不可不知的路由交换安全七宗罪 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__E4_B8_8D_E5_8F_AF_E4_B8_8D_E7_c99_473.htm 企业网络管理员的最主要职责就是保证内网的安全，而在内网各个网络设备中路由交换特别是核心层的设备是对安全需求最高的，那么作为中小企业的网络管理员来说又该如何保证路由交换设备的安全呢?在实际工作过程中笔者接触到很多网络管理员，但是他们在路由交换设置上或多或少存在着安全隐患和漏洞，今天就让我们一起来看看路由交换安全的七宗罪。 密码明文化 有过路由交换配置经验的网络管理员都知道默认情况下我们给路由交换设备添加管理密码都通过enable password命令，不过这样建立的密码并不安全，他是以明文的形式存储在running配置文件中的，我们通过show running可以查看到该信息，非常不安全，因此我们需要通过另外一条命令来添加一个加密过的密码，具体指令为enable secret。 执行命令后我们再通过show running查看配置文件内容的话将会看到密码已经经过加密而存储在配置文件中，当然这个信息也不是百分之百安全的，毕竟MD5信息可以通过暴力破解还有一些站点也提供MD5密文反查服务。不过不管怎么说其安全性大大提高。 密码同一化 还有一些网络管理员认为记忆多了密码容易混淆，所以在配置路由交换设备时使用了和自己管理的服务器一样的密码，实际上这也是不安全的，密码同一化会大大提高网络设备被攻击的可能，毕竟设备多了难免会被攻击，一旦某个设备被入侵，那么密码同一化将造成所有设备密码的泄露。另外路由交换设备自身都提供了很多级密码，例如常规模式密码

，特权模式密码，配置模式密码等，还有console口连接密码，Telnet访问密码等，我们在设置时也要对这些模式与密码区别化，不要全部设置为一样。通过不同级别的密码对不同用户进行授权，从而避免越权问题的发生。 小提示：默认情况下网络设备都可以利用启动期间的BREAK方式来进入到监听ROMMON模式进行口令恢复，这就存在一个安全隐患，任何人只要靠近网络设备就都可以通过控制台端口来完成重新设置密码的任务，所以我们在保证密码记忆牢靠的情况下可以关闭这个密码恢复方式，通过no service password-recovery命令完成关闭ROMMON监听模式的任务。 密码同级化 所谓密码同级化就是指不针对不同模式和不同配置接口分配不同的密码，管理路由器只通过唯一密码即可完成。实际上这也是错误的，毕竟平时访问和管理路由交换设备的用户不可能只有你一个，所以合理的将密码分级设置分级管理是非常重要的，适当的分配visit,monitor,system,manage等权限会让你的安全工作游刃有余，而在实际应用过程中这些密码分级化也大大提高了核心路由交换设备的安全。 另外在密码管理方面还存在一个最大问题，那就是临时密码的处理，很多时候当网络出现故障后也许我们需要向厂商寻求技术支持，在这种情况下我们不应该把原来的密码直接告诉技术支持人员，通过设置一个临时密码的方式来解决远程或异地异人维护问题，在维护完毕后也要记得停止临时帐户，笔者就发现很多下属网络管理员在向我寻求帮助时直接告诉了管理员帐户，又或者即使建立了临时帐户，几个月后还能够通过该帐户登录和管理。这些都为路由交换设备带来了一定的安全隐患。 小提示：默认情况下通过console口控制台登录路由交换设备是

不需要密码的，但是为了保证安全我们还是应该为其设置一个密码，通过以下命令来完成line console 0,login,password XXXXXX，最后再通过service password-encryption命令对设置的密码加密。 管理随意化 实际上对于一台路由交换设备来说，我们可以通过远程终端，本地终端，WEB，TFTP服务器，虚拟终端，SSH等多个方式对其进行配置，在网络设备加固工作时最好都使用本地终端的方式，即通过PC机的超级终端和交换机的Console口进行配置，这是因为在安全加固过程中要避免外界干扰，通过本地终端连接路由器可以防止管理员因为操作不当后被拒绝登录到网络设备事情的发生。 当然如果我们实在需要使用非本地超级终端的方式进行管理，那么最标准的管理路由交换设备的方法是通过访问控制列表ACL来阻止非授权IP地址对路由交换设备的访问，这样就算非法人员知道了管理密码也会因使用的IP未授权而无法入侵。就个人经验来说对内网可以通过划分VLAN虚拟局域网的形式控制访问权限，而对外网则要借助ACL访问控制列表来精细化的分配授权。 管理明文化 管理明文化这个安全缺陷是目前中小企业中最为普遍的问题，大多数网络管理员都通过telnet来管理相关设备，还有部分人员借助设备自身提供的HTTP页面管理模式完成配置工作，要知道不管是telnet还是HTTP都是不安全的，任何连接内网且使用sniffer类工具的人员都可以轻松的嗅探到管理密码及配置口令。所以说在管理上尽量使用SSH或HTTPS等经过加密的协议，这样可以有效避免sniffer类工具的嗅探。关于通过SSH来连接路由交换设备的方法我们在之前的文章中已经介绍过，这里就不详细说明了，感兴趣的读者可以参考相关内容。 要想开启路由交换设备

的HTTPS管理我们需要执行以下操作首先进入到路由交换设备的配置模式，然后执行ip http server-secure，默认HTTPS是使用443端口进行管理和访问的，我们可以通过ip http secure-port XXX来更改默认管理端口。 SNMP低权限 很多网络管理员为了自己方便或者通过第三方工具来管理内网流量，这时我们都需要在核心路由交换设备上开启SNMP协议的支持，SNMP的开启同样存在问题，很多用户都使用默认的snmp社区名以及分配WRITE可读可写的权限，要知道这是非常危险的，很多网络管理软件都可以获取路由交换设备发来的SNMP数据信息，如果对应的管理社区帐户名具备可读可写权限的话，入侵者可以轻易的利用SNMP协议获取路由交换设备的配置文件，再通过暴力破解等方法直接窃取到登录密码。因此在维护路由交换设备时尽可能的不使用SNMP协议，如果必须使用那么修改默认缺省的社区名以及分配一个低的RO只读权限可以在一定程度上保护路由交换设备自身。 网络同一化 最后我要说的则是网络同一化问题，很多企业很少针对网络进行规划，系统集成商实施完后网络参数与配置就没有改变过，要知道网络同一化让企业所有网络设备都处于同一个网络，一方面造成广播数据包的增多，影响网络通讯效率，另外一方面也不利于隐私数据的保护，企业内部任何一台计算机被入侵后都可以将其作为跳板来攻击其他所有设备。因此将网络适当的分隔也是解决上述问题的最好办法。就个人经验来说通过划分VLAN虚拟局域网的方式是最简单和直接有效的，当然在划分时要根据企业网络规模和客户端数量去设计，每个VLAN内部的主机数量要适当。 总结：当然本文介绍的仅仅是大家在网络管理和维护过程中最容

易犯的小毛病，但是有时小错误一样会引来大麻烦，所以说在维护路由交换设备过程中我们应该养成好的习惯，从根本上杜绝上述七宗罪的发生，让企业内网更加安全。