使用Web交换机提高网络安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/284/2021_2022__E4_BD_BF_E7_94_A8Web_E4_c101_284833.htm 尽管防火墙在防止网络入侵方面具有很高的效率，并已成为提交安全Web站点和服务的关键因素，但是，所有这些安全性都是以很高代价取得的。简言之，防火墙会限制性能和可伸缩性。由于防火墙是会造成单故障点的在线设备，因此它会降低网络的可用性。 将防火墙技术与新出现的Web交换技术相结合可以使防火墙的性能、可用性和可伸缩性得到极大的改善。 最常用的防火墙由安装在一台服务器上的软件构成。这台服务器上安装了两块网卡，并被插入到数据路径上。其中的一块网卡连接到网络的公共端，公共端通常为与Internet相连的路由器（即所谓防火墙的“ 不洁 ”端）。另一块网卡与必须保护的资源相连（即所谓防火墙的“ 清洁 ”端）。 防火墙安装在数据路径上，因此限制了网络的性能和可伸缩性，原因是所有通过不洁端和清洁端的数据流都必须流过防火墙。防火墙使用过滤技术和其它由网络管理人员预先设定的策略，对每个数据包进行检查。 问题是最适于防火墙的处理结构并不适于检查高容量的数据包。扩展防火墙的性能十分困难，因为它通常涉及到成本的高昂升级：使用更高性能的配置及目前功能最强大处理器的服务器。 新出现的Web交换技术被人们普遍认为是扩展防火墙容量、提高防火墙设备总体可用性的解决方案。在实现防火墙负载平衡时，需要使用两台Web 交换机：一台安装在防火墙的清洁端，另一台安装在不洁端。每台Web交换机都将输入的IP流通过防火墙发向另一端的对应Web交换

机。这样就实现了在几个防火墙上的负载平衡，因此，使防火墙可以并行运行，扩展了防火墙的性能，并且消除了防火墙成为单故障点的可能。 与传统的包交换机不同，Web交换机具有保持以太网和千兆以太网速率传输的不同TCP会话的能力。由于防火墙是一种状态性（stateful）的设备，因此，所有与建立会话相关的数据包都要流过相同的防火墙。Web交换机智能地保持流经防火墙的数据流的状态信息，因而保证了所有在特定IP源／目的地址对之间传输的数据流都流过同一个防火墙。反过来，这也保证了防火墙建立的会话持续性。 防火墙负载平衡技术也可以被用来减少防火墙需要完成的数据流过滤功能的工作量，这正是实施“ 非军事区 ”（DMZ）技术的主要优点。在DMZ中保存象Internet这类Web服务器要求公共访问的资源。Web交换机需要具有数据流过滤功能来确定哪些数据包应当被传送到DMZ，哪些应当穿过防火墙。从防火墙上去除掉过滤功能大大提高了防火墙性能，加快了用户数据流的速度。 Web交换机被配置为允许或拒绝对DMZ服务器访问的过滤器，以这种方式实现了两级水平的安全性：一级利用配置在Web交换机上的过滤器对访问进行限制，另一级通过由防火墙进行的状态检查限制访问。 为保持防火墙的高可用性，Web交换机利用连续地向防火墙另一端的对应Web交换机上的每个端口发送强制回应命令（ping）来监控防火墙的“ 健康 ”情况。如果防火墙或Web交换机端口出现故障，数据流就被分配到其余的“ 健康 ”Web交换机端口和相关的防火墙上。 防火墙负载平衡利用新型Web交换技术解决了由防火墙引起的许多性能问题和可伸缩性问题。这项技术使防火墙可以并行地运行，在不用进行重大升级

的条件下，大大提高了效率，扩展了性能，并消除了防火墙成为单故障点的可能。 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