如何构建安全的企业防火墙？ PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/0/2021_2022__E5_A6_82_E4_BD_95_E6_9E_84_E5_c99_421.htm 如何构建一个安全的防火墙系统结构。 引子 防火墙是保障网络安全的关键组件，但它只是安全企业网络的一个开端而已。对管理员来讲，有必要关注支持失效转移的多防火墙设计。这种防火墙设计的最终结果应是易于管理、高性能、高可用性、高安全性的组合，而且还要少花钱。 要几个防火墙？ 在防火墙的设计原理上历来有不少争论，争论的一个主要问题是到底拥有几个防火墙是最好的。笔者以为两个防火墙一般不会比一个防火墙好多少。因为在大多数的攻击事件中，防火墙自身的漏洞很少成为问题。黑客们通常并不需要攻克防火墙，因为他们可以通过开放的端口进入，并利用防火墙之后的服务器上的漏洞。此外，防火墙本身并没有什么吸引黑客攻击的地方，因为任何明智的管理员都会将配置防火墙使其丢弃那些连接防火墙的企图。例如，即使在用户的防火墙上有一个已知的SSH漏洞，这种威胁也只能来自防火墙指定的受到良好保护的管理工作站，更别说这种工作站被关闭的情况了。事实上，防火墙的最大问题在于其维护上的薄弱、糟糕的策略及网络设计。在与防火墙有关的安全事件中，人的因素造成的破坏占到了大约99%的比例。更糟的是，如果你运行多个厂商的防火墙，那么其成本将迫使用户放弃一些需要特别关注的问题。用户最好将有限的资源花费在强化一种平台上，而不要全面出击。 防火墙的设计目标 一种良好的防火墙策略和网络设计应当能够减少（而不是根除）下面的这些安全风险： ◆来自

互联网的攻击DMZ服务的攻击 ◆企业网络的任一部分攻击互联网 ◆企业用户或服务器攻击DMZ服务器 ◆DMZ服务器攻击用户、服务器，或者损害自身。 ◆来自合伙人和外延网（extranet）的威胁 ◆来自通过WAN连接的远程部门的威胁 这些目标听起来也许有点太过头了，因为这基本上并不是传统的方法，不过它却其自身的道理。 第一点是非常明显的，那就是限制通过互联网试图访问DMZ服务器的服务端口，这就极大地减少了它们被攻克的机会。例如，在一个SMTP邮件服务器上，仅允许互联网的通信通过25号TCP端口。因此，如果这台SMTP服务器碰巧在其服务器服务或程序中有一个漏洞，它也不会被暴露在互联网上，蠕虫和黑客总在关心80号端口的漏洞。 下一条听起来可能有点儿古怪，我们为什么要关心通过自己的网络来保护公共网络呢？当然，任何公民都不应当散布恶意代码，这是起码的要求。但这样做也是为了更好地保护我们自己的的网络连接。以SQL slammer 蠕虫为例，如果我们部署了更好的防火墙策略，那么就可以防止对互联网的拒绝服务攻击，同时还节省了互联网资源。 最不好对付的是内部威胁。多数昂贵的防火墙并不能借助传统的设计来防止网络免受内部攻击者的危害。如一个恶意用户在家里或其它地方将一台感染恶意代码的笔记本电脑挂接到网络上所造成的后果可想而知。一个良好的网络设计和防火墙策略应当能够保护DMZ服务器，使其免受服务器和用户所带来的风险，就如同防御来自互联网的风险一样。 事情还有另外一方面。因为DMZ服务器暴露在公共的互联网上，这就存在着它被黑客或蠕虫破坏的可能。管理员采取措施限制DMZ服务器可能对内部服务器或用户工作站所造成的威胁是至关重要

的。此外，一套稳健的防火墙策略还可以防止DMZ服务器进一步损害自身。如果一台服务器被黑客通过某种已知或未知的漏洞给破坏了，他们做的第一件事情就是使服务器下载一个rootkit.防火墙策略应当防止下载这种东西。 还可以进一步减少来自外延网（Extranet）合伙人及远程办公部门WAN的威胁。连接这些网络的路由器使用了广域网技术，如帧中继、VPN隧道、租用私有线路等来保障，这些路由器也可以由防火墙来保障其安全。利用每一台路由器上的防火墙特性来实施安全性太过于昂贵，这样不但造成硬件成本高，更主要的是其设置和管理上难度也很大。企业的防火墙借助于超过传统防火墙的附加功能可以提供简单而集中化的广域网和外延网的安全管理。 关键在于防火墙能够限制不同网络区域的通信，这些区域是根据逻辑组织和功能目的划分的。但防火墙不能限制并保护主机免受同一子网内的其它主机的威胁，因为数据绝对不会通过防火墙接受检查。这也就是为什么防火墙支持的区域越多，它在一个设计科学的企业网络中也就越有用。由于一些主要的厂商都支持接口的汇聚，所以区域划分实现起来也就简单多了。单独一个千兆比特的端口可以轻松地支持多个区域，并且比几个快速以太网端口的执行速度更快。 实施一套良好的防火墙策略 安全防火墙架构的首要关键组件是策略的设计。实现这些目标的最为重要的概念是使用原则的需要。在防火墙的策略中，这只是意味着除非有一个明确的原因要求使用某种服务，这种服务默认地必须被阻止或拒绝。为实施默认的服务阻止规则，在所有策略集的末尾只需要全局性地实施一种防火墙策略，即丢弃一切的规则，意思就是防火墙的默认行为是丢弃来自任何源到达任何

目的地的任何服务的数据包。这条规则在任何的防火墙策略中是最后一条规则，因为在某种通信在有机会进入之前，它已经被封杀了。一旦实施了这种基本的行为，就需要对特定的源、特定的服务、对特定的目标地址的访问等实施在一些精心设计的规则。一般而言，这些规则越精密，网络也就越安全。 例如，用户可被准许使用对外的一些常见服务端口，如HTTP，FTP，媒体服务等，但其它的服务和程序除非有了明确的原因才准许通信。在根据企业的需要找到一种特别的原因后，就需要在验证和核准后增加一些严格控制的针对性规则。管理员们常犯的一个错误是他们将用户的权限扩展到了服务和DMZ网络。适用于用户的向外转发数据的规则通常并不适用于服务器。在认真考虑之后，管理员会找到Web服务器并不需要浏览Web的理由。服务器就是服务器，它主要是提供服务，而很少成为客户端。一个根本的问题是DMZ或服务器几乎不应当首先发起通信。服务器典型情况下会接受请求，但几乎不可能接受来自公共的互联网的请求服务，除非是企业合伙人的XML及EDI应用。其它的例外还有一些，如提供驱动程序和软件更新的合法厂商的站点，但所有的例外，都应当严格而精密地定义。遵循这些严格的标准可以极大地减少服务器被损害的可能，最好能达到这样一种程度，只要部署了这种策略，即使服务器没有打补丁，也能防止内部子网的蠕虫传播。 编辑特别推荐: #0000ff>全面解析Web应用防火墙 #0000ff>关于防火墙必须知道的几点 #0000ff>详细配置CiscoPIX防火墙 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