交换机路由器更加安全三种办法 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/251/2021_2022__E4_BA_A4_E6_8D_A2_E6_9C_BA_E8_c101_251134.htm 传统的网络安全技术侧重于系统入侵检测，反病毒软件或防火墙。内部安全如何？在网络安全构造中，交换机和路由器是非常重要的，在七层网络中每一层都必须是安全的。很多交换机和路由器都有丰富的安全功能，要了解有些什么，如何工作，如何部署，一层有问题时不会影响整个网络。交换机和路由器被设计成缺省安全的，出厂时就处于安全设置的状态，特别操作的设置在用户要求时才会被激活，所有其他选项都是关闭的，以减少危险，网管员也无需了解哪些选项应该关闭。 在初始登录时会被强制要求更改密码，也有密码的期限选项及登录尝试的次数限制，而且以加密方式存储。限期的帐号（维护帐号或后门）是不会存在的。交换机及路由器在掉电，热启动、冷启动，升级IOS、硬件或一个模块失败的情况下都必须是安全的，而且在这些事件发生后应该不会危及安全并恢复运作，因为日志的原因，网络设备应该通过网络时间协议保持安全精确的时间。通过SNMP协议连接管理的名称也应该被改变。 抵挡DoS攻击 从可用性出发，交换机和路由器需要能抵挡拒绝服务式Dos攻击，并在攻击期间保持可用性。理想状态是他们在受到攻击时应该能够做出反应，屏蔽攻击IP及端口。每件事件都会立即反应并记录在日志中，同时他们也能识别并对蠕虫攻击做出反应。 交换机及路由器中使用FTP，HTTP，TELNET或SSH都有可以有代码漏洞，在漏洞被发现报告后，厂商可以开发、创建、测试、发布升级包或补丁

。 基于角色的管理给予管理员最低程序的许可来完成任务，允许分派任务，提供检查及平衡，只有受信任的连接才能管理倔们。管理权限可赋予设备或其他主机，例如管理权限可授予一定IP地址及特定的TCP/UDP端口。 控制管理权限的最好办法是在授权进入前分权限，可以通过认证和帐户服务器，例如远程接入服务，终端服务，或LDAP服务。 远程连接的加密 很多情况下，管理员需要远程管理交换机及路由器，通常只能从公共网络上访问。为了保证管理传输的安全，需要加密协议，SSH是所有远程命令行设置和文件传输的标准协，基于WEB的则用SSL或TLS协议，LDAP通常是通讯的协议，而SSL/TLS则加密此通讯。 SNMP用来发现、监控、配置网络设备，SNMP3是足够安全的版本，可以保证授权的通信。建立登录控制可以减轻受攻击的可能性，设定尝试登录的次数，在遇到这种扫描时能做出反应。详细的日志在发现尝试破解密码及端口扫描时是非常有效的。 交换机及路由器的配置文件的安全也是不容忽视的，通常配置文件保存在安全的位置，在混乱的情况下，可以取出备份文件，安装并激活系统，恢复到已知状态。有些交换机结合了入侵检测的功能，一些通过端口映射支持，允许管理员选择监控端口。 虚拟网络的角色 虚拟的本地网络VLAN是第二层上的有限广播域，由一组计算机设备组成，通常位一多个LAN上，可能跨越一个或多个LAN交换机，而与它们的物理位置无关，设备之间好像在同一个网络间通信一样，允许管理员将网络分为多个可管理运行良好的小块，将啬、移动、更改设备、用户及权限的任务简化。 VLAN可在各种形式上形成，如交换口，MAC地址，IP地址，协议类型，DHCP，802.1Q标志或用

户自定义。这些可以单独或组合部署。 VLAN认证技术在用户通过认证过程后授权给用户进入一个或多个VLAN，该授权不是给予设备。 防火墙可以控制网络之间的访问，最广泛应用的是嵌在传统路由器和多层交换机上的，也称作ACLs，防火墙的不同主要在于他们扫描包的深度，是端到端的直接通讯还是通过代理，是否有session. 在网络之间的访问控制中，路由过滤措施可以基于源/目标交换槽或端口，源/目标VLAN，源/目标IP，或TCP/UDP端口，ICMP类型，或MAC地址。对于某些交换机和路由器，动态ACL标准可以用户通过认证过程后被创建，就像是认证的VLAN，不过是在第三层上。当未知的源地址要求连入已知的内部目标时是有用的。 现在的网络要求设计成各层次都是安全的，通过部署交换机和路由器的安全设置，企业可以传统的安全技术创建强壮、各层都安全的系统。 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