不能防范不经由防火墙的攻击。例如：如果允许从受保护网内部不受限制地向外拨号，一些用户可以形成与Internet的直接的SLIP或PPP连接，从而绕过防火墙，造成一个潜在的后门攻击渠道。②防火墙不能防止受到病毒感染的软件或文件的传输。因为现有的各类病毒、加密和压缩的二进制文件种类太多，不能指望防火墙逐个扫描每个文件查找病毒。③防火墙不能防止数据驱动式攻击。当有些表面看来无害的数据被邮寄或复制到Internet主机上并被执行发起攻击时，就会发生数据驱动攻击。防火墙无法防止这类攻击。 二、防火墙的基本原理 自从第一个最简单的包过滤路由器防火墙问世以来，在防火墙产品系列中已经出现了应用各种不同技术的不同类型的防火墙。这些技术之间的区分并不是非常明显，但就其处理的对象来说，基本上可以分为包过滤型和应用网关型、代理服务型三大类：包过滤型防火墙、应用网关型防火墙和代理服务型防火墙。包过滤型防火墙的处理对象是IP包，其功能是处理通过网络的IP包的信息，实现进出网络的安全控制。应用网关型防火墙的处理对象是各种不同的应用服务，其功能是通过对网络服务的代理，检查进出网络的各种服务。因为网络通信是基于网络通信的层次参考模型来进行的，所以，不同类型的防火墙负责处理不同层次的通信数据。如IP包过滤型防火墙负责处理网络层数据，而应用代理型防火墙负责处理应用层数据。 （一）包过滤型防火墙 在遵守TCP/IP协议的网络中，数据是分解为不

同的IP包进行传输的。包过滤型防火墙是应用数据包过滤（packetfiltering）技术在网络层对数据包进行选择，截获每个通过防火墙的IP包，并进行安全检查。如果IP包能通过检查，就将该IP包正常转发出去，否则，就阻止该IP包通过。在这里，进行选择的依据是系统内设置的过滤逻辑，称为访问控制表（accesscontroltable）。包过滤防火墙通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，或它们的组合来确定是否允许该数据包通过。由于在Internet中，提供某些特定服务的服务器一般都使用相对固定的端口，因此，包过滤器只需控制端口就控制了服务。例如，TCP端口23通常提供Telnet服务，所以在包过滤器中只要控制了这个端口，就可以控制Telnet的服务。大多数防火墙都有IP包过滤的功能，其中最常见的是包过滤路由器。它是基于一定的规则来对IP包进行安全检查，这些规则可以归纳为以下几个方面：协议类型，源地址、目的地址，源端口，目的端口 其具体的实现原理是：①通过协议类型控制特定的协议；②通过 IP 地址控制特定的源和目的主机；③通过控制源和目的端口控制特定的网络服务；④通过源/目的控制入网信息和出网信息，即控制信息方向。更进一步，还可以通过制定IP地址和端口的组合规则，要求某些特定服务必须通过某一特定的IP地址进行细致的检查。由于包过滤型防火墙逻辑简单，价格便宜，易于安装和使用，网络性能和透明性好，所以通常安装在路由器上。路由器是内部网络与 Internet 连接必不可少的设备，因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用，适合安全性要求较低的小型电子商务系统。 但是，包过滤型防火墙也有其不足之处，主要

表现在：①为完成某一项特定任务，包过滤的规则可能比较复杂，且不易验证其正确性；②一般的包过滤路由器在审计功能方面显得较弱，因而安全性不足；③数据包的源地址、目的地址以及IP的端口号都在数据包的头部，很有可能被窃听或假冒，这样就会形成各种安全漏洞。（二）应用网关型防火墙 应用级网关（application levelgateways）是在网络应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时，对数据包进行必要的分析、登记和统计，形成报告。实际中的应用网关通常安装在专用工作站系统上。 包过滤型和应用网关型防火墙有一个共同的特点，就是它们仅仅依靠特定的逻辑来判定是否允许数据包通过。一旦满足逻辑，则防火墙内外的计算机系统就建立起直接联系，防火墙外部的用户便有可能直接了解防火墙内部的网络结构和运行状态，这就很有可能导致非法访问和攻击。（三）代理服务型防火墙 代理服务（proxyservice）又称链路级网关或TCP 通道，也有人将它归于应用级网关一类。代理服务型防火墙是针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，其特点是将所有跨越防火墙的网络通信链路分为两段。防火墙内外的计算机系统间应用层的“ 链接 ”，由两个终止代理服务器上的“ 链接 ”来实现，外部计算机的网络链路只能到达代理服务器，从而起到了隔离防火墙内外计算机系统的作用。此外，代理也对过往的数据包进行分析、注册登记、形成报告，同时当发现被攻击迹象向网络管理员发出警报，并保留攻击痕迹。在一个网络中，对于由内向外的请求和由外向内的请求所进行的处理同的。一般认为内部网络比较安全，所以需要

控制外部网络向内部网络的请求。这时，就由代理程序将外部用户对内部网络的服务请求依据已制定全规则决定是否向内部真实服务器提交。代理服务代替外部用户与内部网的服务器进行连接。所以代理服务类似于应用服务和用户之间的转发器。个远程用户请求内部服务时，它首先与这个代理相连，经过认证后，再由代到目的主机，同时将服务器的响应传送给所代理的客户。 在这个过程中，代理既是客户程序又担任服务器的角色。对于真正的请求来说，它是服务器；而对于服务器来说，它是一个客户请求进程。所以在代理的实现中必须既有服务器的部分，又有客户的程序部分。应用级网关和代理服务方式的防火墙大多是基于主机的，性能较好，但比较贵，且安装和使用也比包过滤型防火墙复杂。 三、防火墙的实现方式 由于整个网络的安全防护政策、防护措施及防护目的不同，防火墙的配实现方式也千差万别，下面是几种常见的防火墙实现方式： 1、包过滤路由器 包过滤路由器（screening router）是众多防火墙中最基本、最简单的一种，它可以是带有数据包过滤功能的商用路由器，也可以是基于主机的路由器。许多网络的防火墙就是在被保护网络和Internet网络之间安置包过滤路由器。它与下面谈到的过滤主机网关防火墙的不同点，在于它允许被保护网络的多台主机与 Internet网络的多台主机进行直接通信，其危险性分布在被保护网络的全部主机以及允许访问的各种服务类型上。随着服务的增多，网络的危险性将急剧增加。当网络被击破时，这种防火墙几乎无法保留攻击者的踪迹，甚至难以发现已发生的网络攻击。显然，这种常用的过滤路由防火墙是不安全的。它采取的安全政策属于“ 除了禁止不可的都被允许 ”这

种极端类型。 2、双穴防范网关 另一种经常使用且易于安装的防火墙叫做双穴防范网关（ dualhomed gate-way）。这种防火墙不使用包过滤规则，而是在被保护网络和 Internet网络之间设置一个系统网关，用来隔断 TCP/IP 的直接传输。被保护网络中的主机与该网关可以通信，Internet中的主机也能与该网关通信，但是两个网络中的主机不能直接通信。这种方式的防火墙的安全性取决于管理者允许提供的网络服务类型。 3、过滤主机网关 过滤主机网关（screened hostgateway）防火墙配置时需要一个带包过滤功能的路由器和一台设防主机。一般情况下，设防主机设置在被保护网络，路由器设置在设防主机和 Internet网络之间，这样设防主机是被保护网络惟一可到达 In-ternet网络的系统，通常情况下路由器封锁了设防主机特定的端口，而只允许一定数量的通信服务。一般而言，过滤主机网关防火墙是比较安全的，因为从 Internet网络只能访问到设防主机，而不允许访问被保护网络的其他资源，设防主机居于被保护网络，局域网中的用户与设防主机的可达性相当好，不涉及外部路由配置问题。然而，一旦攻击者登录到设防主机，危害性就变得相当大，整个被保护网络都可能是攻击的目标。 4、过滤子网防火墙 考虑到过滤主机网关防火墙的安全性，在配置防火墙时有必要在被保护网络和 Internet网络之间设置一个孤立的子网，这就是过滤子网（ screened subnet）防火墙。一般情况下，采用包过滤路由器防火墙来孤立这个子网。这样被保护网络和 Internet网络虽然都可以访问子网主机，但跨过子网的直接访问是被严格禁止的。通常，孤立子网需要设置一台设防主机，即用来提供交互式的终端会晤，同时也兼当应用级网关。过滤子网防火墙这

种配置的危害区域相对较小，只集中在设防主机和包过滤路由器上。这种方法使得经过防火墙的所有服务都必须经过应用网关，同时牵扯到网络间路由的重新选择，能够隐藏被保护网络可能遗留的痕迹，许多节点与 Internet网络的连接，都被现有网络的重新编址和子网的重新划分变得不可能。对于网间路由的过滤子网防火墙，当一个新的子网连入时，必须改变配置，以适应新的子网划分和新的网址分配，否则就不能正确地使用防火墙，因此增加了网络的安全性能。对攻击者而言，其必须连续重新设置三个网络的路由而不间断，才能侵入设防主机，进而进入被保护网络，最后再返回到包过滤路由器，而且所有这些都不能被锁住，也不被发现，这在理论上虽有可能，但实现起来无疑是相当困难的。因而过滤子网防火墙的安全性相对较高。除了上面提到的这些防火墙实现方式外，还有应用级网关、代理网关以及混合型网关等多种实现方式。F8F8" 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com